

Óscar Jesús Rubio Martín

# Design of a secure architecture for the exchange of biomedical information in m-Health scenarios

Departamento  
Instituto de Investigación en Ingeniería [I3A]

Director/es  
Alesanco Iglesias, Álvaro  
García Moros, José

<http://zaguan.unizar.es/collection/Tesis>







**Universidad**  
Zaragoza

Tesis Doctoral

# DESIGN OF A SECURE ARCHITECTURE FOR THE EXCHANGE OF BIOMEDICAL INFORMATION IN M-HEALTH SCENARIOS

Autor

Óscar Jesús Rubio Martín

Director/es

Alesanco Iglesias, Álvaro  
García Moros, José

**UNIVERSIDAD DE ZARAGOZA**

Instituto de Investigación en Ingeniería [I3A]

2016





**Universidad Zaragoza**

**PhD Dissertation**

Biomedical Engineering Doctoral Program

---

DESIGN OF A SECURE ARCHITECTURE FOR  
THE EXCHANGE OF BIOMEDICAL INFORMATION  
IN M-HEALTH SCENARIOS

---

PhD Candidate:

**Óscar J. Rubio Martín**

Advisors:

**Álvaro Alesanco Iglesias and José García Moros**

Aragón Institute of Engineering Research (I3A)  
Communications Networks and Information Technologies  
for E-health and Quality of experience group (CeNITEQ)

*Zaragoza, December 2015*







*Dedicado a mis padres, mi hermana y mi novia.*





# Agradecimientos

La realización de una tesis doctoral supone un importante hito en la carrera —de fondo— de cualquier investigador. En las etapas de esta carrera se alternan colaboraciones muy productivas, plazos de entrega ajustados, asistencia a congresos en los que se conocen otros trabajos e investigadores, etapas muy prolíficas en forma de publicaciones, críticas afiladas de nuestros trabajos que nos obligan a mejorar y condiciones económicas que en ocasiones limitan nuestras posibilidades. Como en cualquier instancia de mi vida, en mi camino hacia el doctorado me han acompañado mi familia, mi novia, mis amigos y mis compañeros, tanto para celebrar lo bueno como para afrontar lo difícil.

En primer lugar me gustaría dar las gracias a mi hermana Ana por su cercanía, por sus bromas y por su incombustible *thinking out of the box*; a mi madre por su continuo apoyo, cariño y ejemplo de trabajo; y a mi padre por inculcarme el gusto por la tecnología y la superación —a través del deporte— desde muy pequeño.

Para mi novia Anita un enorme beso por quererme, animarme e ilusionarme cada día más que el anterior, contigo de aquí hasta Las Vegas.

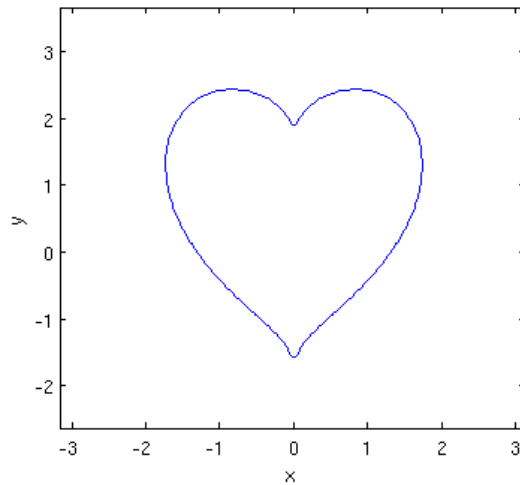
De entre todos mis amigos, mi especial agradecimiento a Nut y Rossi, mis pequeños confidentes y las personas que amenizan cada uno de mis días con sus ocurrencias y reflexiones. También a mis amigos de *tout la vie*, los Nachos, Tamara, Arturo, Patricia, María y Pilar; desde siempre disfrutando de la vida, cuidándonos y creciendo juntos.

A lo largo de estos años universitarios también he tenido la oportunidad de conocer y estrechar lazos con personas extraordinarias. No puedo dejar de acordarme de Pedro y Carlos, Alfonso, Ángel, Manolo, Jesús Lázaro, Mou, Fernando, Julia, Iker, Igor, Xavi, Héctor, Alicja, Álex, Elena y Albert. Con ellos he pasado muchísimas horas de biblioteca, hemos comido y bebido juntos, preparado exámenes y prácticas, jugado a las cartas en la cafetería, compartido vacaciones por Europa, hecho un Erasmus (la mili del siglo XXI), asistido a congresos y disfrutado el *student lifestyle*. También me gustaría resaltar la importancia de todas las personas con las que he coincidido en el laboratorio 2.05. Y muy en especial, mi jefica Eva, que me ayudó mucho en los primeros compases de mi investigación

y ha sido una compañera excepcional; Jose María Saldaña, que me ha dado mil y un páticos y valiosos consejos (los relacionados con *Microsoft* nunca calaron); Idelkys Quintana, que a diario ameniza la atmósfera del laboratorio; y Jesús Trigo, con el que he tenido la oportunidad de colaborar estrechamente durante la última etapa de mi investigación y del que he aprendido muchísimo.

En lo académico, me gustaría comenzar agradeciendo a Álvaro y a Josechu que me diesen la posibilidad de unirme al grupo de Telemedicina y eSalud (ahora actualizado a eHealthZ), que me hayan formado como investigador y que hayan apoyado y supervisado mi trabajo con paciencia y dedicación. Su amplia experiencia, sus acertadas ideas y consejos y su disponibilidad para atender mis consultas me han hecho avanzar y mejorar notablemente. *Last but not least*, me gustaría dar mi sincero reconocimiento a seis grandes profesores de mi etapa pre-universitaria: don Ricardo Gómez, don Dimas Vaquero, Luis Vivas, Arturo Ansón, Teresa Arnal y Ángel Puyuelo. Todos ellos tuvieron una gran influencia en mi, como referentes personales y académicos.

A todos vosotros con mucho  $x^2 + (y - \sqrt{|x|})^2 = 3$ .







## Resumen y conclusiones

El paradigma de m-Salud (salud móvil) aboga por la integración masiva de las más avanzadas tecnologías de comunicación, red móvil y sensores en aplicaciones y sistemas de salud, para fomentar el despliegue de un nuevo modelo de atención clínico centrado en el usuario/paciente. Este modelo tiene por objetivos el empoderamiento de los usuarios en la gestión de su propia salud (p.ej. aumentando sus conocimientos, promocionando estilos de vida saludable y previniendo enfermedades), la prestación de una mejor tele-asistencia sanitaria en el hogar para ancianos y pacientes crónicos y una notable disminución del gasto de los Sistemas de Salud gracias a la reducción del número y la duración de las hospitalizaciones. No obstante, estas ventajas, atribuidas a las aplicaciones de m-Salud, suelen venir acompañadas del requisito de un alto grado de disponibilidad de la información biomédica de sus usuarios para garantizar una alta calidad de servicio, p.ej. fusionar varias señales de un usuario para obtener un diagnóstico más preciso. La consecuencia negativa de cumplir esta demanda es el aumento directo de las superficies potencialmente vulnerables a ataques, lo que sitúa a la seguridad (y a la privacidad) del modelo de m-Salud como factor crítico para su éxito.

Como requisito no funcional de las aplicaciones de m-Salud, la seguridad ha recibido menos atención que otros requisitos técnicos que eran más urgentes en etapas de desarrollo previas, tales como la robustez, la eficiencia, la interoperabilidad o la usabilidad. Otro factor importante que ha contribuido a retrasar la implementación de políticas de seguridad sólidas es que garantizar un determinado nivel de seguridad implica unos costes que pueden ser muy relevantes en varias dimensiones, como la económica (p.ej. sobrecostes por la inclusión de hardware extra para la autenticación de usuarios), el rendimiento (p.ej. reducción de la eficiencia y de la interoperabilidad debido a la integración de elementos de seguridad) y la usabilidad (p.ej. configuración más complicada de dispositivos y aplicaciones de salud debido a las nuevas opciones de seguridad). Por tanto, las soluciones de seguridad que persigan satisfacer a todos los actores del contexto de m-Salud (usuarios, pacientes, personal médico, personal técnico, legisladores, fabricantes de dispositivos y equipos, etc.) deben ser robustas y al mismo tiempo minimizar sus costes asociados.

Esta Tesis detalla una propuesta de seguridad, compuesta por cuatro grandes bloques interconectados, para dotar de seguridad a las arquitecturas de m-Salud con unos costes reducidos. El primer bloque define un esquema global que proporciona unos niveles de seguridad e interoperabilidad acordes con las características de las distintas aplicaciones de m-Salud. Este esquema está compuesta por tres capas diferenciadas, diseñadas a la medida de los dominios de m-Salud y de sus restricciones, incluyendo medidas de seguridad adecuadas para la defensa contra las amenazas asociadas a sus aplicaciones de m-Salud. El segundo bloque establece la extensión de seguridad de aquellos protocolos estándar que permiten la adquisición, el intercambio y/o la administración de información biomédica — por tanto, usados por muchas aplicaciones de m-Salud — pero no reúnen los niveles de seguridad detallados en el esquema previo. Estas extensiones se concretan para los estándares biomédicos ISO/IEEE 11073 PHD y SCP-ECG. El tercer bloque propone nuevas formas de fortalecer la seguridad de los tests biomédicos, que constituyen el elemento esencial de muchas aplicaciones de m-Salud de carácter clínico, mediante codificaciones novedosas. Finalmente el cuarto bloque, que se sitúa en paralelo a los anteriores, selecciona herramientas de seguridad genéricas (elementos de autenticación y criptográficos) cuya integración en los otros bloques resulta idónea, y desarrolla nuevas herramientas de seguridad, basadas en señal — *embedding* y *keytagging* —, para reforzar la protección de los test biomédicos.

Las extensiones de los estándares ISO/IEEE 11073 PHD y SCP-ECG, basadas en el modelo de capas, pueden considerarse robustas, eficientes y respetuosas con sus contenidos y características originales. La primera no añade ningún nuevo atributo a su modelo de datos, cuatro tramas a su modelo de servicios —otras cuatro son extendidas con nuevas subtramas—, y sólo un nuevo sub-estado al modelo de comunicaciones. Además, una arquitectura sencilla compuesta por un dispositivo de salud personal equipado con un simple procesador de 9 MHz y un agregador equipado con un procesador de 1 GHz es capaz de transmitir un electrocardiograma de 3 derivaciones en tiempo real utilizando la capa de seguridad máxima. Los otros requisitos asociados a esta extensión son una configuración inicial del dispositivo de salud y del agregador, la instalación de identificadores/autenticadores de usuarios en estos dispositivos si van a compartirse y la implementación de ciertos perfiles IHE en el agregador para que los datos recogidos puedan integrarse en sistemas de salud. Respecto a la extensión del SCP-ECG, ésta sólo añade una nueva sección con elementos de seguridad y sintaxis para proteger el resto del fichero e implementar un control de acceso basado en roles. El *overhead* introducido en un fichero SCP-ECG protegido es típicamente el 2–13% del tamaño original, y los retardos extra para generar un fichero SCP-ECG protegido y acceder a él para su interpretación suponen respectivamente un 2–10% y un 5% de los retardos originales.

Respecto a las técnicas de protección basadas en señal, el método de *embedding* que se ha desarrollado es la base para la propuesta de una codificación genérica para tests compuestos de señales biomédicas, medidas periódicas e información contextual. Esta codificación ha sido evaluada y específicamente refinada para tests basados en electrocardiogramas y electroencefalogramas, demostrando que el test codificado mantiene su calidad clínica, que el sistema de codificación-acceso es capaz de funcionar en tiempo real (con retardos totales de 2 s para electrocardiogramas y 3.3 s para electroencefalogramas) y que su interfaz tiene una gran usabilidad. Pese a la introducción de elementos de seguridad y metadatos dentro de la señal, para habilitar servicios de m-Salud, se han logrado ratios de compresión que van desde  $\simeq 3$  para transmisión en tiempo real hasta  $\simeq 5$  cuando se funciona *offline*. Complementariamente, el método de *keytagging* permite asociar información a imágenes (y otras señales) por medio de llaves, de una manera segura y sin distorsión. Estas características ventajosas han sido aprovechadas para la implementación de varias medidas de seguridad: autenticación de imágenes, control de integridad y localización de zonas modificadas sin permiso, asociación de información con control de roles, trazabilidad y protección de *copyright*. La evaluación realizada demuestra el notable compromiso robustez-capacidad ofrecido por esta técnica, que permite implementar todas las medidas anteriores simultáneamente, y su compatibilidad con el sistema de compresión JPEG2000, ya que se mantiene el compromiso anterior a la vez que se establece un retardo global de *keytagging* de sólo  $\simeq 120\text{ ms}$  para cualquier tamaño de imagen — lo que evidencia su escalabilidad.

Como conclusión general, se ha demostrado e ilustrado con ejemplos que hay varias formas, complementarias y estructuradas, de contribuir a la implementación de unos niveles de seguridad adecuados para las arquitecturas de m-Salud, con un coste moderado en lo que respecta a economía, rendimiento, interoperabilidad y usabilidad. El panorama de m-Salud evoluciona constantemente a lo largo de todas sus dimensiones, y esta Tesis pretende hacer lo propio con sus seguridad. Además, las lecciones aquí aprendidas pueden servir de guía para la elaboración de esquemas de seguridad más exhaustivos y actualizados, para la extensión de otros estándares biomédicos con niveles bajos de seguridad o privacidad, y para el avance del estado del arte de sistemas de protección basados en señal y sus aplicaciones.





# Abstract

The paradigm of m-Health (mobile health) advocates for the massive integration of advanced mobile communications, network and sensor technologies in healthcare applications and systems to foster the deployment of a new, user/patient-centered healthcare model enabling the empowerment of users in the management of their health (e.g. by increasing their health literacy, promoting healthy lifestyles and the prevention of diseases), a better home-based healthcare delivery for elderly and chronic patients and important savings for healthcare systems due to the reduction of hospitalizations in number and duration. It is a fact that many m-Health applications demand high availability of biomedical information from their users (for further accurate analysis, e.g. by fusion of various signals) to guarantee high quality of service, which on the other hand entails increasing the potential surfaces for attacks. Therefore, it is not surprising that security (and privacy) is commonly included among the most important barriers for the success of m-Health.

As a non-functional requirement for m-Health applications, security has received less attention than other technical issues that were more pressing at earlier development stages, such as reliability, efficiency, interoperability or usability. Another fact that has contributed to delaying the enforcement of robust security policies is that guaranteeing a certain security level implies costs that can be very relevant and that span along different dimensions. These include budgeting (e.g. the demand of extra hardware for user authentication), performance (e.g. lower efficiency and interoperability due to the addition of security elements) and usability (e.g. cumbersome configuration of devices and applications due to security options). Therefore, security solutions that aim to satisfy all the stakeholders in the m-Health context (users/patients, medical staff, technical staff, systems and devices manufacturers, regulators, etc.) shall be robust and, at the same time, minimize their associated costs.

This Thesis details a proposal, composed of four interrelated blocks, to integrate appropriate levels of security in m-Health architectures in a cost-efficient manner. The first block defines a global scheme that provides different security and interoperability levels according to how critical are the m-Health applications to be implemented. This consists of

three layers tailored to the m-Health domains and their constraints, whose security countermeasures defend against the threats of their associated m-Health applications. Next, the second block addresses the security extension of those standard protocols that enable the acquisition, exchange and/or management of biomedical information — thus, used by many m-Health applications — but do not meet the security levels described in the former scheme. These extensions are materialized for the biomedical standards ISO/IEEE 11073 PHD and SCP-ECG. Then, the third block proposes new ways of enhancing the security of biomedical standards, which are the centerpiece of many clinical m-Health applications, by means of novel codings. Finally the fourth block, with is parallel to the others, selects generic security methods (for user authentication and cryptographic protection) whose integration in the other blocks results optimal, and also develops novel signal-based methods —embedding and keytagging— for strengthening the security of biomedical tests.

The layer-based extensions of the standards ISO/IEEE 11073 PHD and SCP-ECG can be considered as robust, cost-efficient and respectful with their original features and contents. The former adds no attributes to its data information model, four new frames to the service model —and extends four with new sub-frames—, and only one new sub-state to the communication model. Furthermore, a lightweight architecture consisting of a personal health device mounting a 9 MHz processor and an aggregator mounting a 1 GHz processor is enough to transmit a 3-lead electrocardiogram in real-time implementing the top security layer. The extra requirements associated to this extension are an initial configuration of the health device and the aggregator, tokens for identification/authentication of users if these devices are to be shared and the implementation of certain IHE profiles in the aggregator to enable the integration of measurements in healthcare systems. As regards to the extension of SCP-ECG, it only adds a new section with selected security elements and syntax in order to protect the rest of file contents and provide proper role-based access control. The overhead introduced in the protected SCP-ECG is typically 2–13 % of the regular file size, and the extra delays to protect a newly generated SCP-ECG file and to access it for interpretation are respectively a 2–10 % and a 5 % of the regular delays.

As regards to the signal-based security techniques developed, the embedding method is the basis for the proposal of a generic coding for tests composed of biomedical signals, periodic measurements and contextual information. This has been adjusted and evaluated with electrocardiogram and electroencephalogram-based tests, proving the objective clinical quality of the coded tests, the capacity of the coding-access system to operate in real-time (overall delays of 2 s for electrocardiograms and 3.3 s for electroencephalograms) and its high usability. Despite of the embedding of security and metadata to enable m-Health services, the compression ratios obtained by this coding range from  $\simeq 3$  in real-time transmission to  $\simeq 5$  in offline operation. Complementarily, keytagging permits

associating information to images (and other signals) by means of keys in a secure and non-distorting fashion, which has been availed to implement security measures such as image authentication, integrity control and location of tampered areas, private captioning with role-based access control, traceability and copyright protection. The tests conducted indicate a remarkable robustness-capacity tradeoff that permits implementing all this measures simultaneously, and the compatibility of keytagging with JPEG2000 compression, maintaining this tradeoff while setting the overall keytagging delay in only  $\simeq 120$  *ms* for any image size — evidencing the scalability of this technique.

As a general conclusion, it has been demonstrated and illustrated with examples that there are various, complementary and structured manners to contribute in the implementation of suitable security levels for m-Health architectures with a moderate cost in budget, performance, interoperability and usability. The m-Health landscape is evolving permanently along all their dimensions, and this Thesis aims to do so with its security. Furthermore, the lessons learned herein may offer further guidance for the elaboration of more comprehensive and updated security schemes, for the extension of other biomedical standards featuring low emphasis on security or privacy, and for the improvement of the state of the art regarding signal-based protection methods and applications.



## Scientific Contributions

Next peer-reviewed scientific publications have been derived from the research of this thesis.

### Publications in International Journals (JCR indexed)

**Ó.J. Rubio**, Á. Alesanco, and J. García, “Introducing keytagging, a novel technique for the protection of medical image-based tests”, *Journal of Biomedical Informatics*, vol. 56, no. 0, pp. 8–29, 2015.

**Ó.J. Rubio**, Á. Alesanco, and J. García, “Secure information embedding into 1D biomedical signals based on SPIHT”, *Journal of Biomedical Informatics*, vol. 46, no. 4, pp. 653–664, 2013.

**Ó.J. Rubio**, Á. Alesanco, and J. García, “A robust and simple security extension for the medical standard SCP-ECG”, *Journal of Biomedical Informatics*, vol. 46, no. 1, pp. 142–151, 2012.

### Submitted Publications in International Journals (JCR indexed)

**Ó.J. Rubio**, J.D. Trigo, Á. Alesanco, L. Serrano and J. García, “Analysis of ISO/IEEE 11073 built-in security and its potential IHE-based extensibility”, *Journal of Biomedical Informatics*.

### Preparation Publications in International Journals (JCR indexed)

J.D. Trigo, **Ó.J. Rubio**, Miguel Martínez-Espronceda, Á. Alesanco, J. García and L. Serrano, “Building standardized, secure, social-media-based mHealth services”, *Journal of Biomedical Informatics*.

### Publications in International Conferences and Proceedings

Á. Alesanco, **Ó.J. Rubio**, E. Cavero, J. Sancho, and J. Garcia, “Secure and com-

pact image-based storage format for DICOM multiframe echocardiogram video”, in *XIV Mediterranean Conference on Medical and Biological Engineering and Computing (MEDICON)*, 2016. [Under review]

**Ó.J. Rubio**, Á. Alesanco, and J. Garcia, “Secure and efficient coding of biomedical signals, periodic measurements and contextual data in Body Area Networks”, in *IEEE Biomedical and Health Informatics (BHI)*, 2014, June, pp. 231–234.

**Ó.J. Rubio**, Á. Alesanco, and J. Garcia, “Seamless integration of watermarks in DICOM images”, in *Computing in Cardiology (CinC)*, 2013, Sept., pp. 25–28.

**Ó.J. Rubio**, Á. Alesanco, and J. Garcia, “A security extension for the standard SCP-ECG based on metadata”, in *Computing in Cardiology (CinC)*, 2012, Sept., pp. 81–84.

#### Publications in National Conferences and Proceedings

**Ó.J. Rubio**, Á. Alesanco, and J. García, “Hacia la integración de ISO/IEEE 11073 PHD en IHE,” in *XXXII Congreso Anual de la Sociedad Española de Ingeniería Biomédica (CASEIB)*, 2014, Noviembre.

**Ó.J. Rubio**, Á. Alesanco, and J. García, “Extensión de seguridad del protocolo SCP-ECG mediante perfiles de acceso y almacenamiento,” in *XXIX Congreso Anual de la Sociedad Española de Ingeniería Biomédica (CASEIB)*, 2011, Noviembre.

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	The m-Health scenario and its security issues . . . . .	1
1.2	The m-Health architecture . . . . .	5
1.2.1	Biomedical data flows and interoperability . . . . .	7
1.2.2	Biomedical tests coding . . . . .	10
1.3	Security trends in m-Health and what can be improved . . . . .	12
1.3.1	Security in protocols for the exchange of biomedical information . . . . .	12
1.3.2	Signal-based protection . . . . .	14
1.3.3	What can be improved? . . . . .	20
1.4	Thesis approach, hypothesis and objectives . . . . .	25
1.5	Research context . . . . .	27
1.6	Thesis outline . . . . .	28
<b>2</b>	<b>M-Health architectures: Background and proposed guidelines for their security enhancement</b>	<b>29</b>
2.1	Overview of major standards for exchanging biomedical information . . . . .	29
2.1.1	IHE & profiles overview . . . . .	30
2.1.2	ISO/IEEE 11073 PHD overview . . . . .	32
2.1.3	SCP-ECG overview . . . . .	35
2.1.4	DICOM overview . . . . .	40
2.1.5	Related publications on the protection of biomedical standards . . . . .	45
2.2	Overview of major biomedical signal coding methods . . . . .	48
2.2.1	Wavelet transform overview . . . . .	48
2.2.2	SPIHT overview . . . . .	51
2.2.3	JPEG2000 overview . . . . .	56
2.2.4	Related publications on signal-based protection . . . . .	58
2.3	Overview of transport technologies in the m-Health architecture . . . . .	61
2.4	Legal regulations . . . . .	63
2.5	Risk assessment of the m-Health architecture . . . . .	65

2.6	Guidelines for the security enhancement of the m-Health architecture . . . .	68
2.6.1	Additive, layered structure . . . . .	68
2.6.2	IHE profiles in each layer . . . . .	70
2.6.3	Suggested algorithms for the SDO Profile . . . . .	73
2.6.4	Integration of signal-based protection within biomedical standards .	77
2.6.5	Implications for IHE and its profiles . . . . .	82
<b>3</b>	<b>Enhancement of the security of standard protocols for the exchange of biomedical information</b>	<b>83</b>
3.1	Enhancement of the security of ISO/IEEE 11073 Personal Health Devices .	85
3.2	Evaluation of the security-enhanced ISO/IEEE 11073 PHD . . . . .	91
3.2.1	Risk assessment . . . . .	91
3.2.2	Implications for ISO/IEEE 11073 PHD . . . . .	93
3.2.3	Impact on the ISO/IEEE 11073 PHD architecture and on its frame- work . . . . .	98
3.2.4	Potential limitations . . . . .	102
3.3	Enhancement of the security of SCP-ECG . . . . .	103
3.3.1	Privacy profiles for Role Based Access Control (RBAC) . . . . .	103
3.3.2	SCP-ECG extension . . . . .	107
3.4	Evaluation of the security-enhanced SCP-ECG . . . . .	110
3.4.1	Risk assessment . . . . .	110
3.4.2	Implications for SCP-ECG and impact on its architecture . . . . .	112
3.4.3	Potential limitations . . . . .	113
3.5	Proof of concept . . . . .	114
3.6	Conclusions . . . . .	115
<b>4</b>	<b>Enhancement of the security of biomedical tests through their associated signals</b>	<b>117</b>
4.1	Novel coding for biomedical tests . . . . .	118
4.1.1	Signal compression . . . . .	120
4.1.2	Embedding metadata within the signal . . . . .	123
4.1.3	Partial signal encryption . . . . .	127
4.2	Experimental evaluation of the coding for biomedical tests . . . . .	128
4.2.1	Evaluation setup . . . . .	129
4.2.2	Bounding signal distortion in compression . . . . .	129
4.2.3	Runtime costs and bandwidth requirements . . . . .	131
4.2.4	Embedding Capacity . . . . .	135
4.3	Proof of concept . . . . .	137
4.4	Secure m-Health applications based on the novel coding . . . . .	139



4.4.1	Risk assessment . . . . .	141
4.4.2	Potential limitations . . . . .	143
4.5	Keytagging biomedical image-based tests . . . . .	144
4.5.1	Preprocessing . . . . .	144
4.5.2	Selection of suitable image features . . . . .	147
4.5.3	Coding and decoding of keytags . . . . .	149
4.5.4	Cryptographic protection of keytags . . . . .	151
4.5.5	Support for JPEG2000 compression . . . . .	155
4.6	Experimental evaluation of keytagging . . . . .	155
4.6.1	Evaluation setup . . . . .	155
4.6.2	Robustness-capacity . . . . .	164
4.6.3	Specificity . . . . .	165
4.6.4	Effect of JPEG2000 compression . . . . .	166
4.6.5	Average runtime cost . . . . .	169
4.6.6	Scalability . . . . .	171
4.7	Protection of biomedical images by means of keytagging . . . . .	172
4.7.1	Integration of keytagging in m-Health architectures . . . . .	173
4.7.2	Image resynchronization . . . . .	173
4.7.3	Image authentication and traceability . . . . .	175
4.7.4	Copyright protection . . . . .	176
4.7.5	Private captioning with RBAC . . . . .	176
4.7.6	Integrity control and location of tampered areas . . . . .	177
4.7.7	Simultaneous implementation . . . . .	177
4.7.8	Risk assessment . . . . .	179
4.7.9	Potential limitations . . . . .	182
4.8	Conclusions . . . . .	182
<b>5</b>	<b>Conclusions</b>	<b>185</b>
5.1	Research objectives achieved . . . . .	185
5.2	Contributions and accomplished results . . . . .	186
5.3	Future work . . . . .	192
	Bibliography . . . . .	197



## List of Figures

1.1	Generic m-Health architecture. . . . .	6
1.2	Turnita's interoperability model. . . . .	8
1.3	Example of enhancement of the security of biomedical image tests through watermarking. . . . .	18
1.4	Building blocks for a secure, cost-efficient, m-Health architecture. . . . .	21
1.5	M-Health architecture intended for simple open-source platforms. . . . .	24
2.1	ISO/IEEE 11073 PHD standards overview. . . . .	33
2.2	ISO/IEEE 11073 PHD three-level architecture. . . . .	34
2.3	SCP-ECG standard overview. . . . .	38
2.4	Calibration regions for the M mode of an echocardiogram acquired with an Agilent device. . . . .	43
2.5	Stack proposal for secure health monitoring . . . . .	46
2.6	5th-level wavelet decomposition of an echocardiogram image. . . . .	50
2.7	2-D wavelet filter bank . . . . .	51
2.8	Subbands and spatial orientation tree of a SPIHT coding example. . . . .	52
2.9	Processes of the JPEG2000 encoder and decoder. . . . .	58
2.10	Building blocks for a secure, cost-efficient, m-Health architecture. Contents addressed in Chapter 2 surrounded in red. . . . .	68
2.11	Layer-based proposal for a secure, cost-efficient, m-Health architecture. . . . .	72
2.12	Echocardiogram regions of the color Doppler mode . . . . .	78
2.13	Example of XML file to support the new image format. . . . .	80
3.1	Building blocks for a secure, cost-efficient, m-Health architecture. Contents addressed in Chapter 3 surrounded in red. . . . .	85
3.2	Steps for a successful first connection between an agent and a manager in the extended X73PHD . . . . .	86
3.3	Finite State Machine of the extended X73PHD . . . . .	94
3.4	A scenario of use for the SCP-ECG security extension . . . . .	105
3.5	Security-enhanced SCP-ECG file types . . . . .	106

3.6	SCP-ECG↔Security-enhanced SCP-ECG graphical user interface . . . . .	114
4.1	Building blocks for a secure, cost-efficient, m-Health architecture. Contents addressed in Chapter 4 surrounded in red. . . . .	118
4.2	Proposed coding (and decoding) for 1D biomedical tests in m-Health archi- tectures . . . . .	121
4.3	Sample ECG and EEG and their compressed, clinically-valid counterparts .	130
4.4	Embedding capacity of <i>Coded Test Units</i> corresponding to sample ECGs and EEGs . . . . .	136
4.5	GUI to code and decode <i>Coded Test Units</i> . . . . .	138
4.6	Main steps for the association of a stable keytag. . . . .	146
4.7	Sample images from the keytagging test set, belonging to different acqui- sition modalities. . . . .	157
4.8	Original <i>ROI</i> of a PET-CT image and the result of performing various modification . . . . .	158
4.9	Integration of keytagging in m-Health architectures. . . . .	172
4.10	Examples of location of tampered areas in keytagged images . . . . .	178

## List of Tables

1.1	Selected IHE profiles, mapped to security and privacy controls . . . . .	13
1.2	Comparison of steganography, watermarking and encryption in the m-Health context . . . . .	15
2.1	SCP-ECG Data Sections . . . . .	37
2.2	Relevant fields of the DICOM header from an Acuson device . . . . .	42
2.3	First steps of a SPIHT coding example . . . . .	54
2.4	Security features of transport technologies eligible for m-Health architectures	62
2.5	IHE profiles to be created and implemented for the enhancement of security and interoperability in m-Health architectures . . . . .	71
2.6	Cryptographic key length recommendations by NIST . . . . .	74
2.7	Cryptoperiods recommended by NIST for different types of key uses . . . . .	75
2.8	Performance of relevant cryptographic functions . . . . .	76
3.1	Operators and notation of the extensions of X73PHD and SCP-ECG . . . . .	84
3.2	Steps for a successful first connection between an agent and a manager in the extended X73PHD (I) . . . . .	88
3.3	Steps for a successful first connection between an agent and a manager in the extended X73PHD (II) . . . . .	89
3.4	Steps for a successful first connection between an agent and a manager in the extended X73PHD (III) . . . . .	90
3.5	Security analysis of the extended X73PHD . . . . .	92
3.6	New and modified frames and attributes in the extended X73PHD (I) . . . . .	95
3.7	New and modified frames and attributes in the extended X73PHD (II) . . . . .	96
3.8	New and modified frames and attributes in the extended X73PHD (III) . . . . .	97
3.9	Overhead and runtime costs of the extended X73PHD . . . . .	99
3.10	Structure and content of the Section 12 Data Part of a security-enhanced SCP-ECG file . . . . .	109
3.11	Typical size of Section 12 fields of a security-enhanced SCP-ECG file . . . . .	112

4.1	Operators and notation of the algorithm for coding biomedical tests . . . .	119
4.2	Structure and content of a <i>Recovery Container</i> . . . . .	126
4.3	Typical size of the containers in a <i>Secure Frame</i> . . . . .	128
4.4	Bitrate required for the transmission of <i>Coded Test Units</i> including <i>meta-</i> <i>data</i> with different elements . . . . .	133
4.5	Runtime costs involved in the coding and decoding of <i>Coded Test Units</i> . .	134
4.6	Average embedding capacity of <i>Coded Test Units</i> corresponding to various ECG and EEG-based tests . . . . .	135
4.7	Operators and notation of the keytagging algorithm . . . . .	145
4.8	Average energy and maximum number of coefficients in the wavelet sub- bands of the images from the keytagging test set . . . . .	148
4.9	Robustness-capacity test I for keytagging . . . . .	160
4.10	Robustness-capacity test II for keytagging . . . . .	161
4.11	Robustness-capacity test III for keytagging . . . . .	162
4.12	Robustness-capacity test IV for keytagging . . . . .	163
4.13	Specificity test for keytagging . . . . .	167
4.14	Robustness-capacity test for keytagging when combined with JPEG2000 compression . . . . .	168
4.15	Runtime cost of keytagging . . . . .	170
4.16	Recommended parameters to implement various keytagging-based security measures . . . . .	174

## List of Algorithms

1	Coding of biomedical tests as <i>CTUs</i> . . . . .	122
2	Decoding of <i>CTUs</i> to biomedical tests . . . . .	123
3	Keytag association . . . . .	152
4	Tag retrieval . . . . .	153
5	Auxiliary procedures used in keytag association and tag retrieval (I) . . . .	153
5	Auxiliary procedures used in keytag association and tag retrieval (II) . . . .	154





# Acronyms

- 3DES** Triple Data Encryption Standard
- 4G** Fourth Generation of mobile telecommunications technology
- ACM** Alert Communication Management profile (IHE)
- ACR** American College of Radiology
- ANSI** American National Standards Institute
- ASCII** American Standard Code for Information Interchange
- ATNA** Audit Trail and Node Authentication profile (IHE)
- BC** Bar Code
- BCH** Bose-Chaudhuri coding
- BIH** Beth Israel Hospital
- BLE** Bluetooth Low Energy
- BPPC** Basic Patient Privacy Consents profile (IHE)
- BT** Bluetooth
- CBC** Cipher Block Chaining
- CCITT** Consultative Committee on International Telegraph and Telephone
- CCM** Counter with CBC-MAC
- CCOW** Clinical Context Object Workgroup
- CD** Concentrator Device
- CDF** Cohen-Daubechies-Feauveau wavelet
- CDSS** Clinical Decision Support Systems
- CEN** European Committee for Standardization
- CIA** Confidentiality, Integrity and Availability
- CMS** Cryptographic Message Syntax
- CO<sub>2</sub>** blood Carbon diOxide saturation
- CoAP** Constrained Application Protocol
- COCIR** European Coordination Committee of the Radiological and Electromedical Industry
- CR** Compression Ratio
- CRC** Cyclic Redundancy Cycle
- CRL** Certificate Revocation List

**CS** Consultation System

**CT** Computed Tomography, Consistent Time profile (IHE)

**CTR** Counter

**CTU** Coded Test Unit

**DCT** Discrete Cosine Transform

**DEC** Device Enterprise Communication profile (IHE)

**DH** Diffie-Hellman

**DHCP** Dynamic Host Configuration Protocol

**DICOM** Digital Imaging and COmmunication in Medicine

**DIM** Domain Information Model

**DNS** Domain Name System

**DS** Digital Signature

**DSA** Digital Signature Algorithm

**DWT** Discrete Wavelet Transform

**ebXML** electronic business using eXtensible Markup Language

**EC** Embedding Capacity

**ECDH** Elliptic Curve Diffie-Hellman

**ECG** ElectroCardioGram

**EEG** ElectroEncephaloGram

**EHR** Electronic Health Record

**EUA** Enterprise User Authentication profile (IHE)

**EUI** Extended Unique Identifier

**FDA** U.S. Food and Drug Administration

**FP** Fingerprint

**FSM** Finite State Machine

**GDPR** European General Data Protection Regulation

**GUI** Graphical User Interface

**HDP** Health Device Profile

**HEVC** High Efficiency Video Coding

**HIPAA** Health Insurance Portability and Accountability Act

**HIS** Health Information System

**HL7** Health Level Seven

**HL7** Health Level 7

**HL7 aECG** Health Level Seven Annotated ECG

**HMAC** Hash-based Message Authentication Code

**HS** Host System

**HSUPA** High-Speed Uplink Packet Access

**HTTP** Hypertext Transfer Protocol

**ICT** Information and Communication Technologies, Irreversible Color Transform

**ID** Identifier

**IEEE** Institute of Electrical and Electronics Engineers

**IMAP** Internet Message Access Protocol

**INR** Internation Normalized Ratio

**IoT** Internet of Things

**IPsec** Internet Protocol security

**ISO** International Standards Organization

**IT** Information Technologies

**ITU-R** International Telegraph Union Radiocommunication standardization section

**IUA** Internet User Authorization profile (IHE)

**JIRA** Japan Industries Association of Radiological Systems

**JPEG** Joint Photographic Experts Group

**JPIP** JPEG2000 Interactive Protocol

**KT** Keytag

**LFSR** Linear Feedback Shift Register

**LIP** List of Insignificant Points

**LIS** List of Insignificant Sets

**LOPD** Ley Orgánica de Protección de Datos (Data Protection Act)

**LSB** Least Significant Bits

**LSP** List of Significant Points

**m-Health** mobile Health

**m-IoT** Internet of m-health Things

**MAC** Message Authentication Code

**MBR** Minimum Bounding Rectangle

**MCAP** Multi-Channel Adaptation Protocol

**MD** Message Digest, Medical Device

**MDER** Medical Device Encoding Rules

**MDS** Medical Device System

**MFER** Medical waveform description Format Encoding Rules

**MHD** Mobile access to Health Documents profile (IHE)

**MIT** Massachussetts Institute of Technology

**MOS** Mean Opinion Score

**MPEG** Moving Picture Experts Group

**MQTT** Message Queue Telemetry Transport

**MRI** Magnetic Resonance Image

**MSSIM** Mean Structural SIMilarity index

**NEMA** National Electric Manufacturers Association

**NFC** Near Field Communication

**NHD** Normalized Hamming Distance

**NiBP** Non-invasive Blood Pressure

**NIST** National Institute of Standards and Technology

**NTP** Network Time Protocol

**OASIS** Organization for the Advancement of Structured Information Standards

**OCSP** Online Certificate Status Protocol

**OOB** Out-of-Band (authentication)

**OS** Operating System

**OUI** Organizational Unique Identifier

**OUP** Originator Usage Period

**PACS** Pictures Archiving and Communications Systems

**PAN** Personal Area Network

**PAT** Private Access Table

**PBC** Push-Button Configuration

**PCD** Personal Care Device

**PDA** Personal Digital Assistant

**PET** Positron Emission Tomography

**PHD** Personal Health Device

**PHDC** Personal Healthcare Device Class

**PHI** Personal health information

**PHMR** HL7 Personal Healthcare Monitoring Report

**PHR** Personal Health Records

**PIN** Personal Identification Number

**PIPEDA** Personal Information Protection and Electronic Document Act

**PIX** Patient Identifier Cross Referencing profile (IHE)

**PM** Persistent Metric

**PRD** Percentage RMS Distortion

**PSNR** Peak Signal-to-Noise Ratio

**QF** Quality Factor

**QR-Code** Quick response code

**RBAC** Role-Based Access Control

**RC** Recovery Container

**RESTful** Representational State Transfer

**RFID** Radio Frequency IDentification

**RFID-T** RFID token

**RIPEMD** RACE Integrity Primitive Evaluation Message Digest

**RLE** Run Length Encoding

**RMS** Root Mean Square error

**RNG** Random Number Generator

**ROI** Region of Interest

**RONI** Region/s of Non-Interest

**RTM** Rosetta Terminology Mapping profile (IHE)

**SAML** Security Assertion Markup Language

**SC** Smart Card

**SCCN** Swartz Center for Computational Neuroscience

**SCP-ECG** Standard Communication Protocol for computer-assisted ElectroCardioGraphy

**SMTP** Simple Mail Transfer Protocol

**SNR** Signal-to-Noise Ratio

**SNTP** Simple Network Time Protocol

**SP** Service Provider

**SPIHT** Set Partitioning in Hierarchical Trees

**SPO2** blood oxygen saturation

**SSIM** Structural SIMilarity index

**SSL** Secure Sockets Layer

**SVD** Singular Value Decomposition

**Temp** body Temperature

**TLS** Transport Layer Security

**TPHS** Third-Party Host System

**US** United States, Ultrasounds

**USB** Universal Serial Bus

**VCO2** Carbon dioxide production

**VO2** Maximal oxygen consumption

**W3C** World Wide Web Consortium

**WCM** Waveform Communication Management profile (IHE)

**Wi-Fi** Wireless Fidelity

**WPA** Wi-Fi Protected Access

**WPS** Wi-Fi Protected Setup

**WT** Wavelet Transform

**WUSB** certified Wireless Universal Serial Bus

**X73PHD** ISO/IEEE 11073 Personal Health Devices

**XACML** eXtensible Access Control Markup Language

**XDS** Cross-enterprise Document Sharing profile (IHE)

**ZHCP** Zigbee Health Care Profile



*“You see, Momo, it’s like this. Sometimes, when you’ve a very long street ahead of you, you think how terribly long it is and feel sure you’ll never get it swept. And then you start to hurry. You work faster and faster and every time you look up there seems to be just as much left to sweep as before, and you try even harder, and you panic, and in the end you’re out of breath and have to stop—and still the street stretches away in front of you. That’s not the way to do it.*

*You must never think of the whole street at once, understand? You must only concentrate on the next step, the next breath, the next stroke of the broom, and the next, and the next. Nothing else.*

*That way you enjoy your work, which is important, because then you make a good job of it. And that’s how it ought to be.*

*And all at once, before you know it, you find you’ve swept the whole street clean, bit by bit. what’s more, you aren’t out of breath.”*

Michael Ende – *Momo*

# 1

## Introduction

### 1.1 The m-Health scenario and its security issues

The term e-Health (electronic health) began to spread by 1999 to describe what Prof. Eysenbach defines as [1] “An emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology.” This definition can also be portrayed as succinct as mathematical: “**e-Health = Medicine + Communication + Information + Society**”. This new medical paradigm supplements existing forms of care, create favorable circumstances for strengthening patient engagement [2] and yields clinical improvement [3, 4]. This progress is primarily based on the digitization of health records, biomedical measurements (e.g. blood pressure, glucose level, body temperature), signals (e.g. pulse-oximetry, electrocardiograms) and tests (e.g. coronary angiographies, echocardiograms, complemented with contextual data such as the conditions of acquisition, personal data of the patient and relevant parts of his/her clinical history) and the deployment of reliable protocols for its storage and transmission. On top of these pillars, novel ICT-based services, such as telemonitoring [5, 6], telediagnosis [7, 8],

teleassistance [9, 10] or e-Prescribing [11], foster an ubiquitous and pervasive access to the users of this medical information: physicians who interpret this information, clinicians caring for the patient, patients, researchers, medical teachers and students, etc.

The paradigm of e-Health evolved to **m-Health** (mobile health) [12, 13, 14] by 2004, to advocate for the integration of emerging **mobile communications, network and sensor technologies in healthcare systems and applications**. In addition to this, m-Health proposes shifting the healthcare model from a hospital-centered care to a user/patient-centered paradigm [15, 16], enabling the **empowerment of users** [17, 18, 19, 20] in the management of their health, the prevention of diseases, a better home-based healthcare delivery for elderly and chronic patients (e.g. providing personalized and dynamic treatments, connection with adequate medical systems) and important savings for healthcare systems due to the reduction of hospitalizations in number and duration. **Health and fitness monitoring, independent living and disease management** are some examples of innovative user/patient-centered mobile health applications [13], belonging to m-Health. These applications use personal health devices (e.g. weighting scales, blood pressure monitors, pulse-oximeters, medication monitors, fall detectors) and/or wearable sensors (e.g. for body temperature, electrocardiography, skin response, etc.) to gather biomedical measurements and signals of the user in different locations (e.g. at home, in hospital, in daily journey), which sometimes are accessed only by the user (to consult his/her health status) but often also by healthcare systems (e.g. to trigger alarms at abnormal values) and by some expert in charge of his/her follow-up. Certainly, these applications help to improve the health management of people, and the parallel spread of powerful mobile devices and networks foster their fast deployment [12]. In fact, the phrase 4G Health [21] encourages the progress of m-Health towards targeted personalized medical systems with adaptable functionalities and compatibility with 4G networks. Furthermore, the combination of Internet of Things (IoT) [22, 23] and m-Health has amalgamated the new concept of Internet of m-health Things (m-IoT) [24, 25, 26], intended for the development of a new, advanced generation of smart, always-connected applications that go beyond machine-to-machine communications.

Although the feasibility and usefulness of pioneer m-Health services has been thoroughly proved, their fixed structure sometimes leads to levels of engagement [27], motivation [28], or connections among their users [29] lower than required. These shortcomings have even resulted in the creation of groups of unsatisfied patients who decide to self-organize, out of the traditional healthcare system, for a higher empowerment and better management of their medical conditions, such is the case of the [Nightscouts](#). Experiences in the literature suggest that creating living networks of users and formal and informal caregivers by means of social media (e.g. social networks such as [Facebook](#) or [Twitter](#))



can alleviate these issues. It is worth noting that besides the predominantly ludic character of social media, new uses in different domains are being investigated and developed nowadays, driven by the attracting features of social media and their remarkable mass of users. A variety of projects using social media in m-Health environments have already been reported [30], for instance including scenarios such as dementia [31], tobacco addiction [32], influenza [33] or control of dietary behavior [34]. Up to 140 health use cases for Twitter are compiled in [35]. Indeed, there are sound reasons to **integrate social media with m-Health**, since the former provides a wide variety of tools [36] — e.g. social networking sites, content communities, collaborative projects, etc. — that enable users to build communities around them — e.g. including other users, formal and informal caregivers — where they can create, share and exchange information — e.g. their biomedical data — in different formats — e.g. plain text, pictures, videos, etc. Therefore, the development of social-media-based m-Health services has the potential to **promote the recruitment and reinforce the engagement of users and their communities**. Considering all above, a fair first approximation to an integrative system was conducted by [37], who implemented a pervasive health system that integrated patient monitoring and social sharing via Twitter.

Many m-Health applications demand high availability of biomedical information to operate. As regards to security, this requirement increases the potential surfaces for cyber-attacks [38] and conflicts with the **rising awareness of users, patients and governments about the sensitive character of this information** [39, 40]. In fact, privacy and security are commonly included among the most important barriers for the success of m-Health [41]. These concerns are fully justified since biomedical information usually attach personal data that permits the identification of the user/patient it belongs to. To shed light on how critic security has become in m-Health, according to [Ponemon Institute](#) — a privacy research firm— 90% of healthcare institutions said their organizations have been victims of one or two data breaches in the last two years, being cyber-attacks the number one cause – followed by employee negligence and lost or stolen devices. **Cyber criminals are increasingly targeting and exploiting healthcare data** — there has been a 125% growth in these attacks over the last five years — because they recognize two critical facts about the healthcare industry: 1) healthcare organizations manage a treasure trove of financially lucrative personal information and 2) they usually do not have the resources to adequately protect these data (e.g. means to prevent attacks) due to an inadequate budget [42]. This situation makes healthcare institutions potentially face high liability costs, including reduction of the turnover of costumers due to damage in reputation, class action lawsuits and costly downtime. It is estimated in [43] that the average global cost of data breach per lost or stolen health record is 363 dollars and that 24.5% of the times it involves more than 10,000 records. As regards to users/patients,

the undue disclosure (e.g. caused by eavesdropping, malicious leaking or revelation) of their biomedical information can cause them social, professional and economical damage (embarrassment, the loss of his/her job or the rise of his/her health insurance policy) [44]. In addition to this, the undue manipulation (tampering, forgery) of this information can cause misdiagnosis and poor treatments, which may endanger the health and life of the patient; and also produce erroneous medical research outcomes, which may adversely affect the patients under consideration. Nonetheless, the primary aim of cyber criminals is economical, so this set of threats are mainly oriented towards extortion. In addition to this, breaches of personal health information [45, 46] fuel financial identity theft, medical fraud and medical identity theft. The first refers to using certain leaked patient information (e.g. his/her social security number and other identity information) to apply for fraudulent loans, charge purchases to credit cards or take-over bank accounts; the second usually involves billing payers for treatments never rendered and the third, a intersection of the previous ones, involves a medical identity (patient identification, insurance information, medical histories, prescriptions, test results) that may be used to fraudulently obtain medical services or the prescription of drugs [47]. Beyond the financial losses, such theft modality implies that relevant information of the patient affected (e.g. his/her blood type) may be changed or mixed with that of a usurper, with a direct impact in his/her care quality and in the obtaining of further medical, life, or disability insurance.

To minimize risks, an adequate protection policy against the aforementioned threats shall be implemented. The protection of users' confidentiality and safety in the m-Health context is addressed by the **Health IT directives** of major regulations such as the Health Insurance Portability and Accountability Act [48] (HIPAA, enacted in United States), the Personal Information Protection and Electronic Documents Act [49] (PIPEDA, enacted in Canada), the European General Data Protection Regulation [50] (GDPR, enacted in Europe) or the Personal Data Protection Act [51] (LOPD, enacted in Spain); and also in communications from major healthcare agencies, such as the FDA safety communication regarding cybersecurity for medical devices and hospital networks [52]. The most common objectives of these regulations are (a) guaranteeing information security, which include requirements to guarantee major security goals [53], including **confidentiality, integrity, availability, accountability, auditability, authenticity, non-repudiation** and **privacy** in the management of biomedical information, mainly by the implementation of security frameworks integrating cryptographic tools and security profiles, data backups and audit records; (b) **patient control over their biomedical data**, based on an adequate management and enforcement of his/her informed consent and on guaranteeing high transparency towards him/her — i.e. not only does the system say that all is safe and good, but the user also gets an idea about where and how his/her data are being consulted; (c) closing the gap between medical device manufacturers and hospital facilities to mini-

mize cybersecurity vulnerabilities (e.g. avoiding hard-coded passwords, providing security updates regularly); (d) prevention and reaction to data breaches, by means of mandatory, periodic risk assessments and audits conducted by experts, and (e) responsibility and substantial sanctions to those that do not thoroughly address the aforementioned measures.

## 1.2 The m-Health architecture

As explained in Section 1.1, a generic m-Health architecture shall facilitate the implementation of m-Health applications, usually grouped in three major (and interrelated) fields: Health and Fitness, Independent Living and Disease Management. Such applications demand a reliable and efficient acquisition of personal biomedical information (e.g. biomedical measurements, signals and/or tests); its adequate storage (which may include a previous or subsequent processing) and a pervasive, ubiquitous and controlled access to the users that need to consult this information (e.g. the patient and his/her formal caregivers). As discussed in [54], the information that is gathered in these applications has the potential to enable three essential feedback loops for improving health outcomes: regarding patient's self care (e.g. how does a certain treatment impacts my health measurements?), clinician-directed summary data to assist decision-making (e.g. how do the side effects and therapeutic benefits of a certain treatment balance out for my patient?) and research evidence (of the treatment tested) to enhance clinical care for groups of patients with similar conditions (populations). Therefore, these information loops may be used to promote health literacy and empowerment among patients (and regular users) and also to feed health researchers with fresh and abundant data sources. To summarize, it can be concluded that the m-Health architecture shall promote the participation of a) users/patients, b) formal and informal caregivers (e.g. physicians who interpret the tests, clinicians caring for the patient, nurses, social workers, relatives) and c) researches, medical teachers and students.

A generic end-to-end m-Health architecture [12, 55] is illustrated in Figure 1.1. At a technical level, the most basic architecture is comprised by two elements, a Personal Health Device or sensor (PHD) that collects and sends the user's/patient's biomedical information and a Host System (HS) that stores the collected information — for example a Hospital Information System (HIS) or a Personal Health Record (PHR). However, since there are usually several PHDs in the personal area network (around the patient/user), and they seldom have the connectivity to reach the HS, most m-Health architectures include a third element, namely the Concentrator Device (CD), a mobile device (e.g. cell phone, PDA, tablet) which gathers the information from the different PHDs and forwards it to the HS.

Furthermore, depending on the intended m-Health application, various other elements can be incorporated into the end-to-end architecture. For example, Service Providers (SP) and medical systems — e.g. alarm systems, Electronic Health Records (EHR), Clinical Decision Support Systems (CDSS), respectively placed before and after the HS, which would perform operations of management, monitoring, processing or follow-up of the patient’s biomedical information. Finally, other elements can connect with the HS to either share medical information, such as Third-Party Host Systems (TPHS), or access that information, such as a Consultation Systems (CS) interfacing the user and the authorized caregivers and researchers with the HS.

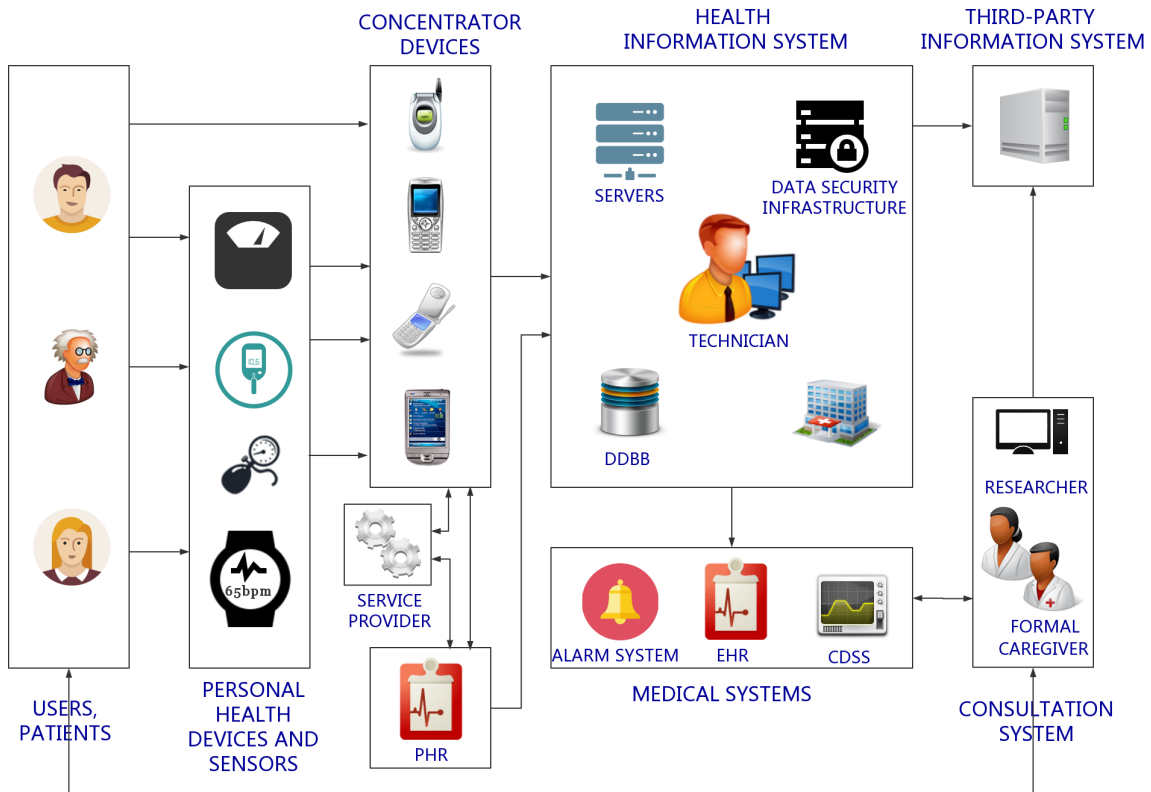


Figure 1.1: Generic m-Health architecture.

Although the initial blueprint of the m-Health architecture has remained valid, the list of devices and platforms which can act as PHDs, CDs and HS has evolved within the last years. As regards to PHDs [56], the initial offer of generic medical devices (e.g. thermometers, pulse oximeters, blood pressure monitors, glucose meters, ECG sensors) and devices to support independent aging (e.g. medication monitors) has been enlarged with more specific devices (e.g. urine analysis, insulin pumps, sleep apnoea monitors, fall detectors, gas detectors) and also with new devices for the promotion of wellness and fitness (e.g. pulsometers, strength monitors, smartbands, etc.). Furthermore, these devices will progressively become wearable [57, 58] to enable unobtrusive sensing [59],

e.g. by means of smart textile technology and flexible-stretchable-printable electronics. Nonetheless, the most important evolution is yet to come with the development and merchandising of Internet-ready PHDs, which will release the potential of m-IoT architectures [25, 60, 26]. With respect to legacy HS, typically hosted in dedicated servers at healthcare facilities, they are being steadily migrated to cloud-based solutions [61, 62] (e.g. based on [Amazon Web Services](#), [Windows Azure](#) or [Joyent](#)), which offer an outsourced, reliable, economic and scalable hosting of data and operational apps. According to the 2014 Healthcare Information and Management Systems (HIMSS) Analytics Cloud Survey [63], 83% of IT executives claim to be using cloud services, pointing out Software-as-a-Service (SaaS)-based applications as being the most popular (66.9%). These survey states that IT executives perceived noticeable benefits after this migration, such as the augment of technological capabilities, the positive contribution to financial metrics and the reduction of time to deploy solutions. Finally, the shifting of PHDs (towards wearable and internet-ready connected) and HS (to cloud-based solutions) will also affect CDs: their function as relay devices may lose importance in future years, but they will still be relevant as monitoring and consultation devices [64]. Furthermore, the initial list of CDs is being enlarged with new smart devices, such as TVs [65], watches [66] and glasses [67]; which will permit the flourishing of health apps with augmented reality [68] and smart services [69].

### 1.2.1 Biomedical data flows and interoperability

Interoperability is both a prerequisite and an enabler for versatile, integrated, efficient and useful communication between PHDs and HS in the context of thorough and high quality m-Health services [70, 71]. Standardization of these biomedical data flows — involving signals, periodic measurements, medical histories and/or contextual information, often grouped in biomedical tests — is a crucial factor in achieving high interoperability levels [72] (see Figure 1.2.1), in order to increase the safety to patients, the efficiency in the use of healthcare resources and the development of medical knowledge [73]. Several standards, protocols and integration initiatives promoting the deployment of end-to-end standard-based interoperable m-Health services furnish today's panorama, including standards for medical device interoperability (i.e. PHD-CD interface), standards for the interoperable exchange of EHRs (i.e. HS-TPHS interface) and integration initiatives for the coordinated use of these standards (i.e. CD-HS, HS-medical systems, PHD-HS interfaces interfaces).

Regarding medical devices interoperability (PHD-CD interface), the foremost solution to ensure the syntactic and (to some extent) semantic interoperability among personal health devices is addressed within the ISO/IEEE 11073 (X73PHD) family of standards [74], initially driven by the Institute of Electrical and Electronics Engineers IEEE and

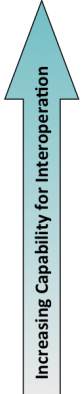
		Definition		Example	 Increasing Capability for Interoperation
Interoperable	Level 5	<b>Dynamic</b>	Dynamic Context understood	Resource and Load Management	
	Level 4	<b>Pragmatic</b>	Context understood	IHE PCD / Continua Use Case based Profiles...	
Integratable	Level 3	<b>Semantic</b>	Meaning understood	Snomed, IHE-PCD RTM, IEEE 11073-10101, LOINC...	
	Level 2	<b>Syntactic</b>	Common Format	HL7, IEEE 11073, Continua...	
Interfaceable	Level 1	<b>Technical</b>	Common Physical and Transport Layers	RS232, Ethernet, 802.11, Zigbee, BT, USB, TCP/IP...	
	Level 0	<b>None</b>	Stand-alone	Stand-alone	

Figure 1.2: Turnita's interoperability model.

then adopted by the European Committee for Standardization CEN and the International Standards Organization ISO. They define the landscape of transport-independent m-Health applications and information profiles, which specify data exchange, data representation, and terminology for communication between personal health devices and aggregators. In second place, there are several protocols [75] for the storage and exchange of waveforms, mainly focused on electrocardiograms (ECGs). The most widespread being the Standard Communications Protocol for computer assisted ElectroCardioGraphy (SCP [76], ISO/IEEE 11073-91064:200 standard), the Health Level Seven (HL7 aECG [77], American standard ANSI), the Medical waveform Format Encoding Rules (MFER [78], Japanese standard partially approved by ISO) and the Digital Imaging and Communication in Medicine (DICOM Supplement 30 [79], American standard NEMA). They specialize in different use cases (diagnostic examinations, home care, emergency care, etc.) and use different storage formats (binary encoded, XML-based [80]). In third place, there are simple non-standard protocols designed for open-source platforms, e.g. based on Arduino [81] or Raspberry Pi [82], which can gather biomedical measurements and signals from a variety of inexpensive sensors.

For the exchange of biomedical information between healthcare entities (intra-HS, HS-medical systems, HS-TPHS interfaces), there are four major alternatives. First, the ISO/EN13606 standard [83], driven by CEN and ISO/IEEE, is able to represent the information included in an EHR in order to achieve the interoperable exchange of EHRs between HS in a semantic interoperable way. Second, Health Level 7 (HL7) [77], founded by American vendors of medical devices and recognized by the American National Standards Institute (ANSI), is an international standard for medical messaging. Its name refers to the fact that it specifies a uniform syntax in the seventh level of the protocol stack. This standard enables information representation in a simple structure of segments,

data types' flags, and mapped fields. It is worth highlighting that HL7 works well as a supplement for the Digital Imaging and COmunication in Medicine (DICOM) [79] standard, used by most Picture Archiving and Communications Systems (PACS) for handling, storing, printing, and transmitting information in medical imaging. Third, openEHR [84] is a proposal related with HL7, but based on an open standard specification, which describes the management and storage, retrieval and exchange of data in EHRs. The key feature of openEHR is that all a person's health data is stored in a "one lifetime", vendor-independent, person-centered EHR. Last, Personal Health Records (PHRs) are tools whose popularity is growing steadily. PHR systems have been defined [85] as patient/user-centric, longitudinal collections of PHRs administrated primarily by patients/users [86] with interfaces to EHR systems and with capabilities to exchange health-related data between other PHR systems and EHR systems. As the PHR system may be standalone software for PC or mobile platforms, the capacity to store PHRs locally is not excluded. One relevant distinction between PHRs and EHRs is that the former presents the information to the person with a vocabulary that he/she can understand. Among other options, Apple enables PHRs through its HealthKit [87] and Microsoft does by means of HealthVault [88].

Several other initiatives, such as Integrating the Healthcare Enterprise (IHE) or the Continua Health Alliance, have been promoted by various healthcare professionals and technology companies to encourage the coordinated use of the aforementioned standards in m-Health architectures (CD-HS, HS-medical systems, PHD-HS interfaces). These two entities focus mainly on different (albeit related) environments. Integrating the Healthcare Enterprise (IHE) [89] is an organization made up of worldwide manufacturers whose main objective, rather than develop new standards, is to identify specific clinical needs and develop technical guidelines (IHE profiles and technical frameworks) that coordinate the use of well established standards (such as HL7 and DICOM) to address these needs. For instance, IHE defines a profile, the Rosetta Terminology Mapping (RTM), which enables the interpretation of X73PHD terminology—and thus, measurements acquired by X73PHD-compliant devices—in IHE systems, such as PHRs, EHRs, alarm systems or CDSS. It can be said that IHE profiles, like RTM, foster a model for pragmatic interoperability within end-to-end m-Health frameworks. Continua Health Alliance [90], on the other hand, is an open non-profit alliance of several industry-leading technology and health companies whose role is to establish a system of interoperable personal connected health solutions with the knowledge that extending those solutions into the home fosters independence, empowers individuals and provides the opportunity for truly personalized health and wellness management. Continua tends to focus on people, and therefore covers the m-Health domains: fitness monitoring, aging independently and managing chronic disease. Their main goal is to leverage existing standards and to close recognized interoperability gaps by means of their Continua Design Guidelines. Among other standards,



Continua endorses the X73PHD standard for medical device interoperability. Apart from technical aspects, a further objective of the alliance is to establish a certification program with a consumer-recognizable logo for the devices.

### 1.2.2 Biomedical tests coding

The core of biomedical tests (e.g. a stress test) are biomedical signals (e.g. an ECG), whose clinical meaning often needs to be complemented with periodic measurements (e.g. body temperature, heart rate, maximal oxygen consumption, carbon dioxide production, speed of the treadmill), medical history and/or contextual information (annotations about the signal, health status of the patient, his/her allergies, medication, etc.). They have a high intrinsic value as enablers of m-Health applications, e.g. for early diagnosis, continuous follow-up and customized care of patients; and, as explained in Section 1.2.1, their exchange by means of well-established standards helps to achieve great interoperability levels. Nonetheless, frameworks with critical energy constraints, such is the case of Body Area Networks (BAN [91]), may not get along with the energy consumption caused by the implementation of standards for the exchange of biomedical information. Their verbosity translates into the demand of extra transmission bandwidth, which causes most of the energy expenditure [92]. As a promising alternative, those frameworks may rather implement a simple biomedical tests coding providing adequate data availability, i.e. comprising secure and efficient storage, exchange and access, to fit the m-Health paradigm. The requirements that such coding shall fulfill may be summarized as:

- **Information associated to the biomedical signal.** Without appropriate data, identifying the signal and enabling its interpretation, biomedical tests may become useless. Therefore, the information in biomedical tests must be arranged as metadata using some data structure and bound to the signal to difficult its lost.
- **Signal compression.** Algorithms for signal compression remove redundancies contained by signals at different levels. These algorithms can be divided into two main categories: lossless, which retrieve the original signal; and lossy, which reach higher compression ratios than lossless at the cost of decreasing signal fidelity. The latter are more interesting since they permit saving much more bandwidth in transmission and space in storage. Nevertheless, in clinical applications the compression ratio must be limited by measurable quality parameters to hold the clinical meaning of the signal and avoid changing its diagnostic interpretation. Among lossy methods, there are three modalities [93]: direct methods (basing their detection of redundancies on direct analysis of the actual signal samples), transformation methods (mainly utilizing spectral and energy distribution analysis for detecting redundancies) and



parameter extraction techniques (e.g. measurement of the probability distribution, subsequently utilized for classification based on *a priori* knowledge of the signal features). The second modality (e.g. discrete cosine transform [94], Karhunen-Loève transform [95], wavelets [96], etc.) generally yields better results, especially the wavelets, which provide a time-frequency representation of the signal with varying resolution for fine description in both domains. Furthermore, the wavelet coefficients can also be compressed by exploiting their similarity, as the SPIHT algorithm does [97], in order to increase the final compression ratio.

- **Security and privacy** in storage and during transmission. As explained in Section 1.1, current legal regulations (the HIPAA [48], the PIPEDA [49], the LOPD [51], the Digital Signature Laws in several countries) demand that any personal health information must be protected, using adequate cryptographic means. The basic requirements are (1) encrypting all private data, (2) embedding a digital signature to verify data integrity and authenticate the signatory, and (3) encrypting the communications. When dealing with biomedical signals, researching on partial encryption schemes [98, 99, 100] may be an interesting manner to reduce operations while maintaining fair privacy levels. In addition to this, steganography [101, 102, 103] may be used as a complement to introduce security or secret elements silently. Watermarking [104], marking all objects in the same way (e.g. to demonstrate ownership) and fingerprinting [105], marking each object specifically (e.g. to identify legitimate *users*) are the most typical applications of steganography.
- **Role-Based Access Control.** M-Health services operate in scenarios with a variety of different stakeholders: patients, relatives, paramedics, nurses, primary care doctors/general practitioners, surgeons, medical specialists and subspecialists, teachers and medical students, researchers, laboratories, insurance companies, governmental oversight agencies, and non-governmental oversight. For the same patient, the information that each user is allowed to access must depend on his role: e.g. if the patient has AIDS, the nurses and the paramedics need to know, but probably not the researchers using his/her medical tests. Attribute-level encryption and de-identification are effective ways to overcome this issue.
- **Low complexity encoding and short access time.** Since the current tendency is building portable medical devices and wearable sensors, which often mount low power processors, the algorithms for encoding and protection should be as simple as possible to not overload them with complex calculations and reduce demand on the battery. Besides, fast execution and transmission are requirements to maintain availability of the test at good levels and allow real-time services.

There are many publications approaching these requisites separately, for example [106, 107, 108] for signal compression, [109, 110] for data embedding into signals and [111, 112, 113, 114, 115] for signal security). Furthermore, there are also proposals to integrate together signal compression and encryption [116, 117, 118, 119, 120], compression and embedding [121, 122, 123, 124, 125]; encryption and embedding [126, 127, 128, 129, 130, 131, 132, 133]. Nonetheless, the definition of a coding harmonizing compression, embedding and encryption, while guaranteeing signal quality, role-based access control, low complexity and short access times is still an open issue.

## 1.3 Security trends in m-Health and what can be improved

### 1.3.1 Security in protocols for the exchange of biomedical information

The standardization of security measures has already been promoted by organizations such as **IHE**, joint committees such as JIRA/NEMA/COCIR and by major standard protocols such as **DICOM**, which dedicates its Working Group 14 to this issue, and **HL7**, which has a Security Working Group. As illustrated in Table 1.1, IHE has issued several profiles to address a variety of security and privacy aspects: Audit Trail and Node Authentication [134] to implement auditability and accountability policies, Consistent Time [135], Healthcare Provider Directory (HPD), Document Digital Signature [136], Document Encryption [137], Secure Retrieve [138], Access Control white paper [139], Basic Patient Privacy Consents [140] to enforce privacy policies, Cross-Enterprise User Assertion [141], Internet User Authorization [142], Enterprise User Authentication [143]). DICOM addresses security in its part 15 [144] and through many supplements [145] — 31 (security enhancements), 41 (security enhancements 2 - Digital Signatures), 51 (Media Security), 55 (Attribute Level Confidentiality), 86 (Digital Signatures for Structured Reports), 95 (Audit Trail Messages), 142 (Clinical Trial De-identification Profiles)) cover security based on different secure profiles regarding: use, transport, digital signature and media storage (among others). HL7 has also published several documents about security, notably its Role-based Access Control Healthcare Permission Catalog [146], its Security and Privacy Ontology [147] or its Healthcare Privacy and Security Classification System [148].

The security measures depicted in IHE (Section 2.1.1) and implemented by DICOM (Section 2.1.4) and HL7 rely on standardized cryptographic resources. Essentially on encryption, which may be symmetric or asymmetric; and on hashing, which is found in digital signatures and message authentication codes. The former is used to implement access control policies (enforcing privacy, e.g. by means of Cryptographic Message Syntax, CMS [151]) while the latter is intended for binary integrity control (tampered/non-tampered),

Table 1.1: Selected IHE profiles, mapped to security and privacy controls

Security & privacy controls IHE profiles	Audit log	Identification & authentication	Data access control	Secrecy	Data integrity	Non-repudiation	Patient privacy
Consistent Time [135] (2003)	✓	-					
Enterprise User Authentication [143] (2003)		✓	-			-	-
Audit Trails and Node Authentication [134] (2004)	✓	✓	✓	✓	✓	✓	✓
Personnel White Pages [149] (2004)		✓	✓			-	
Document Digital Signature [136] (2005)		✓			✓	✓	
Cross-Enterprise User Assertion [141] (2006)		✓	-			-	-
Basic Patient Privacy Consents [140] (2006)			-				✓
Access Control White Pages [139] (2009)		✓	✓	✓			
Healthcare Provider Directory [150] (2010)		✓	-			-	
Document Encryption [137] (2011)			✓	✓	-		
Internet User Authorization [142] (2015)		✓	✓				
Secure Retrieve [138] (2015)		✓	✓				

authentication and non-repudiation. The main issue in this cryptography-based policies is the difficulty to develop cooperative architectures where different users may edit the biomedical test, e.g. by adding annotations or applying filters for better visualization and diagnosis, while maintaining the validity of the security measures implemented. Any change in the biomedical test invalidates all the previous signatures, and even though new signature may be added, the traceability from the origin will be weakened or lost. An alternative is that each user adds his/her changes to the original test, digitally signs it and delivers the signed updated test to the rest of the users. In this way, the rest of the users can access and/or store the updated test with security, and add new updates from the last test version by following the same procedure. Nonetheless, as the number of users and updates of the test grows, this approach becomes quite impractical in terms of delays, bandwidth and storage. Another limitation, inherent to cryptographic-based approaches, is that the biomedical test (e.g. an image) becomes totally unprotected when extracted from its standard file (e.g. a DICOM file).

To date, there are also several protocols that give little consideration to security and privacy issues. **X73PHD** basically **delegates** this task **on the implementation of a secure transport layer** (e.g. Zigbee Health Care Profile or Bluetooth Health Device Profile [152]), which can only authenticate and encrypt the frames exchanged by the personal health devices and the aggregators. No means are provided to authenticate the users

and the legitimacy of personal health devices and aggregators, to attach digital signatures on the measurements/signals acquired or to encrypt the measurements/signals that need to be stored in the personal health devices when the connection with the aggregator is broken. Similarly, in the case of **SCP-ECG** the **lack** of security specifications extends from its transmission protocol to its storage policy, neither of them including **any sort of protection**. Regarding the MFER standard, it does not directly address security, but neither does it include patient data except by means of HL7. Thus, it can thus benefit from HL7 security policies/recommendations. Lastly, **the protocols associated to open-source platforms** are very simple and its security usually **rely on** implementing a **secure transport layer and on not including any identification of the user**, which on the other hand limits its integration with medical systems (e.g. personal and electronic health records).

Regarding protocols associated to open-source platforms, they need to implement security to facilitate compliance with m-Health applications, be able to operate in real-time and also optimize its bandwidth (e.g. by coding measurements and signals), since low-power sensors spend most of their energy in transmission [153].

### 1.3.2 Signal-based protection

The security measures implemented by the aforementioned protocols are strictly based on the application of different cryptographic elements to the biomedical files and/or to the communications between entities. Nonetheless, the addition of signal-based protection techniques, relying on the basis of steganography, has the potential to rise the security and privacy levels of the m-Health architecture. Two related alternatives can be highlighted: generic steganography (also known as embedding or data hiding techniques), which permits including significant amounts of data within biomedical — cover — signals, which silently become stego-signals; and watermarking, an evolution or particular case of steganography which permits binding limited amounts of data to the signals with adjustable strength to implement different security applications — it was originally intended for copyright protection. Table 1.2 summarizes and compares the defining features of steganography, watermarking and encryption.

#### Steganography/embedding/data hiding

In the m-Health context, **data embedding techniques** [154, 155, 156, 157] **aim at introducing** significant amounts of **relevant data and/or security elements into** — cover — **biomedical signals in an imperceptible, secure and efficient manner**. Although in traditional steganography the cover object and the secret data have

no relation, it is usual in biomedical embedding that cover biomedical signals — 1-D signals (e.g. ECGs, EEGs), images and/or videos — are related with the embedded contents, which may be patient information, codes to enable fast indexing, hashes and digital signatures for integrity control, digital envelopes including protected information, other biomedical signals, QR codes for authentication or linking to valuable data, etc — see [158, 159, 160, 161, 162] It is worth noting that the larger the cover biomedical signal, the higher the payload capacity — i.e. biomedical videos (e.g. echocardiograms) can host much more secret data than 1-D signals (e.g. ECGs) of the same duration.

Table 1.2: Comparison of steganography, watermarking and encryption in the m-Health context, based on [154]

Criterion/ method	Steganography	Watermarking	Encryption
Carrier	Any digital media	Mostly biomedical images, also 1-D signals and videos	Usually text based, with some extensions to digital media
Secret data	Biomedical payload	Watermark content (when private)	Biomedical plain text/media
Key	Recommended	Optional	Necessary
Input elements	At least two, unless in self-embedding	At least two	Usually one
Detection	Blind	Usually informative (i.e. original cover or watermark is needed for recovery)	Blind
Authentication	Full retrieval of data	Usually achieved by cross correlation	Full retrieval of data
Main applications	Secret captioning or communications	Authentication, integrity control, captioning	Data protection
Result	Stego-file	Watermarked-file	Cipher-text
Main concerns	Distortion, detectability and capacity	Distortion, robustness and detectability	Robustness
Main attacks	Steganalysis	Image processing and collusion	Cryptanalysis
Visibility	Never	Not usually	Always
Confidentiality	Always	Sometimes	Always
Fails when	Detected	Removed/replaced and detected when confidential	Decrypted
Relation to cover	Not necessarily related to the cover. The secret data is usually more important.	Usually becomes an attribute of the cover, which is more important than the data.	N/A
Flexibility	Free to choose any suitable cover	Cover choice is restricted	N/A

Regarding embedding methods, several possibilities are available. There are — usually simple — approaches working in the temporal or spatial domain; methods working in transform domains, which take advantage of the frequency decomposition (which is associated to different energy levels) of the image to perform a more transparent and less detectable embedding; and even proposals to hide information in compressed domains to harmonize embedding and compression. In addition to this, a series of approaches work with histograms since certain modification (e.g. controlled shifting) can achieve reversibility. Furthermore, there are techniques based on spread-spectrum principles that permit spreading the secret payload throughout the cover signal. This preserves the statistical properties of the image, which results in good stego signal quality, capacity and security. Similarly, model-based steganography (also known as adaptive steganography and statistics aware steganography) pursues embedding the secret payload without altering the statistical properties of the cover.

Although the biomedical embedding of a secret payload in biomedical signals with any of the techniques above will certainly imply some degree of distortion — reversible techniques can remove the distortion only after extracting the embedded content —, **the top priority is that its clinical value is not affected**. Even if the clinical quality of the signal can be guaranteed in a simple manner, still the application of embedding in the m-Health context presents two noticeable drawbacks. First, these techniques are not specifically designed to endure modifications on the hosting signal, so any person not aware of the embedded data may perform some processing on the signal (e.g. the application of filters) causing the partial or total removal of the data. Second, the integration of embedding in standardized biomedical files is controversial since the standardization requires the thorough and public definition of the elements to be embedded, while the purpose of any steganographic technique is to hide these contents as much as possible.

### Watermarking

General watermarking methods may be applicable to different types of signals, but in the m-Health context watermarking is mainly focused on biomedical images. Nonetheless, the underlying principles of image watermarking techniques can be adapted to 1-D signals, videos, etc. **Medical Image Watermarking** [163, 164] (MIW) techniques enable the embedding of limited amounts of hidden data (e.g. biomedical information, security elements), one or several watermarks, within biomedical images by means of certain image processing and random keys. One of its main differences with respect to data embedding techniques is that **the image can be manipulated** (e.g. annotated, compressed with JPEG2000 [165], adjusted with different contrast and brightness) by the users **without interference in its security** — regardless if the user performing the image modifica-

tions knows about the existence of the watermarks — and that the former enables a good variety of complementary security measures [166, 164, 167]:

- Role-based access control (RBAC), so that each authorized user can read and/or edit certain contents of the image-based test according to his/her professional role, e.g. physician, researcher, teacher, etc.
- Integrity control, to detect if the image has been tampered with, which would endanger its clinical value.
- Tamper location, pinpointing the areas where the image has been manipulated, which may be helpful to validate images that are modified in permissible areas.
- Authentication, assessing if the image received corresponds to the image originally acquired, to an image derived from the original or to an unrelated image.
- Private captioning, associating private information with the image, only retrievable by authorized users of the authenticated image.
- Traceability control for user accountability, by associating marks from each entity that processes the image.
- Copyright protection, to pursue illegal copies if the image has a commercial use.

As illustrated in Figure 1.3, the random keys generated for watermarking are symmetrically required to retrieve the embedded data. Regarding the watermarks, there are **different types** and they may be combined to implement a security policy. **Robust** watermarks [168], whose content is retrievable even if the image has undergone heavy modifications, may be used for authentication, traceability and copyright protection. **Semifragile** watermarks [169], whose content is retrievable only if those modifications are mild (e.g. if the image preserves its clinical value), may be used for private captioning — although sometimes are also proposed for integrity control. Moreover, several semifragile watermarks, intended for different users, may be embedded in the same image in order to implement role-based control. Finally, **fragile** watermarks [170], whose content is retrievable only if the image is intact, may be used to implement integrity control and location of tampered areas in the image — although sometimes are also proposed for captioning and authentication. It is worth highlighting that MIW techniques are required to produce a minimum distortion on the image to preserve its clinical value. In fact, they are often grouped in **four categories depending** on the manner how they cope with this requirement of high transparency.



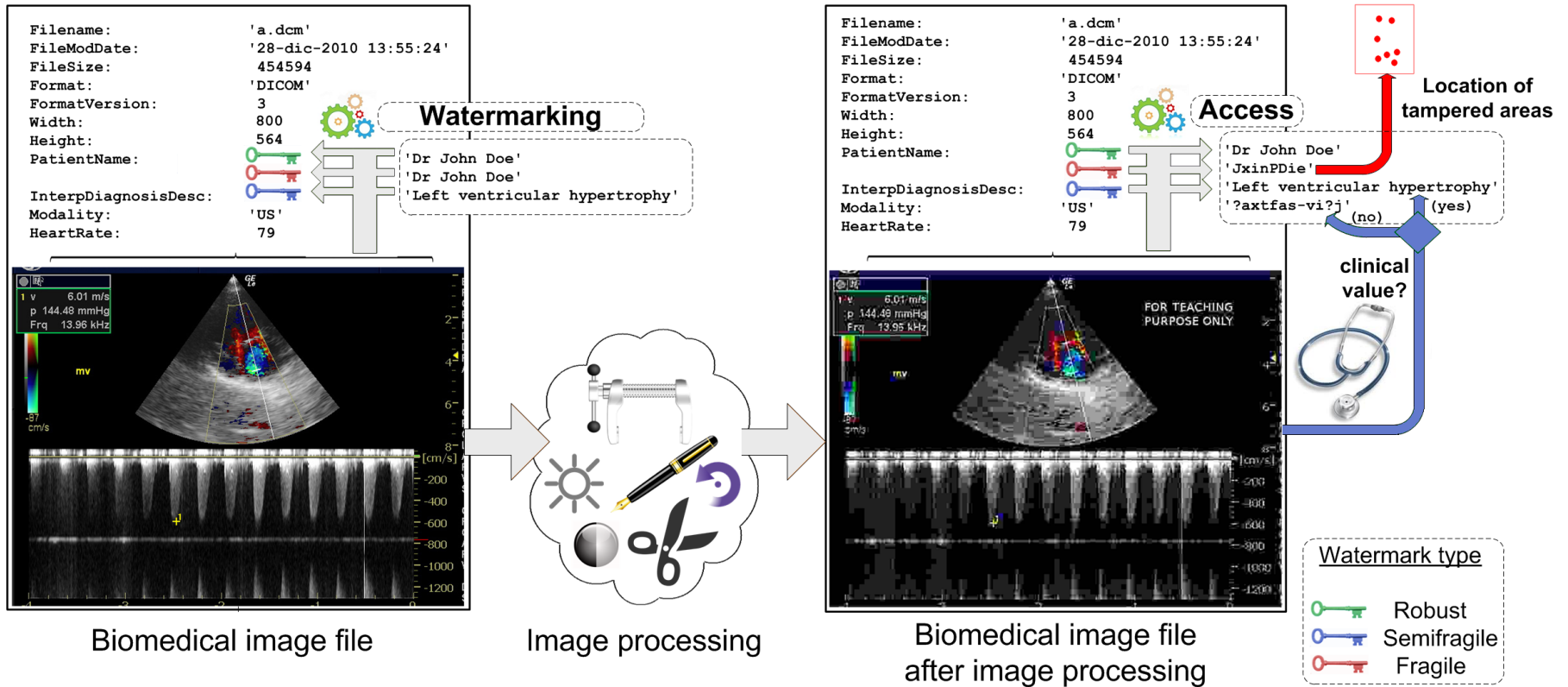


Figure 1.3: Example of enhancement of the security of biomedical image tests through watermarking.



The first group are the **non-reversible techniques** [171], which **produce a permanent distortion** on the image because they perform non-invertible operations (e.g. bit quantization, replacement or truncation). As a consequence, a thorough clinical assessment is necessary to guarantee that the clinical value of the watermarked images is preserved. The second group of MIW techniques [172] corresponds to **those that embed mainly in regions of non-interest (RONI)** of the image. This minimizes the interference of the watermarks with the clinical content and avoids the need of clinical assessment. However, the **security** of these techniques **against eavesdropping and forgery is low**, since the modified pixels/coefficients where the watermarks were embedded are easy to identify in the *RONI*, which is usually black. Moreover, the *RONI* may be used to insert visible watermarks or removed if medical image compression [173] is applied. In both cases the watermark(s) would be partially or totally removed. The third group are the reversible techniques, which distort the image but can recover its original quality by fully removing the watermarks after they have been detected and validated. This new concept of watermarking was first introduced in [174] and it has undergone relevant improvements. Nevertheless, any **reversible technique** has two important drawbacks. First, it **requires a secure environment** since the image is unprotected once the watermarks are removed. Second, a user not allowed to access certain watermarks will neither be able to remove them, so he/she will work with a lower-quality version of the image. Finally, the fourth group are the **zero-watermarking/non-watermarking techniques** [175], which bypass the image distortion introduced by the rest of watermarking techniques by avoiding the embedding step. Instead, they **propose associating the watermarks to certain features extracted from the image** (or from a transformed version). Although these last techniques seem promising for the m-Health context, few works have been proposed and they show certain shortcomings. First, most existing proposals do not include a thorough risk assessment, which is the most basic feature of a security technique. Second, most proposals focus on implementing only one or two security applications (e.g. image authentication, private captioning, copyright protection). Third, the watermark coding process is based on an XOR operation of certain image features with the contents to be associated, which does not guarantee an optimum robustness-capacity tradeoff — this is important when a variety of simultaneous security applications are to be implemented. Fourth, most proposals do not include a complexity analysis demonstrating their simplicity and scalability. Fifth, most proposals do not integrate appropriate cryptographic elements for the protection of the watermarks.

In general terms, several disadvantages hinder the integration of watermark-based policies in standards such as DICOM and in m-Health architectures. First and most important, there is a **tradeoff between capacity, robustness and image distortion** — except for zero-watermarking techniques, whose tradeoff is only between capacity and robustness.

Thus, as new watermarks are added, especially if they are robust, the quality of the image decreases and the image may lose its clinical value — this affects greatly to non-reversible techniques. Regarding the robustness-capacity tradeoff, it implies that robust watermarks cannot be long. Second, **watermarks embedded by different users may interfere** between them, since each new watermark may destroy part of the content of the others — in the case of zero-watermarking techniques, the content of a watermark may reveal part of the content of other watermarks associated to the same image. Finally, the use of non-reversible, region-based and reversible watermarking **in cooperative m-Health architectures would imply an important cost in bandwidth and delays**, since every time that a user embeds a watermark in an image, he/she has to deliver the watermarked image together with the watermark keys to the rest of users. If an image is watermarked several times by different users, it needs to be transmitted every time to the rest of users.

### 1.3.3 What can be improved?

This Thesis studies a proposal for the integration of appropriate levels of security and privacy levels **in m-Health architectures** in a cost-efficient manner, to cope with the requirements depicted in Section 1.1. As illustrated in Figure 1.4, this proposal may be divided into four interrelated blocks. There shall be a block —colored in blue in Figure 1.4— depicting a **global security scheme** that guarantees different security and interoperability levels according to how critical are the m-Health applications to be implemented. In addition, it shall be guaranteed that all the protocols that cooperate in the m-Health architecture for the acquisition, exchange and/or management of this information meet the security standards described in the former security scheme. Therefore, there shall be a block —colored in dark green in Figure 1.4— that addresses the **extension of certain biomedical standardized protocols** that put little emphasis on certain aspects of security and/or privacy. Complementarily, there shall also be a block dedicated to the development of **novel, secure codings for biomedical tests** —colored in light green in Figure 1.4—, since those are sometimes handled out of the format of a standardized protocol given its high content in clinical information. Finally, in parallel to the former blocks, there shall be a block —colored in orange in Figure 1.4— including selected security methods to be integrated in the rest of them. Within this block, it is worth highlighting a sub-block dedicated to the development of **novel methods for a supplementary protection of biomedical tests through their associated signals**.

At the time of designing the global security scheme, it is worth reminding that the Integrating the Healthcare Enterprise (IHE) initiative already promotes and guides the coordinated use of different standards in healthcare systems (e.g. PHRs, EHRs, alert managers, CDSS), by defining profiles intended for use cases in the medical domain —

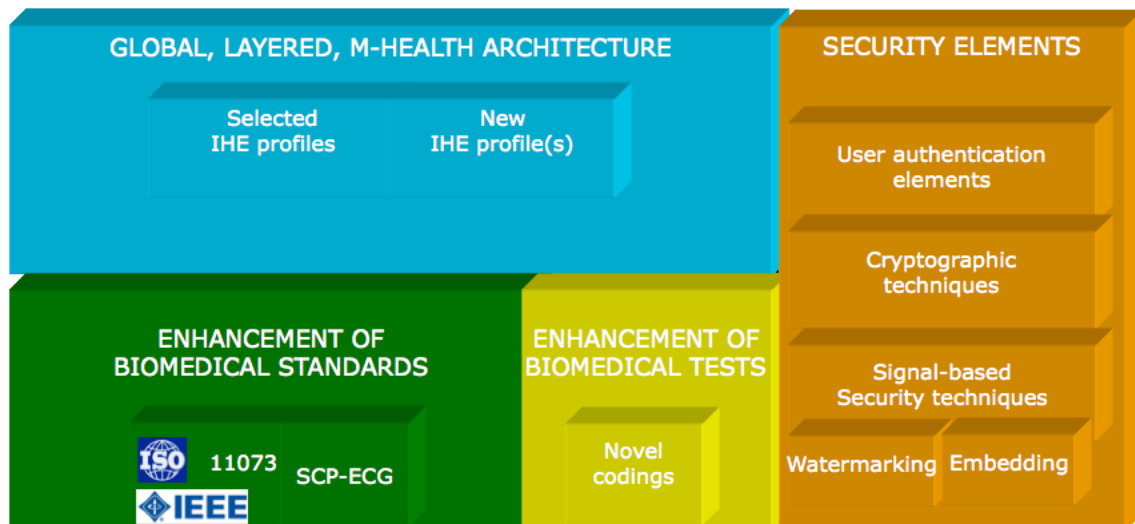


Figure 1.4: Building blocks for a secure, cost-efficient, m-Health architecture.

some of them dedicated to security. Nonetheless, an m-Health, IHE-based framework (e.g. X73PHD-IHE) would lack continuity in security and privacy — given that PAN protocols like X73PHD or SCP-ECG are very limited in this respect — and it would also lack in specifications about the IHE profiles — apart from Rosetta, which permits sharing a common terminology between X73PHD and IHE — required to implement different m-Health applications. Thereby, the proposal of a flexible model (e.g. layered and additive) linking adequate IHE profiles with the demands of different m-Health applications — e.g. oriented to health and fitness, independent living or chronic disease management; involving cabled or wireless setups; oriented to in-hospital care or remote monitoring — would be fundamental for the development of secure, interoperable and cost-efficient solutions in m-Health architectures. Such design shall comprehensively address the vulnerabilities detected after a risk assessment of a generic m-Health architecture.

With respect to the strengthening of vulnerable standard biomedical protocols, most effort shall be dedicated to PAN protocols. Two major, widespread and quite different protocols deserve their security enhancement: ISO/IEEE 11073 PHD and SCP-ECG.

- The ISO/IEEE 11073 standard for Personal Health Devices enables an interoperability model between generic PHDs, which can gather a variety of biomedical measurements (e.g. weight, blood pressure) and signals (e.g. ECGs), and concentrator devices — e.g. health appliances, routers. X73PHD provides a robust syntactic model and a comprehensive terminology, but it places limited emphasis on security and on interoperability with IHE-compliant systems and frameworks. However, the implementation of m-Health applications are increasingly requiring features like secure connection to mobile concentrators — e.g. smartphones, tablets —, sharing of

devices among different users with privacy and interoperability with certain IHE-compliant healthcare systems. Therefore, proposing a comprehensive IHE-X73PHD extension based on the global security design of the m-Health architecture and tailored to the features of X73PHD (especially its built-in security) would be of great relevance. In this regard, the procedures to support the new features — such as the identification of users to enable the sharing of PHDs and/or CDs with privacy, the protection of the communications or the compliance with EHRs and CDSS — shall be carefully chosen to minimize the impact on the X73PHD models, on its architecture (in terms of delays and overhead) and on its framework. Moreover, the extended X73PHD shall preserve its essential features while extending them with added value.

- The SCP-ECG defines an interoperability model to allow the standardized storage and exchange of ECGs between medical ECG devices (carts) and ECG user systems but it does not integrate any security-related feature. Again, an enhancement of this standard based on the global security design and adapted to its specifics would help in the configuration of robust m-Health architectures. Therefore, such approach shall permit SCP-ECG files to be stored safely and proper access to be granted (or denied) to users for different purposes: interpretation of the test, consultation, clinical research or teaching. The access privileges shall be scaled by means of role-based profiles supported by cryptographic elements (encryption, digital certificates and digital signatures), arranged as metadata extending the protocol. The resulting extension shall have a low impact on the file size and access times, and be compliant with any version of the standard.

As regards to signal-based techniques, embedding and watermarking, the former may be of great use for the development of optimal biomedical test codings (see Section 1.2.2), while the second may be mainly used to strengthen the security of standard biomedical protocols with advanced features:

- The main difficulty of embedding techniques in the m-Health context is finding the place where they can be truly useful. As illustrated in Figure 1.5, these techniques would be appropriate to develop optimal test codings that could be integrated/encapsulated by simple PAN protocols (e.g. those associated to open-source platforms) and also by well-established standards, to guarantee a layer of protection when the signals are extracted and handled out of the standardized format. Since the signal is the core of the typical biomedical test, it makes sense to develop optimal biomedical test codings where different types of information may be embedded within the signal (e.g. an ECG) to guarantee a tight association. As explained in Section 1.2.2, it would be necessary that the coding of the signal with the embedded data integrates

security and privacy, and enables high compression ratios in order to reduce the energy for transmission. The most efficient manner to harmonize these requirements is by performing the embedding in an adequate compressed domain, in such a manner that the resulting signal preserves its clinical quality and the embedded data is hidden and protected with a layer of cryptography. Regarding the contents to be embedded, they would typically be periodic measurements (e.g. NiBP, Temp, CO<sub>2</sub>, SPO<sub>2</sub>, pulse rate), contextual data (extracts of the health records of the patient) and/or security elements (e.g. digital signatures, authentication codes).

- Watermarking might have been a good security complement for biomedical standards like DICOM, whose security measures have traditionally been implemented by means of cryptography. Authentication, traceability control for user accountability, private captioning with role-based access control or integrity control with tamper location are some examples of security application that may be added by means of watermarking. However, certain drawbacks derived from the fact that most watermarking processes modify the image, degrading its clinical quality (see Section 1.3.2), explain why biomedical standards hitherto do not integrate them — despite the existing research works [176, 177, 178, 179, 132]. The development of a novel zero-watermarking-based technique meeting two essential requirements, 1) the ability of performing a secure and fast association of different types of data to certain image features and 2) the non-modification of the image (e.g. by encoding the “watermarks” as a function of selected image features and the data to be associated), would presents five relevant improvements. First and most obvious, the image would always preserve its clinical quality without the need for assessment. Second, the most stable features could be used to associate information, which would guarantee optimum robustness-capacity. Third, no complex rules would be necessary for a secure and robust selection of the image features. Fourth, image collusion and forgery attacks would have no effect on this type of “watermarked” images and the rest of threats could be prevented with basic cryptographic protection measures. Fifth, this technique would enable the deployment of secure applications and efficient, cooperative architectures, since each user could add information related with the test with no risk of distorting or removing the information associated by others. To share the updates of the information associated to the test, it would be enough to send the new “watermarks” to the rest of the users.

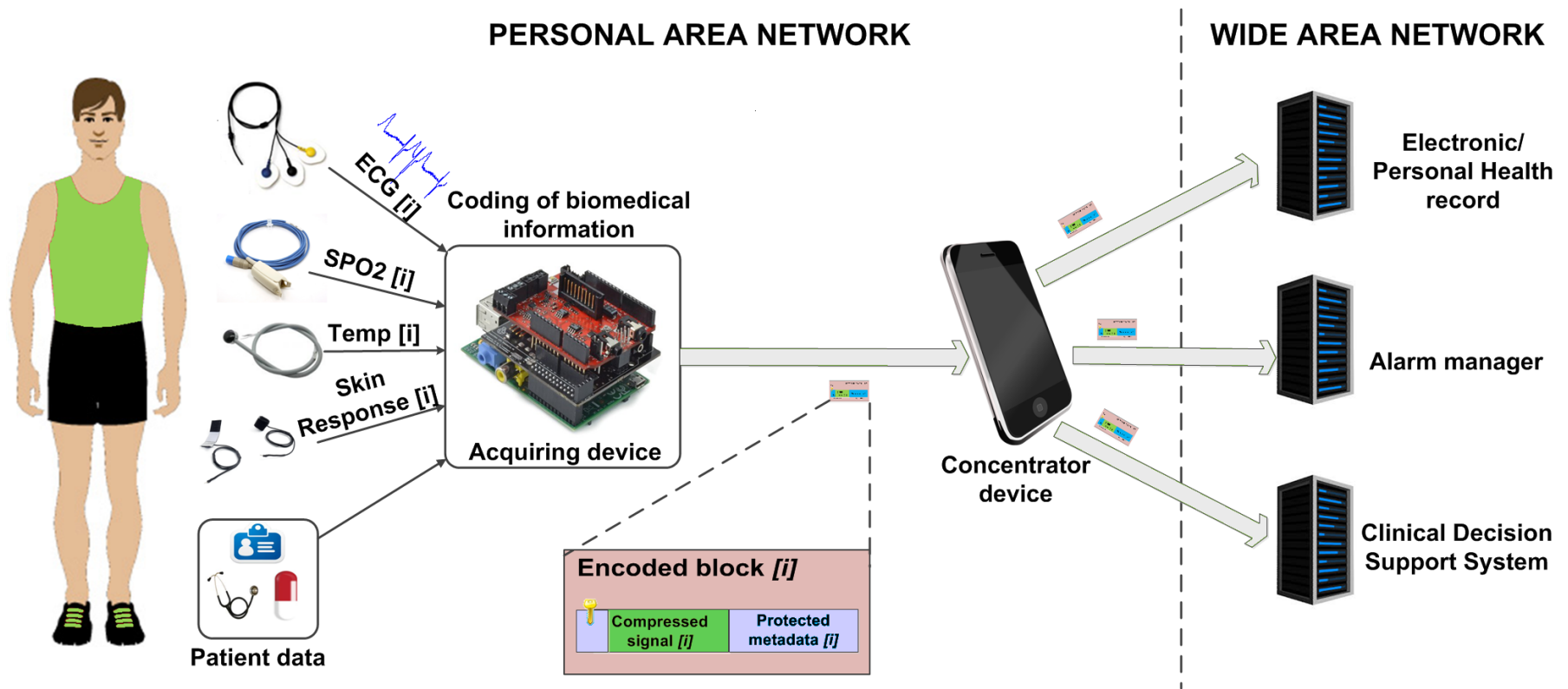


Figure 1.5: M-Health architecture intended for simple open-source platforms, based on the efficient and secure coding of biomedical information acquired by several sensors and interfaces.

## 1.4 Thesis approach, hypothesis and objectives

The **general approach of this Thesis** is to research and make contributions to the field of ICT applied to the Health area. Nowadays, research results in Communication Technologies and the Information Society are considered strategic. Moreover, the application of these technologies to the Health area through the deployment of secure and cost-efficient m-Health architectures facilitates citizens' access to a broad variety of services for the prevention, detection, follow-up and research of health conditions. Therefore, investigations in this area are highly relevant thanks to the benefits that users/patients, caregivers, researchers and the whole health system enjoy.

Specifically, the **focal aim of this Thesis** is on designing an architecture that enables the secure exchange of biomedical information in m-Health scenarios —focusing on biomedical tests, mainly comprised by signals that may attach measurements and/or contextual data. This Thesis rests on two fundamental pillars: (a) the investigation on the improvement of the security levels of protocols conducting the standardized storage and/or transmission of biomedical information and (b) the contributions on the development of novel methods for the protection of biomedical tests (e.g. cardiac rest tests) through secure codings based on their associated signals (e.g. ECGs, echocardiograms), which may be stored out of standardized formats (given its intrinsic clinical value) or transmitted with simple protocols not including basic security —e.g. highly efficient PAN protocols.

This approach suggest the five **uppermost hypothesis**:

- A layer-based security proposal would permit the harmonization of standardized protocols in m-Health architectures and the promotion of personalizable and cost-efficient applications.
- A moderate security extension of the ISO/IEEE 11073 models would enable the harmonization with IHE, to enhance the interoperability of personal health devices with health information and medical systems (e.g. electronic health records, clinical decision support systems, alert systems), without limiting the previous functionalities of this set of standards.
- A simple security extension of SCP-ECG would guarantee adequate protection and enforcement of role-based access control policies while maintaining small file sizes, fast access times and compliance with regular SCP-ECG viewers and editors.
- The research on codings based on orthogonal transformations, which scale the energy of signals efficiently, would enable the development of novel, cost-efficient techniques for the secure embedding of large amounts of information —to support m-Health services— on small-size biomedical signals while maintaining their clinical value.

- Medical Image Watermarking techniques, particularly those based on orthogonal transformations and zero-watermarking, contain robust basis for the evolution towards innovative, non-distorting and efficient techniques for enhancing the security of biomedical tests.

Thus, the major aim of the Thesis, together with the above mentioned hypothesis, lead to the **overall objectives**:

- Design of a secure and cost-efficient m-Health architecture which facilitates the development of services with different protection and interoperability requirements and bridges contributions to the security of standards and biomedical tests.
- Study, proposal and evaluation of methods to enhance the security of standard protocols for the exchange of biomedical information, according to criteria that maximize their interoperability and cost-efficiency.
- Design and evaluation of novel, efficient methods to enhance the security of biomedical tests through their associated signals, and which may be integrated by both simple and standardized exchange protocols.

On a deeper level, the following detailed objectives can be mentioned. They are presented subdivided into the main topics of the thesis. First of all, as regards to the **contributions on the design of a secure and cost-efficient m-Health architecture**:

1. *To prepare a detailed risk assessment of a generic m-Health architecture.*
2. *To analyze common demands of major legal regulations regarding the m-Health context.*
3. *To present a well-depicted, cost-efficient, global security proposal for protecting the exchange of biomedical information in m-Health architectures.*
4. *To translate the previous global security proposal into specific measures that guarantee adequate levels of security and interoperability.*
5. *To assess the security of the m-Health architecture after its enhancement.*

Second, concerning **standardized protocols**:

6. *To design a cost-efficient security extension, based on 3), for the standard ISO/IEEE 11073 PHD.*
7. *To appraise and discuss the implications and the impact of the former extension on the ISO/IEEE 11073 PHD models, architecture and framework.*
8. *To analyze the implications of the extension of ISO/IEEE 11073 PHD on IHE.*



9. *To design a robust and simple security extension, based on 3), for the standard SCP-ECG.*
10. *To evaluate the impact of this extension on SCP-ECG, by means of a proof of concept.*
11. *To define adequate means to enable the integration of novel signal-based protection methods in DICOM.*

Third, as regards **to techniques for the protection of biomedical tests through their associated signals:**

12. *To conduct reviews on the state of the art about methods that permit embedding large amounts of hidden data on signals, laying emphasis on the biomedical types.*
13. *Design of an optimal coding for biomedical tests — signals, periodic measurements and contextual information — that facilitates the development of secure and cost-efficient m-Health services.*
14. *To develop such optimal coding through a proof of concept, evaluate it and adjust its parameters optimally for both offline and real-time operation.*
15. *To conduct reviews on the state of the art about watermarking, laying emphasis on Medical Image Watermarking methods.*
16. *To develop a novel, non-distorting and efficient technique, inspired in the most promising watermarking methods, for the protection of biomedical images in m-Health architectures.*
17. *To propose optimal parameter configurations for the previous technique (e.g. for the selection of certain image features) in order to associate information to the biomedical image in stable, semistable and volatile manners and to evaluate the robustness, specificity and scalability of these alternatives.*
18. *To propose different configurations (content type and length of the data to be associated to the image; stable, semistable or volatile association; data detection threshold) for the implementation of complementary image-based security applications.*

## 1.5 Research context

This thesis, entitled “Design of a secure architecture for the exchange of biomedical information in m-Health scenarios” and supervised by Álvaro Alesanco Iglesias and José García Moros, has been performed in the framework of the [eHealthZ Research Group](#) of the Aragón Institute of Engineering Research (I3A), within the Biomedical Engineering Doctoral program of the University of Zaragoza, Spain.

Regarding its research context, this Thesis has been developed mostly within wider projects in the lines of Providing security to e-Health environments and m-Health tele-monitoring architectures, such as:

1. PI029/09: “Analysis of echocardiogram coding and real-time transmission through communications networks”.
2. MCINN - TIN-2011-23792/TSI: “Ontology-based interoperable architecture for patients telemonitoring and clinical decision support”.

## 1.6 Thesis outline

The rest of this Thesis is organized as follows: the state of the art of all topics covered — e.g. standards for the exchange of biomedical information, signal coding methods, security technologies — is presented in Chapter 2. This chapter also introduces the proposal of a global design for a m-Health architecture integrating security levels in line with different m-Health applications, which is the central issue of this Thesis. Such proposal specifically guarantees that all the biomedical information exchanged, according to biomedical standards and/or ad-hoc formats, is adequately protected.

The contributions to the enhancement of biomedical standard protocols with low security levels are outlined in Chapter 3. Particularly, this Chapter introduces a security extension for the protocols ISO/IEEE 11073 and SCP-ECG, including a thorough analysis of the implications on their architectures, i.e. on their data and communication models, and also on their frameworks, including attacks that are hindered and how these extension affect the usability of the systems, the delays to access the biomedical information or the interoperability with health information and medical systems.

The development of novel signal-based techniques for the protection of biomedical tests is addressed in Chapter 4. It deepens into two complementary techniques, the former permits embedding high amounts of hidden and protected data into compressed biomedical signals while preserving their intrinsic clinical value — and includes optional support for efficient signal encryption; the latter, called keytagging, permits associating information — with variable strength — to biomedical signals without causing any distortion to them. Furthermore, a series of security applications and scenarios of used are drawn for these techniques, by setting operation parameters that yield optimal features (e.g. compression levels, delays, robustness, specificity, capacity).

Finally, Chapter 5 summarizes research objectives achieved, contributions and accomplished results of this Thesis, and it also lays out suggestions for future lines of research.

*“If you don’t know where you are going, any road will get you there.”*

Lewis Carroll

*“A designer knows he has achieved perfection not when there is nothing left to add, but when there is nothing left to take away.”*

Antoine de Saint-Exupery

# 2

## M-Health architectures: Background and proposed guidelines for their security enhancement

This first part of this Chapter describes the foremost materials — i.e. background — of this research, which includes overviews of major standards for the exchange of biomedical information (Section 2.1), of major biomedical signal coding methods (Section 2.2), of transport technologies eligible in m-Health architectures (Section 2.3) and of legal regulations applicable to this context (Section 2.4). The second part addresses two relevant methods developed in this research, an assessment of the risks of the m-Health architecture (Section 2.5) and the proposal of robust guidelines for its security enhancement (Section 2.6) — which are followed and materialized in detail in Chapters 3 and 4.

### **2.1 Overview of major standards for exchanging biomedical information**

This section introduces the main features of four relevant standardization initiatives in the m-Health context: IHE, focusing on the profiles involved in the secure exchange of biomedical information in the m-Health context (Section 2.1.1); two protocols for the exchange of biomedical measurements and signals that require security enhancements, ISO/IEEE

11073 PHD (Section 2.1.2) and SCP-ECG (Section 2.1.3); and a standard for the exchange of biomedical images and videos, DICOM (Section 2.1.4), whose cryptography-based security may be enhanced through signal-based methods. Finally, Section 2.1.5 compiles and analyzes previous efforts for the security enhancement of these standards.

### 2.1.1 IHE & profiles overview

Integrating the Healthcare Enterprise (IHE) [89] is a non-profit organization founded in 1998 by healthcare professionals and industry members to improve the way computer systems in healthcare share information. IHE is organized by clinical and operational domains, each defining its own integration profiles and technical frameworks. The former define accurately how different communication standards, such as DICOM [79], HL7 [77], IEEE, W3C and security standards, can be implemented to meet specific clinical needs. The latter establish how these integration profiles can be coordinated to facilitate appropriate sharing of medical information and to support optimal patient care. It is worth highlighting that the IHE domains for Patient Care Devices and Health IT infrastructure are closely related with m-Health architectures. In fact, these domains include several integration profiles (Table 1.1) that would solve most of the security issues described in Sections 2.4-2.5 and that would improve interoperability with different healthcare systems:

- *Rosetta Terminology Mapping (RTM)* [180]. This defines a vendor-neutral harmonized mapping for patient care device observations based on ISO/IEEE 11073-10101 nomenclature terms and Unified Code for Units of Measure (UCUM) [181], to facilitate the syntactic — and to some extent semantic — interoperability between devices and systems. The Rosetta Table also works as a temporary repository, in the form of XML files, to allow inclusion of new terms.
- *Consistent Time (CT)* [135]. This provides the means to guarantee that the system clocks — also time stamps and authentication logs — of the devices in a network are synchronized with a median error less than 1 second. It requires the use of the Network Time Protocol (NTP) [182].
- *Device Enterprise Communications (DEC)* [183]. This enables a consistent communication between a Patient Care Device and other systems, such as CDSS or EHRs. This communication may include physiological data (e.g. heart rate, patient weight), point-of-care laboratory tests (e.g. home blood glucose tests), continuous data (e.g. ECG, EEG) —but without addressing real-time operation—, patient information and contextual data. This data can be filtered so that each system receives only the information that it is subscribed to. The current profile does not address issues of privacy, security and confidentiality associated with cross-enterprise communication

of personal measurements. However, it strongly recommends the implementation of IHE compliant transactions for automated acquisition of patient ID credentials — e.g. by means of bar codes (BC) or radio frequency identification tokens (RFID-T) — in order to reduce errors, increase user safety and enhance device and drug effectiveness. This profile works by means of HL7 v2 messages and depends on the CT profile.

- *Alert Communication Management (ACM)* [184]. This permits a Patient Care Device to send the notification of an alert to a portable device, such as a smartphone or a tablet. This alert may be a physiological alarm (e.g. heart rate out of the safe range for a patient) for a caregiver, a technical alert (e.g. ECG leads off the patient) or advisories not related with an alarm. This profile extends DEC.
- *Waveform Content Module (WCM)* [185]. This provides the semantics and the data structure (based on the IEEE 11073 Domain Information Model) to enable the transmission of waveforms acquired by Patient Care Devices (e.g. ECGs) to the IHE actors involved in the DEC and ACM profiles. These waveforms can be provided as bounded waveforms, snapshots associated with a diagnostic encounter or with an alarm event; or as continuous waveforms to be used for remote real-time monitoring. This profile is an option for DEC and ACM.
- *Audit Trail and Node Authentication (ATNA)* [134]. This enforces personal health information integrity and confidentiality and user accountability by implementing local user authentication in the nodes of the health IT infrastructure (e.g. based on username and password, biometrics, smart cards or magnetic cards), connection authentication between communicating nodes (using certificates for authentication and secure transport) and audit trails (by means of the Syslog protocol [186]). This profile depends on CT.
- *Cross-Enterprise Document Sharing (XDS)* [187]. This provides standard-based means — mainly based on HL7 v2 and OASIS ebXML [188] — for managing the sharing of documents between any healthcare organization. This profile depends on ATNA and CT.
- *Enterprise User Authentication (EUA)* [143]. This enables centralized user authentication management — compliant with ATNA — and provides users with reliable and fast single sign-on, which can be based on passwords, tokens, smart-cards and biometrics. This profile relies on Kerberos [189] and HL7 Clinical Context Object Workgroup (CCOW), and it depends on CT.
- *Patient Identifier Cross Referencing (PIX)* [190]. This provides interoperability when cross-referencing patients among different systems. This profile uses the HL7

v2 protocol and depends on CT.

- *Basic Patient Privacy Consents (BPPC)* [140]. This permits patient privacy consent(s) to be recorded so that patients can selectively control access to their healthcare information. It defines a mechanism — equivalent to that in EHR systems — to enforce this policy. This profile complements XDS, so implementation of the latter is required.

In addition to this, the IHE white paper “Medical Equipment Management: Cyber Security” [191] addresses the increasing risks associated with different types of personal care devices, specifically those risks of malware outbreaks and breaches of personal health information, and provides guidance on countermeasures at different levels — device protection, network architecture, life-cycle management, security best practices — to solve these problems.

### 2.1.2 ISO/IEEE 11073 PHD overview

The ISO/IEEE 11073 is a set of standards aimed at providing interoperability between personal health devices (referred to as “agents” in the X73PHD context) and concentrator devices, usually called “managers” (e.g. smartphones, personal computers, personal health appliances, maybe smart TVs), which has been successfully implemented in several devices and platforms [192, 193, 194]. The architecture of a typical X73PHD-compliant system involves a number of entities (Figure 2.11-A), namely:

- **Users:** The person the measurements belong to.
- **Agents:** The personal health devices used to take such measurements (e.g. weighing scale, thermometer, pulse oximeter, etc.).
- **Managers:** The concentrator devices used to aggregate the measurements from agents. Managers can associate to several agents simultaneously, but agents can associate to only one manager at a time.
- **Administrators:** The person in charge of managing agents and managers. In a home environment any user can play the role of administrator.

Furthermore, there are three additional entities that are common in a healthcare framework (Figure 2.11-B):

- **Manufacturers:** The companies producing the devices (agents or managers).
- **Certification authorities:** Entities that issue digital certificate to uniquely identify each entity (e.g. an agent, a managers, a user, etc.).

- Health Information System (HIS): The information system the data may be sent to, it includes other systems such as PHRs, EHRs, CDSS or alarm systems —which may also operate independently from the HIS.

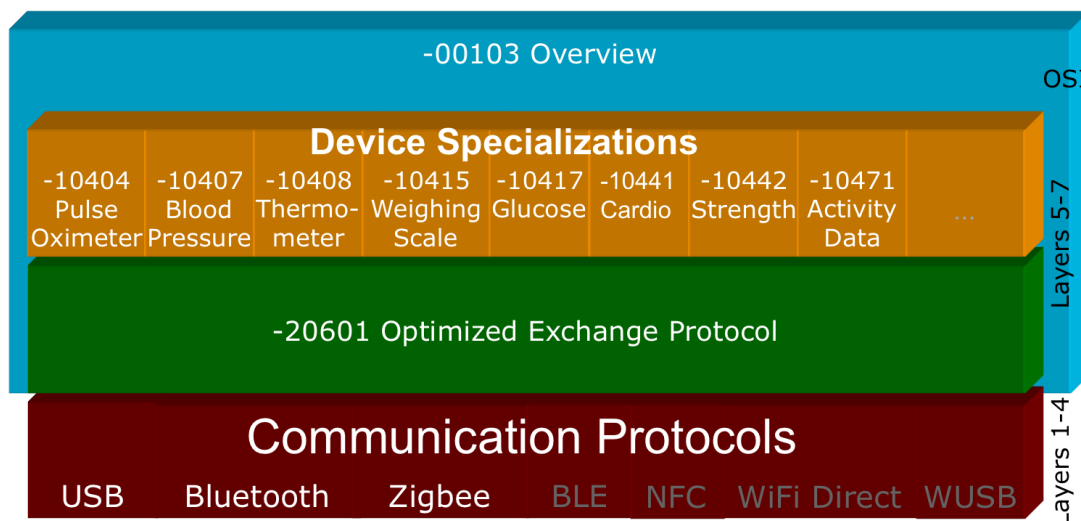


Figure 2.1: ISO/IEEE 11073 PHD standards overview.

Among the ISO/IEEE 11073 family (Figure 2.1), it is worth highlighting the 11073-20601<sup>TM</sup>-2014 Optimized Exchange Protocol. This defines a reference model (Figure 2.2) based on an object-oriented paradigm that guarantees extensibility and reusability by defining three interrelated models:

- Domain information model (DIM). The DIM characterizes information from an agent as a set of objects with one or more attributes, which describe measurement data that are communicated to a manager as well as elements that control behavior and report on the status of the agent. The DIM covers the definition of the MD system (MDS) object, scanner objects (for data reporting), different metrics (numeric, real-time sample array –RT-SA–, and enumeration objects) and persistent metric (PM) objects, used for data storage.
- Service model. The service model provides data access primitives that are sent between the agent and manager to exchange data defined in the DIM. These primitives include commands such as Get, Set, Action, and Event Reporting.
- Communication model. The communication model supports the topology of one or more agents communicating over point-to-point connections to a single manager. The dynamic system behavior for each point-to-point connection is defined by a connection finite state machine (FSM), which defines the states and sub-states that an agent and manager pair passes through, including states related to connection, association, and operation.

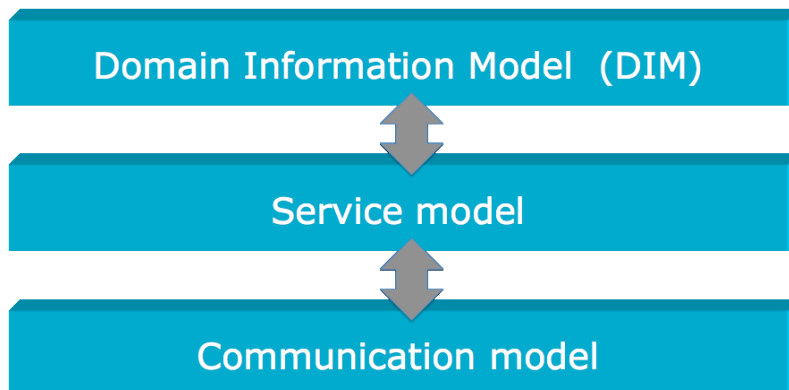


Figure 2.2: ISO/IEEE 11073 PHD three-level architecture.

Complementarily, several agent specializations have been issued and grouped in three different domains:

- Disease Management (ranging from ISO/IEEE 11073-10400 to 11073-10439), which includes specializations for pulse oximeters, heart rate monitors, blood pressure monitors, thermometers, weighing scales, glucose meters, ECG 1–3 leads, international normalized ratio (INR) monitors —of blood coagulation—, body composition analyzers, peak flows and, under development, for insulin pumps, sleep quality monitors, urine analyzers, sleep apnoea breathing therapy equipment and continuous glucose monitors.
- Health and Fitness (ranging from ISO/IEEE 11073-10440 to 11073-10469), with specializations for heart rate monitors, weighing scales, thermometers, cardiovascular fitness and activity monitors, strength fitness equipment and physical activity monitors.
- Independent Living (ranging from ISO/IEEE 11073-10470 to 11073-10499), which groups specializations for disease management devices plus independent living activity hubs and medication monitors.

### Security features

While Health, Fitness and Independent Living applications are mainly intended for user self-control of his/her health condition — which may be based on maintaining a PHR and supervision by an alarm system —, Disease Management applications usually require some degree of medical supervision — which may be based on the connection to an EHR, CDSS and/or alarm system. Therefore, these applications demand integration capabilities and security requirements. X73PHD does not address the former and, regarding the latter, only a few aspects can be considered as security-related features:



- **User identification:** The conditional attribute PersonID may be used to differentiate different persons in a store-and-forward scenario. As a conditional attribute, agents may not support this feature. This attribute is vendor-dependent and is modeled as a 16-bit unsigned integer. In any case, the process of mapping this ID to a specific person is outside the scope of the standard.
- **Device identification and authentication:** In X73PHD, managers are not identified. Agents include the mandatory attribute System-ID in their DIM, which is an IEEE EUI-64 which, in turn, consists of a 24-bit organizationally unique identifier (OUI) followed by a 40-bit manufacturer-defined ID. There is also the mandatory attribute System-Model, which contains the manufacturer's name and the manufacturer's specific model information in a printable ASCII form. Neither of these, however, is used by X73PHD to complete a mutual agent-manager authentication. They are only used to discern different agents in a manager and, eventually, to speed up the configuration process of known agents. Nonetheless, the underlying transport technology may implement its own procedure for secure device pairing.
- **Time coordination:** In X73PHD, agents shall implement a way of reporting the time when measurements were taken if the measurements delivered by the agent are not "freshly acquired". Timestamps are mandatory when the measurements come from the temporary storage of the agent — the PM-store.
- **Encryption:** X73PHD does not define any encryption mechanism. However, data may travel encrypted if such a feature is implemented by the lower layer transport technology.

### 2.1.3 SCP-ECG overview

With the spread of digital electrocardiography, the SCP-ECG [76] was created in the early 90s to allow the storage of ECGs and the interchange between medical ECG devices (carts) and ECG user systems. It was initially supported by the European Committee for Standardization (CEN) to achieve interoperability among most medical ECG equipment. Now it is integrated in the ISO/IEEE 11073 family and the goal is more ambitious: to interoperate with other medical devices as well. Nevertheless, harmonization is needed to coordinate both standards [195].

The SCP-ECG defines a binary encoded format of data and mechanisms for the compression of the ECG signal in order to reduce the final size of the ECG file. This permits the transmission of ECGs in scenarios with low transmission ratios and the saving of disk space in storage. Although the SCP-ECG was primarily intended for 12-lead records in

short-term tests, it allows different numbers of leads and it has been successfully adapted to stress tests, Holter recordings and real-time transmission [196, 197].

This standard also supports ECG measurements (i.e. average RR intervals), ECG feature extraction (i.e. onset/offset of P waves and QRS complexes), pattern recognition, ECG interpretation (i.e. normal ECG, left ventricular hypertrophy, left anterior fascicular block, posterior myocardial infarction) and diagnostic classification.

Regarding SCP-ECG compliant software, there are many freely available programs [198] including viewers, writers, parsers, format and content checkers. There are also methods for the harmonization of this ECG standard with others, such as the aforementioned DICOM Waveform Supplement 30 [199], HL7 aECG [200] and MFER (Part 2.6 of the protocol).

### SCP-ECG structure and data content

The SCP-ECG is divided into 12 different sections (Table 2.1), defined by its own encoding rules and preceded by a common header (Figure 2.3). Regarding their contents, five different groups may be distinguished:

- **Section 0:** this stores the **pointers** to the start of the remaining sections in the record. This section does not contain any information itself, so it is considered as public.
- **A, Section 1 - tags 0-3, 5, 14-26, 31:** these fields contain the identification of the patient and the physician(s), institution(s) and device(s) involved in the acquisition, analysis and diagnosis of the ECG. These data must be considered as highly confidential since they can identify the patient (directly or indirectly) in a file full of health data.
- **B, Section 1 - tags 4, 6-13, 27-30, 32-35, 255:** these contain general information about the patient (e.g. age, weight, height), his/her health condition (e.g. medical history, drugs) and data for the correct interpretation of the ECG (type of filtering applied). This part (together with parts **C** and **D**) may be used to find correlations between medical condition of large groups of patients and the more likely causes/risk factors for a variety of heart diseases. In terms of privacy, these data itself do not identify the patient.
- **C, Sections 2-6:** these identify the leads which are present in the record (*Section 3*) and store **the ECG signal data** (*Section 6*), which may be kept as uncompressed raw data or alternatively compressed by different methods. The compression ratio which can be achieved ranges from less than 2-4:1, when only using Huffman tables

(*Section 2*), or up to 6-20:1 when combining second-order differences (using *Sections 4* and *5*) with Huffman encoding and downsampling, at the cost of lower signal quality. In the absence of patient identification, (**A**), this information can not be used against the patient: even if it is used for biometric identification, another ECG from the same patient must be known previously, so no new information is obtained.

- **D**, *Section 7-11*: these sections can be optionally added to include:
  1. global **measurements** (*Section 7*) and measurements from each lead independently (*Section 10*), to help the physician’s work;
  2. the **diagnostic interpretation of the ECG** record (*Section 8*), which must be consistent with the manufacturer interpretive statements (*Section 9*) and the universal ECG interpretive statement codes and coding rules (*Section 11*);

These data interprets or helps to interpret the ECG of the patient, so if he/she is identified (**A**), this information must be treated with strict confidentiality.

Sections numbered 12 to 127 and those above 1023 are reserved for future use. Regarding compliance, the ISO/IEEE 11073-91064:200 protocol version defines two categories:

1. Demographics and ECG rhythm data (uncompressed or with lossless compression).
2. Demographics, ECG rhythm data (uncompressed, with lossless compression or with high compression) and reference beats.

Parts **B** and **D** are optional, hence they will be referenced as [**B**] and [**D**].

Table 2.1: SCP-ECG Data Sections

Section	Status	Content
-	Required	2 bytes CRC Checksum
-	Required	4 bytes Record Length
0	Required	Pointers to data areas in the record
1	Required	Header information – patient data/ECG acquisition data
2	Dependent	Huffman tables used in encoding of ECG data
3	Required	ECG lead definition
4	Optional	QRS location (if reference beats are encoded)
5	Optional	Encoded reference beat data if reference beats are stored
6	Required	“Residual signal” if beat subtraction is performed, otherwise encoded rhythm data
7	Optional	Global measurements
8	Optional	Textual diagnosis from the “interpretive” device
9	Optional	Manufacturer specific diagnostic and overreading data from the “interpretive” device
10	Optional	Lead measurement results
11	Optional	Universal statement codes resulting from the interpretation



## SCP-ECG Messaging/Transport Protocol

Since the standard is intended for the exchange of SCP-ECG files, between ECG medical devices (carts) or between carts and user devices (computers, PDAs, smartphones, etc.), it dedicates:

- Annex D to recommending a simple architecture and a set of control (ID, Status, Done, Advisory) and request messages to send/receive a) ECGs (types S, R), b) ECG lists for specified patients (types E, L), or c) patient lists for specified names (types I, P); and
- Annex E to giving a possible solution for low level transport of data (physical function and data link function layers).

Protecting the communications involving patient data is as important as protecting the SCP-ECG files, so this issue must be addressed in the security policy.

### File size and access delays

The size of SCP-ECG files is highly concentrated in its part *C*, which stores the signal. This protocol supports the storage of raw signals and the use of simple compression methods, which depending on the signal length achieve compression rates ranging from 2-4:1 (lossless compression) to 6-20:1 (lossy compression). Assuming that the typical signal duration ranges from 10 to 30 seconds and the acquisition bitrate from 3000 bps (e.g. MIT-BIH Compression database [201]) to 8000 bps (e.g. T-Wave Alternans Challenge database [202]), this results in:

- minimum expectable signal size of  $\frac{3000 \text{ bps} \cdot 10 \text{ s} \cdot 12 \text{ (leads)}}{6 \text{ (CR)}} \text{ bits} = 7.32 \text{ KB}$ .
- maximum expectable signal size of  $8000 \text{ bps} \cdot 30 \text{ s} \cdot 12 \text{ (leads)} \text{ bits} = 351.6 \text{ KB}$ .
- typical expectable signal size of  $\frac{4000 \text{ bps} \cdot 10 \text{ s} \cdot 12 \text{ (leads)}}{2 \text{ (CR)}} \text{ bits} = 29.3 \text{ KB}$ .

Regarding the remaining parts, *A*, composed of up to 19 fields, typically takes less than 1 KB since it only contains IDs, names and free-text short descriptions. Part *[B]*, composed of up to 18 fields, typically takes less than 0.5 KB since most fields are described with 1-4 bytes and only a few require free-text description. Part *[D]*, composed of up to 5 sections, is not expected to be larger than 2 KB, mainly contributed by Section 8 (expected less than 0.35 KB) and Section 11 (expected less than 1.2 KB). Since only four fields of part *A* (2,14,25,26) and part *C* are mandatory, the minimum expectable file size is  $\simeq 7.4 \text{ KB}$ . In the opposite case, the maximum expectable size of a file is the sum of maximum of each

part,  $(A) 1KB + (B) 0.5KB + (C) 351.6KB + (D) 2KB = 355 KB$ . In the most typical cases, the expectable size is  $\simeq (A)0.5KB + (B)0.25KB + (C)29.3KB + (D)1KB = 31 KB$ .

The delays associated to the SCP-ECG may be divided into:

- Collection of information about the patient and the recording session to complete parts **A** and **[B]**. It depends on the means, a person typing the data can spend several seconds (typically a minute) on this task, while a proper connection to a patients database speeds up this operation (to typically 0.2-0.5 s).
- Acquisition of the signal, to be stored in part **C**. This is equal to the signal duration, between 10 and 30 seconds. If the signal is compressed, there is a small additional delay of  $\simeq 50$  ms.
- Analysis of the signal to obtain part **[D]**. It comprises the obtaining of global measurements and measures from each lead independently (40-120 ms) and its interpretation by a cardiologists ( $\geq 1$  minute) and sometimes an analyzing device (10-30 ms).
- Access to the file contents by using an application. Loading the data fields and plotting the signal leads on screen typically takes less than 50 ms.

Two typical delays can be obtained from these data, (1) the delay to obtain a basic SCP-ECG file (parts **A**, **[B]** and **C**) is  $\simeq 10$ -30 seconds, and (2) the delay to access the file and interpret it (using and/or completing part **[D]**) is  $\simeq 1$  minute.

### Security features

The SCP-ECG includes no security policy, so its security extension must be designed carefully. In the first place the main aspects of this standard must be analyzed in detail, since the extension must be in harmony with the scope of the protocol, maintain its structure, protect adequately and be able to retrieve its exact contents, not change substantially its file sizes and associated delays and allow interoperability with existing devices and software. Secondly the measures adopted by other major medical protocols to enforce reliability and privacy must be surveyed. Third, the security measures that the SCP-ECG shall implement must be accurately established no minimize costs.

#### 2.1.4 DICOM overview

In response to the increasing use of digital images in radiology, the American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA) formed a joint committee in 1983 to create a standard format for storing and transmitting medical

images. The committee published the original ACR-NEMA standard in 1985. This has subsequently been revised and in 1993 the standard was renamed DICOM. DICOM is administered by the NEMA Diagnostic Imaging and Therapy Systems division and each year the standard is updated. Details of recent improvements can be found on [79].

The standard describes how to format and exchange medical images and associated information, both within the hospital and also outside the hospital. DICOM interfaces are available for connection of any combination of the following categories of digital imaging devices: (a) image acquisition equipment such as computed tomography, magnetic resonance imaging, computed radiography, ultrasonography, and nuclear medicine scanners; (b) image archives; (c) image processing devices and image display workstations; (d) hard-copy output devices such as photographic transparency film and paper printers.

DICOM addresses five general application areas:

1. Network image management.
2. Network image interpretation management.
3. Network print management.
4. Imaging procedure management.
5. Offline storage media management.

DICOM is a message standard that facilitates interoperability of medical imaging equipment by specifying:

1. For network communications, a set of protocols to be followed by devices claiming conformance to the standard.
2. The syntax and semantics of Commands and associated information which can be exchanged using these protocols.
3. For media communication, a set of media storage services to be followed by devices claiming conformance to the standard, as well as a File Format and a medical directory structure to facilitate access to the images and related information stored on interchange media.

### **DICOM file format**

A single DICOM file contains both a header (which stores information about the patient's name, the type of scan, image dimensions, etc), as well as all of the image data. The header and the image data are stored in the same file. The image data follows the header information.

Table 2.2: Relevant fields of the DICOM header from an Acuson device

Field	Contents
Filename	[1x65 char]
FileModDate	“12-nov-2010”
FileSize	2361370
Format	“DICOM”
FormatVersion	3
Width	1024
Height	768
BitDepth	8
ColorType	“truecolor”
FileMetaInformationGroupLength	204
MediaStorageSOPClassUID	“1.2.840.10008.5.1.4.1.1.6.1”
TransferSyntaxUID	“1.2.840.10008.1.2.1”
ImplementationClassUID	“1.2.276.0.7230010.3.0.3.5.4”
Modality	“US”
Manufacturer	“SIEMENS”
InstitutionName	“HC LOZANO BLESA”
ManufacturerModelName	“ACUSON SC2000”
PatientName	[1x1 struct]
PatientID	“XXXXXXXXXXXXX”
PatientBirthDate	“XX”
PatientSex	“X”
HeartRate	88
SequenceOfUltrasoundRegions	[1x1 struct]

The size of the header varies depending on the acquisition device and image type. The DICOM elements required depend on the image type that are listed in Part 3 of the DICOM standard [203]. DICOM requires a 128-byte preamble (these 128 bytes are usually all set to zero), followed by the letters 'D', 'I', 'C', 'M'. This is followed by the header information, which is organized in groups: general information, patient, study, series, frame of reference, equipment and image information. In Table 2.2 some fields of a header for an ultrasound device are shown. Of particular importance is the “Transfer Syntax Unique Identification” which reports the structure of the image data, revealing whether the data has been compressed or not. Another important field in the DICOM header included in the ultrasound is the regions calibration, see “SequenceOfUltrasoundRegions” in Table 2.2. It defines regions on the ultrasound image with different calibration and the calibration parameters in order to be able to perform measurements on the ultrasound



regions. The calibration header is defined in Part 3 of the DICOM standard [203]. The regions definition depends on the echocardiogram devices and not all the devices define these regions. In Figure 2.4 the calibration regions for an M mode are shown. There are four calibration regions that are defined with four coordinates each one: “Region Location Min X0”, “Region Location Min Y0”, “Region Location Max X1” and “Region Location Max Y1”. The “Region Spatial Format” and the “Region Data Type” of each region indicates the type of mode and data within the region. For example M mode or 2-D mode (tissue or flow) and color bar or spectral (CW or PW Doppler).

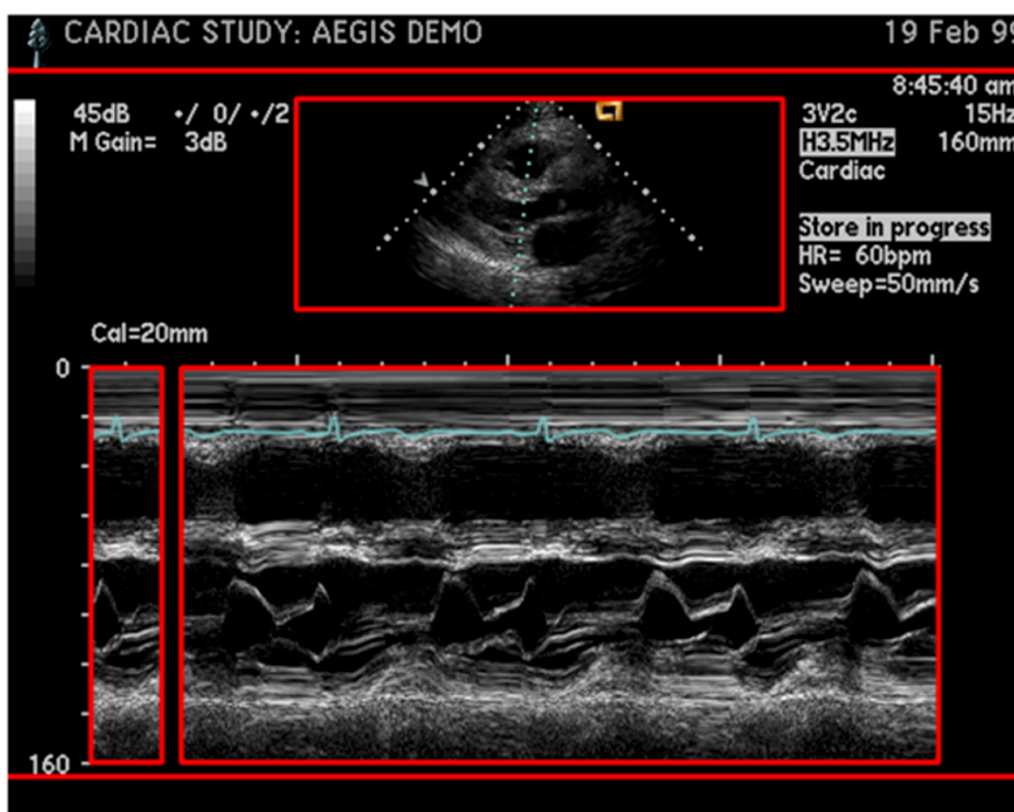


Figure 2.4: Calibration regions for the M mode of an echocardiogram acquired with an Agilent device.

The DICOM image exam can be compressed either lossless or lossy in order to reduce disk space. The image format is specified in the “Transfer Syntax Unique Identification” header. The codecs included in DICOM are described in Part 5 of the standard. The image formats supported for DICOM are raw data, lossless Run Length Encoding (RLE) [204], JPEG [205] lossy and lossless mode, JPEG-LS lossless and near-lossless mode, JPEG2000 [165] lossless and lossy mode, MPEG-2 MP@ML and MP@HL image compression, and MPEG-4 AVC/H.264 [206] high profile video compression.

## Security features

DICOM dedicates its Working Group 14 to develop extensions to the standard that address the technical details of providing secure information exchange. These extensions are published in the form of DICOM supplements (Section 1.3.1) and in part 15 of the standard [144]. It is worth highlighting that there is a tendency to harmonize the security policies of IHE, DICOM and HL7. Currently, DICOM includes security specification that permit:

- Integrating Audit Trail and Node Authentication profile (IHE) (ATNA). These contribute to access control by limiting network access, by implementing:
  - User authentication, which is local for each node.
  - Connection authentication between nodes.
  - Audit trails for user accountability.
- Implementing secure transport connection (e.g. by means of Transport Layer Security [207] — TLS —, with Kerberos [189] or SAML [208] for identity negotiation), in order to guarantee data integrity during transit, entity authentication and confidentiality during transit via encryption. This protects against eavesdropping, masquerading and tampering.
- Embedding Digital Signatures (DS), which
  - Guarantee data integrity for the life of the file.
  - Identify signatories, with optional timestamps.
  - May be included in Digital Signature Profiles (Base, Creator and Authorization RSA Profiles).
  - May be included in Structured Reports.
- Implementing storage security profiles, which basically allows encapsulation of a DICOM file into a Secure DICOM File guaranteeing confidentiality, integrity and optionally data origin authentication. A Secure DICOM File shall contain an Enveloped-data content protected by means of Cryptographic Message Syntax (CMS) [151].
- Protecting the confidentiality of sensitive attributes, by means of:
  - De-identification and re-identification.
  - Removal of sensitive data information (corresponding to certain DICOM attributes — patient ID, study, series, date of acquisition — or to text annotations) burned on the image.

- Distortion of recognizable visual information in the image that permits the recognition of a patient.
- Implementing robust network address management, with secure Domain Name System (DNS) [209] and Dynamic Host Configuration Protocol DHCP [210] configurations.
- Implementation accurate time synchronization of the machines in a network by means of Network Time Protocol or Simple Network Time Protocol (NTP/SNTP) [182, 211].

### 2.1.5 Related publications on the protection of biomedical standards

The security extension of SCP-ECG is not addressed specifically by any research work. However, the analysis of certain related works can offer certain guidance on the matter. For instance, [212] proposes an extension of this protocol, e-SCP-ECG+, to be included in health monitoring systems, permitting the inclusion of information about positioning, allergies, and five additional biomedical signals: noninvasive blood pressure (NiBP), body temperature (Temp), Carbon dioxide (CO<sub>2</sub>), blood oxygen saturation (SPO<sub>2</sub>), and pulse rate. The way in which it defines new sections and tags and implements software components can be adapted to the purpose of enhancing the security of the protocol. In addition, there are relevant works about ECG frameworks addressing security, although not integrating it into the standard. [213] defines a proposal of protocol stacks — depicted in Figure 2.5, which includes SCP-ECG, MFER, HL7 and may also include X73PHD — to be implemented by the entities in a m-Health network. However, it can be observed that in this proposal all the security relies on the physical layer in the communication between the sensor device (PHD) and the gateway (CD) and that the authenticated access to the encrypted data (AAA) is defined out of the standards. Furthermore, the files are not digitally signed. Similarly, [214] depicts a workflow where ECG files in SCP-ECG, HL7 aECG and XML Mortara formats are encrypted with a secure, password-derived — AES-256 — session key and sent to a central mailbox via secure Simple Mail Transfer Protocol (SMTP with SSL/TLS), where it is forwarded to the reviewer through secure Internet Mail Access Protocol (IMAP with SSL/TLS). Again, the files are not digitally signed, there is no definition of access control policy or at least a robust key management. Regarding this issue, [215] depicts an ECG framework whose security components include not only AES encryption but also privacy protection and access control (based on eXtensible Access Control Markup Language [216] — XACML — and SAML). Finally, [217] defines a 12-lead ECG telemedicine service with enhanced security and privacy protection, based on [Windows Azure](#). To safeguard the ECG data in the cloud, this framework includes

authentication for the use of Web roles and Worker roles, data encryption during message communications among roles, and ECG file encryption and verification while ECG reports are retrieved in storage accounts and database. In addition to this, ECG files are transmitted via SSL based HTTP (HTTPS) where ECG files are protected by certificate based encryption and verification.

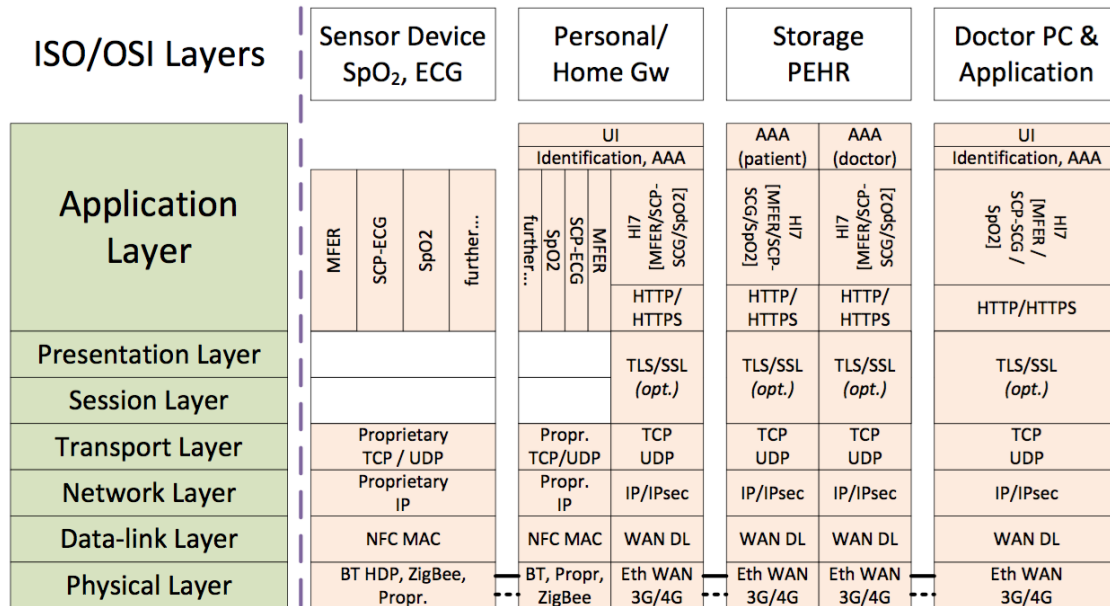


Figure 2.5: Stack proposal for secure health monitoring, according to [213].

Regarding X73PHD, several publications address to certain — albeit different — extents the enhancement of the X73PHD security. [218] recommends the symmetric encryption, based on AES, of the measurements contained in PrstApdu frames and evaluates its cost — the transmission delay grows from 18 to 26ms. However, a key management policy is not defined. [219] recommends the use of NFC as a reliable and convenient out-of-band pairing method when using Bluetooth as transport technology for X73PHD communications — being this a peripheral enhancement, since the standard is independent from the transport technology. [220] proposes the joining use of Universal Plug and Play (UPnP) and IEEE 11073 in home networks, establishing a UPnP *Device-Protection* service that controls the access of different concentrating devices — smart TVs, game centers, smartphones — to user’s personal information. Nonetheless, the agent-manager communication is not specifically protected and there are no means to distinguish the measurements from different users who may share agents. More focused on the standard, [221, 222] implement and discuss modified agent-manager association procedures, based on mutual challenge-response authentication — a certificate-based authentication method cannot be implemented since the agent has no direct means to check the validity of a certificate. The former uses the RSA2048 algorithm to perform digital signature — of timestamped

challenges —, which introduces high overhead, and implements USB Personal Healthcare Device Class for a secure transmission. The latter derives a biometric key from the user fingerprint, obtaining an insufficient 80% success rate. Another approach [223] focuses on low-powered PHDs. It proposes either including the sending date and time in the initial association frame of X73PHD and encrypting it partially — to hinder replay attacks and obtain certain privacy —, or encrypting the whole message and attach an authentication code — for integrity control. Nonetheless, still several attacks could thrive — e.g. user impersonation, devices hacking. The proposal in [224] handles both agent-manager authentication and encryption by means of a complex architecture, relying on either Device Profile Web Services — for hospitalary and domiciliary setups — or Bluetooth Health Device Profile — for high-mobility scenarios. This proposal includes global IDs for medical devices, the involvement of authorities beyond the manager, the administration of many cryptographic keys and the attachment of timestamps to verify their validity. However, it does not analyze the implications of this proposal on the X73PHD models and on its framework, and it lacks of details for an implementation based on its proposal. Moreover, none of the works mentioned consider fulfilling legal regulations (Section 2.4) or coordinating X73PHD with certain IHE profiles (Section 2.1.1), which would increase the usefulness of PHDs inside the healthcare ecosystem. On the other hand, [85] addresses both issues, but without proposing any specific security enhancement for the X73PHD and presenting a unique solution that limits the communications of X73PHD-compliant devices to PHR systems only. Finally, it is worth noting that the authors of [225] propose including remote controls in X73PHD and, from the perspective of security, they claim that the suitability of some use cases — e.g. configuration of pacemakers, drug pumps, insulin dispenser — should be analyzed.

As explained in Section 1.3.1, the Working Group 14 of DICOM has been very active in including security policies — e.g. encapsulation of DICOM files by means of cryptographic envelopes — and cryptographic elements — e.g. digital signatures —, some of them previously suggested in the literature [226, 227, 228], for the security enhancement of the standard. Therefore, it is foreseeable that more advances will be steadily included in the coming years. For instance, the integration of openID [229] for decentralized authentication of users accessing DICOM objects through HTTPS-based Web Access to DICOM Object (WADO [230]) services has already been addressed in the literature [231]. In addition, the implementation of QR-Code authentication for mobile DICOM image retrieval has also been proposed [232]. Similarly, Latch [233] might be integrated as a safety switch adding an additional level of security to the DICOM online services, switching them off when the user does not need them. Furthermore, it is likely that new forms of efficient anonymization (e.g. pseudonymization [234]) and encryption, such as quaternion-based encryption [235] or searchable encryption [236, 237, 238], which is intended for a very

efficient, robust and flexible privacy protection, are implemented by DICOM when these techniques become mature enough. Alternatively, there is also a variety of proposals to enhance the security and privacy of DICOM files through signal-based techniques, which strengthen the binding between the biomedical image and its metadata. As discussed in Sections 1.3.1 and 1.3.2, they can be of interest for certain security applications and scenarios — e.g. medical cooperative architectures. For instance, steganographic techniques have been proposed to embed silently into the biomedical DICOM image: the DICOM header [162] — in order to reduce the overall file size with very low quality loss —, a security-enhanced DICOM header [159] encapsulated in a digital envelope, or patient record information [239, 240]. Similarly, various watermarking approaches have been proposed for different purposes, such as the enhanced verification of integrity and authenticity in individual [176, 178] and multiframe DICOM files [241], the location of tampered areas in volumetric DICOM images [242] or the enhanced protection of patient information confidentiality [243, 244]. Furthermore, certain works propose combining several techniques to implement several security measures simultaneously in DICOM images, such as authentication and data hiding [177], watermarking of encrypted images [132] to enable integrity control while protecting privacy, or even joining lossless compression and encryption [245] to enable the embedding of contents for authentication, captioning (e.g. with EHR/DICOM metadata) with controlled access retrieval and tamper location.

## 2.2 Overview of major biomedical signal coding methods

This section introduces two widespread biomedical signal coding methods based on the wavelet transform (Section 2.2.1), which facilitate compression preserving the clinical content of: 1-D signals — SPIHT, Section 2.2.2 — and individual images and short videos (multiframe images) — the DICOM-compliant JPEG2000, Section 2.2.3. Finally, Section 2.2.4 presents relevant signal-based protection techniques, which may comply with these (and other) coding methods.

### 2.2.1 Wavelet transform overview

The wavelet transform comprises the coefficients of the expansion of a original signal  $x(t)$  with respect to a basis  $\psi_{w,n}(t)$ , each element of which is a dilated and translated version of a function  $\psi$  called the mother wavelet, according to

$$\psi_{w,n}(t) = \frac{1}{\sqrt{2^w}} \psi\left(\frac{t - n \cdot 2^w}{2^w}\right), \quad w, n \in \mathbb{Z}, \quad (2.1)$$

where  $\mathbb{Z}$  is the set of integers. Depending on the choice of the mother wavelet appropriately, the basis can be orthogonal or biorthogonal. The wavelet transform coefficients, given by

the inner product of  $x(t)$  and the basis functions

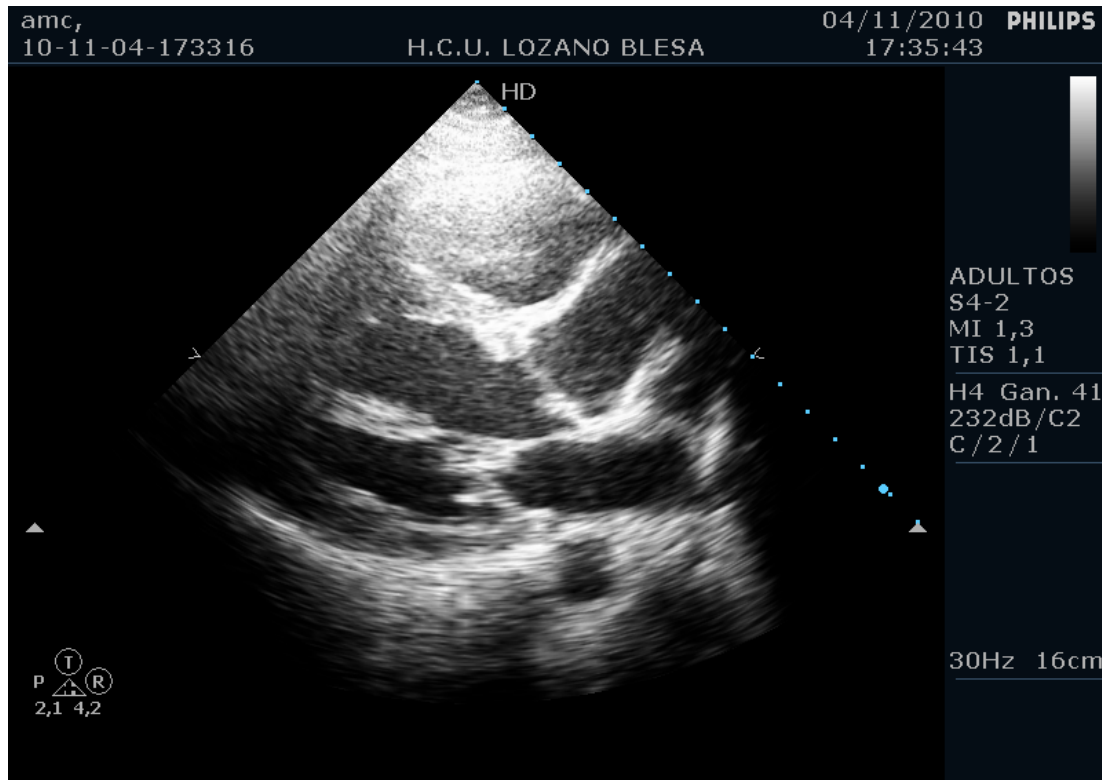
$$W(w, n) = \langle x(t), \psi_{w,n}(t) \rangle \quad (2.2)$$

comprise the time-frequency representation of the original signal. The wavelet transform has good localization in both frequency and time domains, having fine frequency resolution and coarse time resolution at lower frequency, and coarse frequency resolution and fine time resolution at higher frequency. Since this matches the characteristic of most signals, it makes the wavelet transform suitable for time-frequency analysis. In data compression, the wavelet transform is used to exploit the redundancy in the signal. After the original signal is transformed into the wavelet domain, many coefficients are so small that no significant information is lost in the signal reconstructed by setting these coefficients to zero.

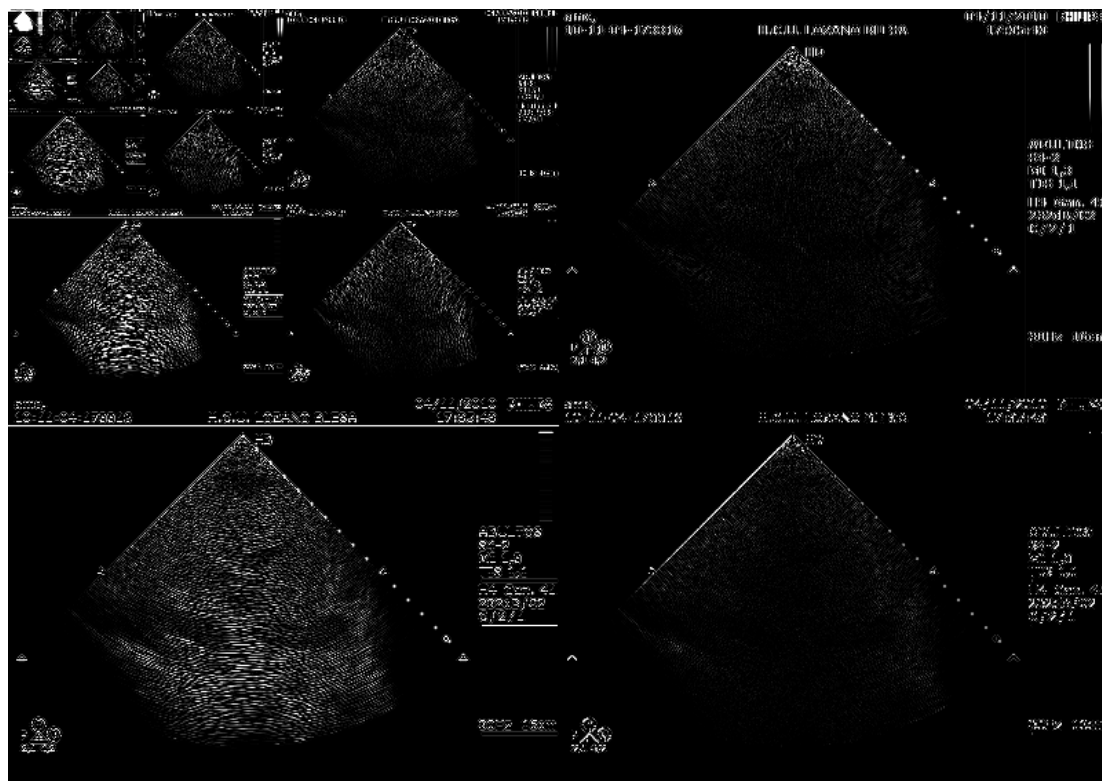
In digital signal processing, the fast-forward and inverse wavelet transforms are implemented as tree-structured, perfect-reconstruction filter banks. The input signal is divided into contiguous, non-overlapping blocks of samples called frames and is transformed frame by frame for the forward transform. Within each frame, the input signal is filtered by the analysis filter pair to generate low-pass and high-pass signals, which are then down-sampled by a factor of two. Then this analysis filter pair is applied to the downsampled low-pass signal recursively to generate layered wavelet coefficients. In different layers, the coefficients have different frequency and time resolution. In layer  $i$ , each coefficient corresponds to two coefficients in layer  $i + 1$  in the time domain. For the inverse transform, the coefficients in the highest layer are upsampled by a factor of two (zeros are inserted between successive samples), filtered by the low- and high-pass synthesis filter and added together to get the low-pass signal for the next layer. This process is repeated for all layers until the full size signal is reached to complete the inverse transform.

Similarly, the 2-D discrete wavelet transform [246] decomposes images into several scales (see the 5th-level decomposition of an echocardiogram represented in Figure 2.6), located in ordered regions of the transformed image, which host coefficients concentrating certain frequencies. This enables efficient compression —e.g. by means of SPIHT (Section 2.2.2) or JPEG2000 (Section 2.2.3)— since any entropy and/or run-length coding that exploits adequately the self-similarities of the quantized coefficients across different scales achieves high compression ratios. The main advantage of using wavelets over other transforms is its variable resolution: the higher frequencies, which correspond to details of the image, are represented with higher spatial resolution than the lower frequencies. The image is initially filtered by rows and columns with two filters, decimated by two and arranged in four subimages:  $LL, LH, HL, HH$  — this process is represented in Figure 2.7. The process is iteratively repeated, taking the last  $LL$  as input, until reaching the desired  $j$ -th decomposition level.





(a) Original image



(b) Wavelet decomposition

Figure 2.6: 5th-level wavelet decomposition of an echocardiogram image.



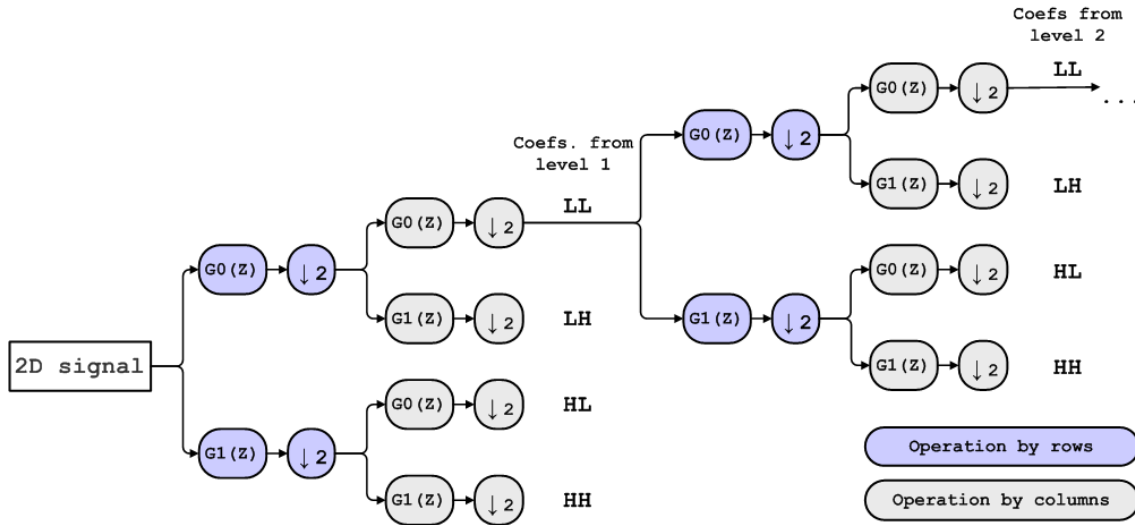


Figure 2.7: Calculation of the first wavelet decomposition levels of a 2-D signal.

In implementation, the number of layers/decomposition level of the wavelet transform, the filter pair and the frame size of the signal need to be appropriately selected. The number of layers determine the coarsest frequency resolution of the transform and should be at least four for adequate compression. The selection of different analysis-synthesis filter pairs, which correspond to different wavelet bases, is very important for obtaining high performance in the desired application: typically effective data compression, but also in associating information to the signal (e.g. by means of watermarking). Information for the design of perfect reconstruction filter pairs can be found in [247]. The frame size is taken to be a power of two that exceeds the number of layers. For 1-D signals, the frame should contain several periods of the biomedical signal, but should still be short enough for acceptable coding delay and memory usage.

### 2.2.2 SPIHT overview

SPIHT was firstly presented in [97] as an efficient method for coding wavelet coefficients (Section 2.2.1) in 2-D image compression. In [106] the algorithm was adapted to the one-dimensional (1-D) case and applied to ECG signals, revealing that it was very efficient in compression and in computation when compared with previous ECG compression methods. In addition to this, the SPIHT algorithm accounted with several desirable properties: multiresolution scalability, progressive lossy to lossless coding, compatibility with lossless entropy coding, low complexity (use of simple operators), moderate memory usage and symmetric coding-decoding. These features motivated the later extension of the algorithm to the 3-D [248] and 4-D cases [249], and its successful VLSI implementation in silicon for ECG real-time compression in low-power applications [250].

The principles of the SPIHT algorithm are partial ordering of the transform coefficients by magnitude with a set partitioning sorting algorithm, ordered bit plane transmission and exploitation of self-similarity across different layers. By following these principles, the encoder always transmits the most significant bit to the decoder.

### Temporal orientation trees

Basically the (1-D) algorithm uses a *temporal orientation tree* structure (Figure 2.8) to define the temporal parent-offspring relations in the wavelet domain. Every point in layer  $i$  corresponds to two points in the next layer  $i + 1$ , with the arrow indicating the parent-offspring relation. This definition is analogous to that of *spatial orientation trees* [97] for the 2-D case. Each node either has no offspring or two offspring. In a typical 1-D signal, most of the energy is concentrated in low frequency bands, so that the coefficients are expected to be better magnitude-ordered as we move downward following the temporal orientation tree to the leaves (terminal nodes).

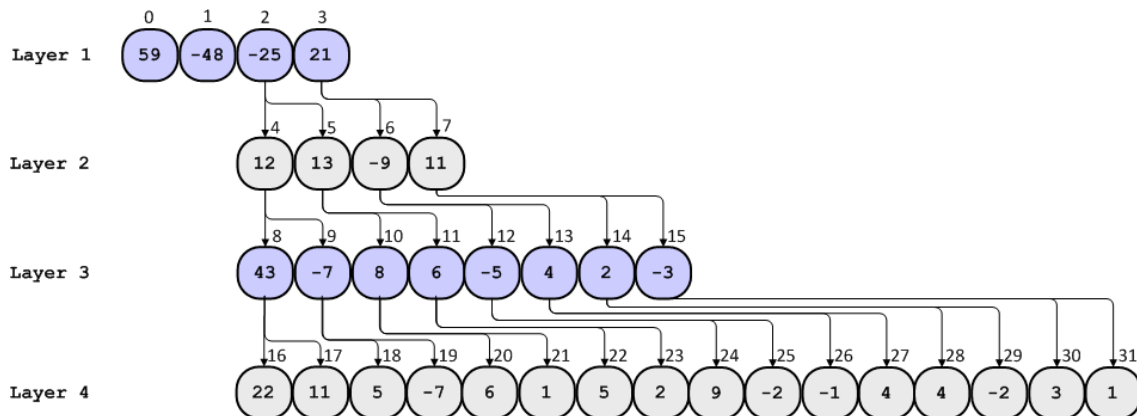


Figure 2.8: Subbands and spatial orientation tree of a SPIHT coding example.

### Set partitioning sorting algorithm

The same set partitioning rule is defined in the encoder and decoder. The subset of subband coefficients  $c_i$  in the subset  $T$  is said to be significant for bit depth  $n$  if  $\max_{i \in T} \{|c_i|\} \geq 2^n$ , otherwise it is said to be insignificant. If the subset is insignificant, a zero is sent to the decoder. If it is significant, a one is sent to the decoder and then the subset is further split according to the temporal orientation tree until all the significant sets are a single significant point. In this stage of coding, called the *sorting pass*, the indices of the coefficients are put onto three lists, the list of insignificant points (LIP), the list of insignificant sets (LIS), and the list of significant points (LSP). In this pass, only bits related to the LSP

entries and binary outcomes of the magnitude tests are transmitted to the decoder. In implementation, the entries in the LIP and LIS which have the same parent are grouped into an entry atom. For each entry atom in LIP, a pattern is estimated in both encoder and decoder to describe the significance status of each entry in the current sorting pass. If the result of the significance test of the entry atom is the same as the specified pattern, one bit is used to represent the status of the whole entry atom which otherwise had two entries and representation of significance by two bits. If the significance test result does not match the pattern, the result of the significance test is transmitted for each entry in the atom. Since most biomedical signals (e.g. ECGs) have periodic characteristics, the pattern is correctly estimated with high probability, so were able to save one bit frequently enough to give noticeable improvement in compression performance.

### Refinement pass

After each sorting pass, the significant coefficients for the threshold  $2^n$  are obtained, and then the  $n$ th most significant bit of every coefficient found significant at a higher threshold are sent to the decoder. By transmitting the bit stream in this ordered bit plane fashion, we always transmit the most valuable (significant) remaining bits to the decoder. The outline of the full coding algorithm is as follows:

1. *Initialization.* Set the list of significant points (LSP) as empty. Set the roots of similarity trees in the list of insignificant points (LIP) and insignificant sets (LIS). Set the significance threshold  $2^n$  with  $n = \lfloor \log_2(\max_i |c_i|) \rfloor$ .
2. *Sorting pass.* Using the set partitioning algorithm distribute the appropriate indices of the coefficients to the LIP, LIS, and LSP.
3. *Refinement pass.* For each entry in the LSP significant for higher  $n$ , send the  $n$ th most significant bit to the decoder.
4. Decrement  $n$  by one and return to step 2 until the specified bitrate or distortion is reached.

### An example of the SPIHT coding process

This section includes a simple example showing how the coding algorithm works. A four level wavelet decomposition of an input signal of length 32 produces the 32 wavelet coefficients distributed among the subbands as shown in Figure 2.8, with the arrows indicating the parent-offspring relationships in the temporal trees. The number in each cell is the value of the integer-rounded wavelet coefficient. The actions of the coding process are shown in Table 2.3. Below are the most important definitions:

Table 2.3: First steps of a SPIHT coding example

Step	Point or set tested	Output bit	Action	Control lists	Code bits accumulated
1				LIS = 2A, 3A LIP = 0, 1, 2, 3 LSP = empty	
2	c0	1	c0 to LSP	LIP = 1, 2, 3	1
		+		LSP = 0	2
	c1	1	c1 to LSP	LIP = 2, 3	3
		-		LSP = 0, 1	4
	c2	0	none		5
	c3	0	none		6
3	$D(c2)$	1	descending tests	LIS = 2A, 3A	7
	c4	0	c4 to LIP	LIP = 2, 3, 4	8
	c5	0	c5 to LIP	LIP = 2, 3, 4, 5	9
			changes of type	LIS = 3A, 2B	
	$D(c3)$	0	none	LIS = 3A, 2B	10
4	$L(c2)$	1	add new sets	LIS = 3A, 4A, 5A	11
	$D(c4)$	1	descending tests	LIS = 3A, 4A, 5A	12
	c8	1+	c8 to LSP	LSP = 0, 1, 8	13, 14
	c9	0	c9 to LIP	LIP = 2, 3, 4, 5, 9	15
			changes of type	LIS = 3A, 5A, 4B	
	$D(c5)$	0	none	LIS = 3A, 5A, 4B	16
	$L(c4)$	0	none	LIS = 3A, 5A, 4B	17
5				LIS = 3A, 5A, 4B LIP = 2, 3, 4, 5, 9 LSP = 0, 1, 8	
6			reduce threshold		
7	c2	1	c2 to LSP	LSP = 0, 1, 8, 2	18
		-		LIP = 3, 4, 5, 9	19
	c3	1	c3 to LSP	LSP = 0, 1, 8, 2, 3	20
		+		LIP = 4, 5, 9	21
	c4	0	none	LIP = 4, 5, 9	22
	c5	0	none	LIP = 4, 5, 9	23
	c9	0	none	LIP = 4, 5, 9	24
8	$D(c3)$	0	none	LIS = 3A, 5A, 4B	25
	$D(c5)$	0	none	LIS = 3A, 5A, 4B	26
	$L(c4)$	1	add new sets	LIS = 3A, 5A, 8A, 9A	27
	$D(c8)$	1	descending tests	LIS = 3A, 5A, 8A, 9A	28
	c16	1+	c16 to LSP	LSP = 0, 1, 8, 2, 3, 16	29, 30
	c17	0	c17 to LIP	LIP = 4, 5, 9, 17	31
			remove c8 from LIS	LIS = 3A, 5A, 9A	
	$D(c9)$	0	descending tests	LIS = 3A, 5A, 9A	32
9	c0	1			33
	c1	1			34
	c8	0			35
10			reduce threshold		
...					

- **LIS** contains sets of wavelet coefficients which are defined by tree structures, and which had been found to have magnitude smaller than a threshold (are insignificant). The sets are designated by, but exclude the coefficient corresponding to the tree or all subtree roots, and have at least two elements.
- **LIP** contains individual coefficients that have magnitude smaller than the threshold.
- **LSP** points found to have magnitude larger than the threshold (are significant).
- $O(c_i)$  in the tree structures, the set of offspring (direct descendants) of a tree node defined by point location ( $i$ ).
- $D(c_i)$  set of descendants of node defined by point location ( $i$ ).
- $L(c_i)$  set defined by  $L(c_i) = D(c_i) - O(c_i)$ .
- Type A entry in LIS: the entry  $i$  represents  $D(c_i)$ .
- Type B entry in LIS: the entry  $i$  represents  $L(c_i)$ .

and explanations:

1. The largest coefficient magnitude is 59, so the threshold is 32. The LSP set is empty, the initial LIP are coefficients  $\{0, 1, 2, 3\}$  and initial LIS are coefficients  $\{2, 3\}$ .
2. *Sorting pass in LIP*: SPIHT begins to code the significance of individual coefficients in LIP.  $c_0$  is significant: a one is sent followed by a positive sign bit, and  $c_0$  is moved to the LSP.  $c_1$  is significant; a one is sent followed by a negative sign bit, and  $c_1$  is moved to the LSP. ( $1+$  represents positive significant,  $1-$  represents negative significant).  $c_2$  and  $c_3$  are both insignificant, so a zero is sent for each.
3. *Sorting pass in LIS*: After finishing the LIP, SPIHT begins to test the LIS (active entry indicated by bold letter). For type A entry, when an entry in LIS is significant, a one is sent. Then its two offspring are checked like an entry in the LIP. If  $L(c_i)$  is not empty, that entry is moved to the end of the LIS and changed to type B. If is empty, that entry is removed from the LIS. When an entry in the LIS is insignificant, a zero is sent. In this case, the type A  $D(c_2)$  is found significant, and split into offspring  $c_4$ ,  $c_5$ , and  $L(c_2)$ , which goes to the end of the LIS as type B.  $c_4$  and  $c_5$  are found to be insignificant, they are moved to the LIP and two zeros are sent.  $D(c_3)$  is insignificant, so a zero is sent.
4. For a type B LIS entry, if it is significant, a one is sent, add its two offspring to the LIS as type A, and remove that entry from LIS. If it is insignificant, a zero is sent. In this case,  $L(c_2)$  is significant, so a one is sent and the offspring of  $c_2$ ,  $c_4$  and  $c_5$  become roots of type A sets in the LIS, and  $L(c_2)$  (2B) is removed from the LIS.

$D(c4)$  and  $D(c5)$  are then tested as above with the actions given in the table.

5. *Refinement pass*: After the sorting pass. SPIHT begins the refinement pass. Each old entry of LSP (the coefficients which became significant under the last threshold) is checked. Send a one if it is significant under this threshold and reduce its magnitude by the current threshold. Since this is the first refinement pass, there are no old LSP entries. These new entries of LSP,  $c0$ ,  $c1$ , and  $c8$ , are reduced in magnitude by the current threshold of 32, so that their values become  $c0(27)$ ,  $c1(16)$ , and  $c8(11)$ .
6. *Sorting Pass in LIP*: Check the significance for LIP entries under threshold 16.  $c2$  and  $c3$  are significant and moved to the LSP, while  $c4$ ,  $c5$  and  $c9$  remain insignificant.
7. Reduce the threshold to 16.
8. *Sorting pass in LIS*: Check the significance for LIS entries under threshold 16.
9. *Refinement pass*: check old LSP members  $c0$ ,  $c1$  and  $c8$ , send their significance information, reduce the magnitude of significant old LSP entries and all new entries in LSP. Their values become  $c0(11)$ ,  $c1(0)$ ,  $c8(11)$ ,  $c2(9)$ ,  $c3(5)$ , and  $c16(6)$ .
10. Reduce the threshold to 8 and repeat sorting pass and refinement pass until the bit budget or quality requirement is reached.

In the decoder side, the same process is executed. The only difference is that the significance decisions found in the encoder — by comparing the coefficients to a threshold — are input to the decoder. The lists are initialized identically and formed in the decoder exactly as in the encoder. In the refinement pass, the threshold is added to the significant coefficients, instead of subtracted. The addition or subtraction of threshold is equivalent to adding or removing a bit in a bit plane representation of the coefficient's magnitude.

### 2.2.3 JPEG2000 overview

JPEG2000 is an image compression standard that uses the state of the art wavelet technology. It was created in 2000 by members of the Joint Picture Experts Group with the intention to solve most of the limitations of the original JPEG standard (created in 1992) based on the discrete cosine transform. The JPEG2000 algorithm provides an efficient representation and interchange of digital images with different characteristics (scientific, medical, rendered graphics, etc.), allowing different imaging models, e.g. client/server, real-time transmission, image library archival, limited buffer and bandwidth resources. JPEG2000 also provides low bit-rate operation with rate-distortion and improves the subjective image quality performance of the previous standard, JPEG. Although this standard is still not as widely used for natural images as its forerunner, it is widespread in medi-

cal imaging and included in the DICOM standard. According to the mean opinion score (MOS) of medical experts [251], this codec maintains good clinical quality at compression ratios up to 8-16 for magnetic resonance, ultrasound and X-ray images. Compared to JPEG, it presents a better image distortion-rate tradeoff and for an equal objective distortion (e.g.  $PSNR = 35\text{ dB}$ ), it obtains a higher MOS.

### JPEG2000 features

JPEG2000 has many features, which were not available in most of the previous image coding standards. They include:

- Excellent coding performance. It features superior rate-distortion and subjective image quality performance especially at low bit rates. This is useful in applications whereby file size or transmission time is critical.
- Lossless and lossy compression. It is capable of lossless compression, which is important to some medical imagery and image archival applications.
- ROI coding. It allows certain areas of an image to be encoded at higher fidelity. More information on this feature can be found in [252].
- Spatial and Signal-to-noise ratio ( $SNR$ ) scalability. It allows progressive recovery of images by resolution or quality.
- Good error resilience. It has added bitstream robustness to the presence of bit errors. In addition, its flexible file formats JP2 and JPX allow the handling of color-space information, metadata, and interactivity in networked applications as developed in the JPEG Part 9 JPEG 2000 Interactive Protocol (JPIP) protocol.

### JPEG 2000 encoder and decoder structure

As depicted in Figure 2.9a, the core structure of the JPEG2000 encoder follows a typical sequence of operations used in a transform coding scheme, which consists of transformation, quantization and entropy coding. The JPEG2000 encoder works as follows. First, the original image with unsigned data is DC-level shifted. Then, the component transformation can be carried out if the original image has multiple components. This procedure provides decorrelation among image components and hence improves compression efficiency. There are two component transforms available: one is reversible and may be used for lossy or lossless coding, while the other is irreversible and may only be used for lossy coding. Before proceeding further, it should be noted that the image components can be partitioned into tiles, which are rectangular non-overlapping blocks, and thus creating tile

components that can be compressed independently of each other.

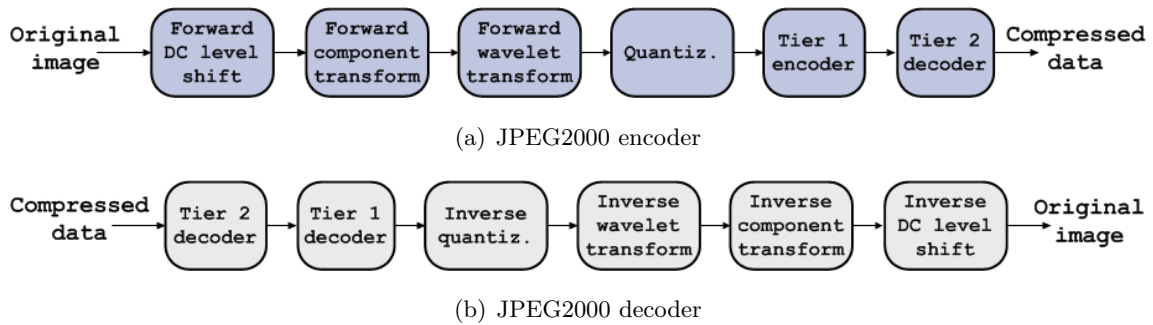


Figure 2.9: Processes of the JPEG2000 encoder and decoder.

Wavelet transform [253] (Section 2.2.1) may be performed on the tile components. In the lossy case, an irreversible Daubechies 9-tap/7-tap filter is employed, whereas in a lossless case, a reversible 5-tap/3-tap filter is used. The wavelet transform decomposes the tile-components into different decomposition levels, each of which contains a number of subbands filled with transform coefficients. Before entering into the entropy coding phase, the quantization process is carried out to reduce the precision of the transform coefficients. Note that for the lossless case, the quantizer is set to one, i.e. no loss in precision.

The remaining encoding process is grouped into two tiers. In the tier-1 encoder, the quantized transform coefficients associated with each subband are arranged into rectangular blocks called code-blocks. Then, a bit-plane coding technique with three coding passes is applied to each code-block, and the symbols that it produces are coded using an adaptive binary arithmetic coder. In the tier-2 encoder, the inclusion and the order of appearance of bit-plane coding passes along with the actual coding pass data are assembled together to form the final compressed data. Finally, as regards to the JPEG 2000 decoder, its core structure is illustrated in Figure 2.9b. It basically reverses the processes of the encoder.

#### 2.2.4 Related publications on signal-based protection

This section extends the content of Section 1.3.2, which explains the fundamentals and types of steganography and watermarking and discusses its potential security applications and current shortcomings in the m-Health context.

Regarding embedding techniques, a categorization according to the embedding method is established in Section 1.3.2. The approaches working in the temporal or spatial domain may replace certain least significant bits of the signal [158, 159], change magnitude levels, modify the difference between adjacent samples [254, 240], perform quantization index



modulation [255], multiple base notational or embedding based on prediction. The methods operating in transform domains choose mainly the Discrete Cosine Transform (DCT) [256] and the Discrete Wavelet Transform (DWT) [257], while the proposals working in compressed domains usually choose JPEG [160, 258] and SPIHT [259] bitstreams. As regards to alternative embedding methods, the approaches working with histograms that are focused in reversible transformations [161, 260] have good presence in m-Health, while examples of spread-spectrum techniques [261] and model-based methods [262] are infrequent.

With respect to medical image watermarking techniques (MIW), they may be classified as non-reversible — producing a permanent distortion on the image —, operating mainly in the RONI — to minimize image distortion —, reversible techniques — which can recover the original image after removing the watermarks —, and zero watermarking — constructing watermarks based on the main features of the images in order to avoid the embedding step which causes image distortion. The following paragraphs summarize and classify different efforts — intended for enhancing the security of biomedical images or that could be adapted to this purpose — in the four categories.

The non-reversible MIW techniques can perform the watermark embedding in different domains. The simplest approaches work in the spatial domain, mainly performing the replacement of least significant bits (*LSB*) in pixels [227, 171, 241] to embed fragile watermarks, although there are also proposals to host robust watermarks by using more significant bits [263, 264, 265]. Moreover, the transformation of the image prior to watermarking can yield interesting properties. For instance, the use of regions of different amounts of energy in transform domains allows the embedding of multiple (robust, semifragile and fragile) watermarks in the same image [266, 267, 268]. There are watermarking-based methods using the discrete cosine transform (DCT) [269, 160, 270] — thus, which are compliant or could be adapted to the JPEG codec —, using discrete wavelet transforms (DWT) [271, 272, 267, 268, 273, 274, 275, 276] — thus, which are compliant or could be adapted to the JPEG2000 codec —, and others, such as the discrete wavelet packet transform [277] or wave-atoms [278]. Furthermore, the robustness against geometrical transformations, such as rotation-scaling-translation (RST), is also addressed — to different extents — by certain watermarking techniques — see a survey in [279]. There is a good variety of methods to achieve this enhanced robustness, such as with the use of the Fourier-Mellin transform [280], with log-polar coordinates [281], with the Radon transform [282, 283], with the S-Radon transform [284] (which is invariant to shearing), with Zernike moments [285, 286], with singular value decomposition (SVD) [287, 288], and with joint approaches such as DCT-SVD [289], DWT-SVD [290, 291], Zernike-SVD [292], or even DCT-DWT-SVD [293, 294]. Alternatively, the compressed domain can also be used for

watermarking, usually exploiting the theory from compressed/compressive sensing [295]. There are examples with SPIHT [108], JPEG [296], JPEG2000 [297], and even encrypted JPEG2000 images [298]. It is also worth noting that although the choice of the embedding domain is very relevant in watermarking, the procedure to target the most appropriate pixels/coefficients — and inside them, the most adequate bits for watermarking — is also an important factor to balance the tradeoff between robustness and imperceptibility. Certain works focus on the optimization of this procedure, e.g. by means of fast neural networks [299], particle swarm optimization [274], differential evolution [300], or by learning from the coefficient relations established by compression algorithms like SPIHT [301].

The MIW techniques that distinguish the *ROI* and *RONI* of the image prior to watermarking are intended to minimize the interference of the watermarks with the clinical content of the image. Regarding the embedding domain, any of the listed above (DWT, DCT, SVD, joint approaches, etc.) would be suitable, since these techniques only require specifically to perform the corresponding spatial separation between *ROI* and *RONI* — before or after the domain transformation. A common practice is embedding robust watermarks in the *RONI* area surrounding the *ROI* [172, 302, 303, 177, 244, 245] to try to avoid its deletion if the image is clipped. Nevertheless, some works propose embedding in random locations [176, 304, 305] to increase the capacity. As regards to embedding — total or partially — in the *ROI*, this practice is only allowed for fragile watermarks — e.g. for integrity control —, since the distortion caused is minimal.

The MIW reversible techniques — see a recent survey in [306] — were first introduced in [174], and since then a variety of methods have been developed. Difference expansion, an integer wavelet transform with high redundancy, was proposed early on in [307], obtaining low-distortion and high-capacity. This scheme has been adapted for several uses, such as the embedding of patient data in the *ROI* of DICOM images [177] — for enhanced robustness to image clipping without image distortion. Histogram operations, such as circular interpretation of bijective transformations [308], are also an effective manner to implement reversible watermarking with notable endurance to lossy compression. The addition of a virtual border where patient data is inserted in the *LSB*, at the cost of increasing the image size, has also been proposed [309]. The use of an estimator signal to determine which pixel blocks can embed information was proposed in [310], further used to embed a digest of the knowledge associated to the image [311], and refined in [178] by introducing a random location signal for security and implementing tamper detection and location. Furthermore, this work was extended to volumetric images in [242]. Similarly, [312] depicts an effective tamper location watermarking based on partitioning an authentication area into small regions in a hierarchical manner, and [243] proposes the reversible embedding of R-S-vectors and patientID to provide authentication and confidentiality.

Zero-watermarking techniques were first proposed in [313], and since then a few works that adapt the research from non-reversible MIW have been proposed —see a recent review in [175]. As examples of these adaptations, there are approaches working in the space domain [314, 315, 316], in transform domains [313, 317, 318, 319, 320], with image moments resistant to certain geometrical transformations [321], with decompositions of the image (e.g. SVD) [322], with principle components [323], and hybrid approaches [324, 325, 326, 327, 328, 329]. Regarding techniques in the space domain, some of them propose using most significant pixel bits [314], while others prefer high order cumulants [315] or scale invariant features [316]. With respect to transform domains, it has been proposed associating watermarks to selected high magnitude coefficients from the DCT domain [313, 317], to the low frequency coefficients from the DFT [318] and DWT domains [319], and using the 3D-DCT [320] to work with biomedical volume images. Finally, there are several hybrid approaches, such as combining the use of DCT and DWT [324], DWT and SVD [325], the phase feature from low to middle bands in DFT domain and two generalized Radon transformations [326] —to identify the rotation and scaling parameters of geometrical image transformations—, Contourlet transform and SVD [327] —for unambiguous authentication of medical images—, log-polar mapping and DWT [328], and log-polar mapping, SIFT and DWT [329].

## 2.3 Overview of transport technologies in the m-Health architecture

M-Health architectures require that their transport technologies have support for both “reliable” (i.e. confirmed) and “best-effort” (i.e. unconfirmed) bidirectional transport services. Those transport profiles containing only unidirectional transport services or only best-effort transport services are not eligible to be used in standards like X73PHD (Section 2.1.2). In addition, some specific features are required to be present in the selected transport technology. If they are not, it is possible to build a convergence layer (also referred to as “shim” layer) to meet the required characteristics.

Some transport technologies already count with a specialization to handle healthcare data. Such technologies are: Universal Serial Bus Personal Healthcare Device Class (USB-PHDC [330]), Zigbee Health Care Profile (ZHCP [331]) and Bluetooth Health Device Profile Multi-Channel Adaptation Protocol (BT HDP/MCAP [332]). Besides, there are currently ongoing efforts to develop X73PHD-compliant devices with Bluetooth Low Energy (BLE [333]) as transport technology. Additionally, some other transport technologies — namely, Near Field Communication (NFC [334]), Wireless Fidelity (Wi-Fi) Direct [335] or Certified Wireless Universal Serial Bus (WUSB [336]) — could theoretically be used

and therefore are considered in this Thesis as well. A complete review of them, including features such as coverage, topology, frequency band or data rate can be found in [337].

Table 2.4: Security features of transport technologies eligible for m-Health architectures

	Transport standard	Secure device pairing/joining	Frame/packet encryption	Frame/packet authentication	Additional security
Already-in-use technologies	USB-PHDC	-	-	-	Physical security
	ZHCP	Trust center authorizes new devices using out-of-band methods	128-bit AES	CCM* mode = Counter mode CBC-MAC	Freshness (frame counter), mesh privacy (network key) and device2device privacy (link keys)
	BT HDP/MCAP (CORE v2.1 + EDR)	Secure Simple Pairing: Elliptic Curve Diffie-Hellman (ECDH) + passkey entry or Out-Of-Band (OOB) protocol	E0 (LFSR-based)	E1, SAFER+ based	-
Eligible technologies	BLE	OOB protocol (no ECDH currently)	128-bit AES	CCM Mode	Device address change on a frequent basis, packet counter
	NFC	-	-	-	Physical security (10 cm from devices)
	WiFi Direct	WiFi Protected Setup (WPS) with PIN, PBC, NFC or USB	WPA2 = 128-bit AES	CCMP Mode —CCM derived—	Packet counter, access control with layer management
	Certified Wireless USB	Out-of-band first association: numeric or cable + Diffie Hellman	128-AES	CCM	Support for one-time association and easy revocation

The security features of these transport technologies are summarized in Table 2.4. From this review, it can be observed that USB-PHDC and NFC are particular cases, since their security relies only on the difficulty to access the physical medium (the cable connecting the two devices or a radius of 10 cm around them) and on the foreseeable security on the application layer. In the rest of the cases, the device pairing or joining (when there is a network architecture) is carried out by a user or by an authority (e.g. a trust center), usually by means of out-of-band method [338, 339], such as pushing a button (PBC), introducing a PIN/passkey in one or in both devices, or enabling NFC and approaching them.

Furthermore, there is some derivation or negotiation of the session key(s) for encryption, e.g. using the protocol Diffie-Hellman (DH) [340] or the more advanced Elliptic Curve Diffie-Hellman (ECDH [341]). In the case of network topologies, there may be different session keys so that each device can either communicate only with another one (e.g. link keys in ZHCP) or broadcast frames/packets to all of them (e.g. network key in ZHCP). The encryption with the session key(s) provides privacy, and it is performed with 128-bit Advanced Encryption Standard [342] (AES) in CBC mode [343], to avoid the dictionary attack. Except in BT HDP/MCAP, which uses a stream cipher based on Linear Feedback Shift Registers (LFSR [344]). The ciphers use Message Authentication Codes (MAC) to authenticate the packets/frames and counters (CCM/CCM\*/CCMP [345] operation modes) to prevent replay attacks. Only BT HDP/MCAP uses a different approach, a SAFER+ [346] based authentication. Finally, some technologies enable additional security features, such as device address change to difficult tracking (BLE), access control in conjunction with layer management (WiFi Direct), or support for one-time association and easy revocation (WUSB).

## 2.4 Legal regulations

The security requirements of personal health information (PHI) are usually defined by strict ethics and legislative rules to which concerned entities must adhere. There are several guidelines and standards for protecting PHI. In the first place, it is worth highlighting the ISO 27799 [347], a basic international standard which specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this international standard, healthcare organizations and other custodians of health information will be able to guarantee a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability (CIA) of PHI. ISO 27799 relies on the implementation of ISO/IEC 27002 [348], which depicts a code of practices for the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

In addition to this, some countries count with their own security and privacy policies. It is worth highlighting two regulations from US, the Health Insurance Portability and Accountability Act (HIPAA) [48] and the Code of Federal Regulations number 45 (CFR 45) [349], and two regulations from Europe, the European Directive 95/46/EC [350] and the General Data Protection Regulation (GDPR) [50]. These four regulations are expressions of such constraints. The HIPAA Privacy Rule regulates the use and distribution of PHI to entities linked with the patient in order to facilitate treatment, payment or health

care operations. It mandates disclosing only the minimum necessary information required to achieve a certain purpose (primary or secondary authorized by the the patient) and keeping track of disclosures of information and document privacy policies and procedures. Complementarily, the purpose of the HIPAA Security Rule is to identify and adopt national standards — including requirements and addressable implementation specifications — for safeguards to protect the CIA of electronic PHI. Regarding CFR 45 (part 164: security and privacy), this regulation pursues guaranteeing the CIA of all electronic PHI that a covered entity or business associate creates, receives, maintains, or transmits. To achieve this purposes, it requires protection against any reasonably anticipated threats or hazards to the security or integrity of PHI and against any reasonably anticipated uses or disclosures of PHI that are not permitted. With respect to Directive 95/46/EC, it regulates the processing of personal data — any information relating to an identified or identifiable natural person — within the European Union. This regulation establishes that the processing of PHI can only be done under conditions of transparency, specified explicit and legitimate purposes and proportionality, i.e. data shall be adequate, relevant and not excessive with respect to the purpose for which it is collected and/or further processed. Finally, as regards to the GDPR —whose adoption is expected by 2017—, it has been designed as the replacement for the obsolete Directive 95/46/EC. This regulation takes into account the developments that shape the current technological panorama — e.g. cloud computing, social networks. Some of the GDPR key points include the extension of privacy obligations to foreign companies processing data of EU residents, the harmonization of data protection regulations throughout the EU, strict responsibility and accountability duties, legal obligation to notify data breaches, right of the data subject to request erasure and right to request a copy of his/her data in a format usable and ready to be to transmitted to another processing system.

The legislative rules, as mentioned above, are based on strict ethics that give rights to the users/patients and duties to the health professionals and technicians. The biomedical standards (e.g. ISO/IEEE 11073, SCP-ECG, DICOM, etc.) and their associated technical frameworks can play a crucial role in the development and implementation of security and privacy protection features. Although certain aspects of these regulations cannot be addressed by the biomedical standards (e.g. the administration of backups, the protection and control of physical media, or the notification of data breaches), important aspects of security and risk management in the context of information security can be implemented by biomedical standards in order to enhance the compliance with these regulations. In brief, the following security requirements can be demanded to the biomedical standards and their surrounding frameworks:

- All concerned entities (e.g. PHDs, CDs, PACS in hospital or clinic, and consultants/

specialists at distant places) shall have appropriate levels of security and privacy.

- CIA of all PHI have to be ensured during measurements/test acquisition session, consultation process, and information transmission, processing, management, and preservation.
- In all domains and scenarios, proper authorization process must be employed through transmission and access controls.

On the other hand, the security concept derived from the regulations mentioned above can be established through different stages. The major stages make a cycle including: (1) initial threat analysis/risk assessment of the scenario — Section 2.5, (2) determination of appropriate level(s) of security — Section 2.6, (3) establishment of the security policy — Sections 3.1, 3.3, 4.1, 4.4, 4.5 and 4.7, (4) final threat analysis/risk assessment — Sections 3.2.1, 3.4.1, 4.4.1 and 4.7.8 — and (5) discovery or publication of new threats, which implies going back to (1).

The initial risk assessment helps to determine the expected threats from the entities involved in the m-Health context (e.g. PHDs, CDs, etc.). The determination of the appropriate level(s) of security shall include all entities involved in the m-Health context and may depend on the type of m-Health domain or application. The establishment of the security policy deals with either reducing the probability of occurrence of the threats or reducing the damage if an adverse event is unavoidable. This includes the selection of suitable measures that reduce the risks to a tolerant level. Some examples of such measures are the protection of configurations, communications, stored data and tests; the identification and authentication of users and devices; the implementation of access controls, audit trails audit and accountability systems; etc. As regards to the final risk assessment, it includes the evaluation of the selected security measures, examining the cost-effect relationship — Sections 3.2.2, 3.2.3, 3.4.2, 4.2 and 4.6 — as well as analyzing any further risk or limitation — see Sections 3.2.4, 3.4.3, 4.4.2 and 4.7.9. The security enhancement cycle ends when certain new threats appear, such as the discovery of vulnerabilities affecting implemented security algorithms or the inclusion of new, non-secure entities or protocols in m-Health frameworks, which indicates the beginning of the next cycle.

## 2.5 Risk assessment of the m-Health architecture

A typical m-Health architecture, as the illustrated in Figures 1.1 and 2.11-A, involves several entities that need to cooperate in order to acquire and transmit the biomedical measurements (signals and/or tests) of the user. Although the transport technologies used to communicate between PHDs and CDs may implement security (Section 2.3), there is

uncertainty about the actual identities of the entities involved (e.g. users, PHDs, CDs, medical systems, etc.). This extends to a lack of reliability about the provenance and integrity of commands and data transmitted along this framework. Various threats may cause loss, corruption or theft of the measurements, thus endangering the health and the privacy of the user. To address these issues, the hot spots in m-Health architectures shall first be analyzed. The following potential risks have been compiled from three reference publications on the matter; [351] covers the topic of security in e-governance, [352] specifically deals with the e-Health scenario and [353] with the transmission chain of a medical health monitoring system (the m-Health scenario).

- **Users:** If the PHD does not support personal ID attributes (e.g. personID in X73PHD agents), it is hard or impossible to differentiate the measurements of different users. When these attributes are supported, simple methods to distinguish users (e.g. a push button, a keyboard) do not authenticate them. Even if some user authentication method is implemented, an attacker may try to impersonate users by using open sessions or stolen credentials — e.g. shoulder surfing users' passwords, stealing the user access token, faking the biometric recognition of the victim. If the purpose is causing denial-of-service (DoS), introducing wrong passwords several times might be enough. Finally, those measurements of the user acquired outside the hospital and not digitally signed may later be repudiated by medical entities.
- **Personal health devices:** A counterfeit/hacked PHD may forward the gathered measurements and/or the user identity credentials to an unauthorized device. Besides, if the PHD stores the measurements provisionally (e.g. in the case that the connection with the concentrator device is temporarily unavailable), an attacker may attempt to establish a local access to retrieve them — from the disk, from cache or from the RAM memory. A third possible misconduct, which may affect the user follow-up, is to reprogram the PHD to deliver fake measurements when using it. Finally, in setups with several PHDs and CDs (e.g. hospitals), a PHD may wrongly send the measurements of a user to a CD that was not intended to receive them.
- **Personal health devices — concentrator devices communication:** This is especially sensitive in the case of wireless technologies because of the easy access to the physical medium, which brings several opportunities to attackers. First, they may attempt to inject their own commands in the PHD-CD communication and eavesdrop the exchanged frames to obtain measurements. If the communication relies on a secure transport technology, frames are encrypted and authenticated. Cracking the keys used for encryption, authentication or signature usually requires a very significant effort, but less so when the keys are too short, used over long periods of time or for several purposes at the same time (e.g. encryption and signature). In the absence



of counters or timestamps, attackers may perform replay attacks to inject encrypted frames that have been eavesdropped and it is known that correspond to certain commands. Another possibility is to perform a man-in-the-middle attack: the attacker associates with the PHD and CD, even negotiating encryption with each one, to inject commands and obtain measurements without restrictions. On the other hand, injection of noise can be used to disturb the communications and cause DoS.

- **Concentrator devices:** A counterfeit/illegitimate CD may attempt to associate to one or several PHDs to obtain both measurements that they store and measurements that they will acquire in future sessions. Besides, a rightful CD temporarily storing measurements may also be a target of hacking attacks (e.g. code injection) to corrupt those data, or to steal the data via local access — from the disk, from cache or from the RAM memory. Finally, it must be guaranteed that the access to the acquired measurements is limited to authorized users (e.g. the physicians that supervise a patient) and systems.
- **Concentrator devices — health system communication:** Typically by means of the Internet or mobile networks (e.g. 4G). Information transmitted at this point is very sensitive because it may include data from different PHDs. The main threats at this point are the impersonation of a HS to retrieve measurements from rightful CDs; the impersonation of CDs to deliver fake measurements to rightful HS; and the use of weak encryption in rightful transmissions, which facilitates eavesdropping. Since the information to be exchanged may be formatted according to different protocols — e.g. HL7, CEN/ISO 13606 [83] —, specific protection measurements provided by those protocols shall be considered. Otherwise, at least standard protection of the communications — e.g. by means of TLS [207] (transport level) or IPsec [354] (IP level) — shall be implemented.
- **Health system and administrator.** The reliability of the measurements received from PHDs/CDs and their suitable delivery to the intended professionals (physicians, researchers, etc.) are the main security issues faced by these entities. For the former, the identification of the patient to whom the measurements belong (and of the devices that acquired and forwarded them) and the verification of its integrity are essential requirements. For the latter, the administration of a robust role-based access control and the management of audit trails.

## 2.6 Guidelines for the security enhancement of the m-Health architecture

This section presents the guidelines proposed to enhance the security of m-Health architectures, in order to prevent the threats analyzed in Section 2.5, taking into account the background introduced in Sections 2.1-2.4. The contents included in this section are represented in Figure 2.10, surrounded in red. Particularly, Section 2.6.1 proposes a global, layered structure adapted to the features of different m-Health applications and Section 2.6.2 translates these layers into — already-existing and new — IHE profiles, some of them involving user authentication elements. Section 2.6.3 specifies the cryptographic recommendations for this proposal, Section 2.6.4 draws a way to integrate signal-based protection — keytagging — in this structure and eventually Section 2.6.5 analyzes the implications of this proposals for IHE and its profiles.

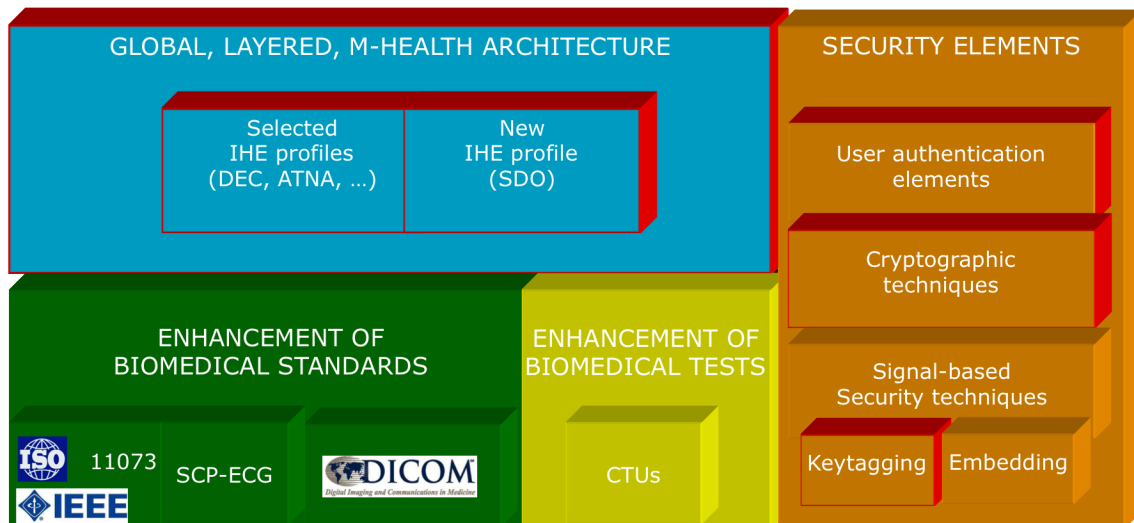


Figure 2.10: Building blocks for a secure, cost-efficient, m-Health architecture. Contents addressed in Chapter 2 surrounded in red.

### 2.6.1 Additive, layered structure

M-Health applications, often grouped in the domains of Health and Fitness, Independent Living and Disease Management, require different levels of security and interoperability with healthcare systems (Section 2.1.1). Furthermore, in a real-world market, users expect to have a choice ranging from cheap PHDs and CDs (intended only for basic home monitoring) to increasingly more expensive devices (those which include more dynamic and secure uses). An additive, layered approach is thus a reasonable and cost-effective

manner of providing varying, enhanced security and interoperability levels for different m-Health applications in a gradual manner. The following bottom-up layered structure would provide a specific solution for the applications of the different domains—and its associated PHD specializations, see for instance Section 2.1.2— within a general policy.

- Layers 0.x — intended for simple applications (e.g. basic monitoring) not requiring integration with PHRs, EHRs, alert managers or CDSS—and thus with low security demands.
  - Layer 0 — to be used when taking health measurements in cabled setups.
  - Layer 0.5 — to be used when taking health measurements in wireless setups.
- Layers 1.x — intended for applications which may require integration with PHR systems and alert managers (typically belonging to the domains of Health, Fitness and Independent Living)—and thus with medium-high security demands.
  - Layer 1.0 — to be used when users own their personal devices/equipment.
  - Layer 1.5 — to be used when users share the devices/equipment.
- Layers 2.x — intended for applications which may require integration with EHR systems, alert managers or CDSS (typically belonging to the Disease Management domain)—and thus with high-very high security demands.
  - Layer 2.0 — oriented to patient emergency monitoring and in-hospital care.
  - Layer 2.5 — intended for patient remote monitoring, follow-up and laboratory tests.

It is worth noting that only the security measures and interoperability capabilities of each layer have been fixed. The examples of assignation of specific m-Health domains to the Layers, however, are illustrative. Any user would be able to buy a higher or lower device, according to their needs or the requirements of the specific domain or scenario.

As depicted in Figure 2.11-A-B, the implementation of these layers would not conflict with the already-existing interoperability between PHDs and CDs (e.g. driven by means of X73PHD), since a CD would still be able to associate and operate with one or more PHDs simultaneously. The only restriction added is that the layer established for an application needs to be supported by the user, PHD(s) and CD involved in the test(s) acquisition session. To give an example, if the user uses an identification method which is valid up to Layer 2.0, the PHD is compliant up to Layer 1.5 and the CD is compliant up to Layer 2.5, they can all work together using up to Layer 1.5—therefore, this setup would not be appropriate for Disease Management applications. It is also worth noting that there would be five different ways of accessing the tests in the CD. In Layers 1.0+,

the administrator —that is the user in Layer 1.0— would be able to access all the tests any time and the automated online processes (e.g. warnings if some measurement are abnormal) as they reach the CD —after validating and decrypting them. Besides, each user would be able to directly access his/her stored tests whereas authorized professionals (e.g. trainers, physicians) would be able to access the tests of certain users for professional use (e.g. training monitoring, follow-up of a patient). Additionally, in Layers 2.0+ automated offline processes (e.g. monthly analysis of measurements) would be able to access protected tests stored in the CD after it associates with the PHD(s) that acquired them.

### 2.6.2 IHE profiles in each layer

A proposal for the implementation of the layers depicted in Section 2.6.1 by means of the IHE profiles introduced in Section 2.1.1 is summarized in Table 2.5. The entities of the m-Health framework that implement each of these profiles are illustrated in Figure 2.11 —they are connected by arrows labelled with the profile name. In the first place, it is worth highlighting that there is a need for a new IHE profile, tightly bound to ISO/IEEE 11073-20601 and called Secure Device Observation (SDO), whose main aim is providing appropriate levels of security in the PHD-CD association, configuration and operation to enable the secure acquisition of user measurements/tests (DEC), alerts (ACM) and waveforms (WCM). The security countermeasures defined by SDO, intended to minimize the risks analyzed in Section 2.5, may be divided into several components. There is a component dedicated to challenge-based PHD-CD authentication, CBA, which enhances the proposals in [221, 222, 224]. In addition, another component addresses the secure setting and renewal of cryptographic elements, SRC, in order to hinder key stealing and/or cracking. Furthermore, the SEC component implements secure communications (encrypted and authenticated) and the UID component carries out user ID capture, so that this is attached with the user's measurements/tests to prevent their loss. Additionally, the CMA component controls the measurements acquisition to prevents user impersonation and acquisition of measurements/tests by unauthorized PHDs and/or CDs. Moreover, the MV component verifies that the measurements/tests come from a rightful PHD. In addition, the UDS component guarantees that the user's DS is attached with the user's measurements/tests to prevent their repudiation by medical entities that did not acquired them. Complementarily, the SST implements secure standard storage to hinder the stealing of measurements or their corruption by means of local access. Finally, there is also an optional component for strengthening the security of measurements/tests through signal-based protection methods, SBP, which may be considered as a complement to the protection provided by cryptography and authenticators. An example of implementation of the SBP component is depicted in detail in Section 2.6.4.



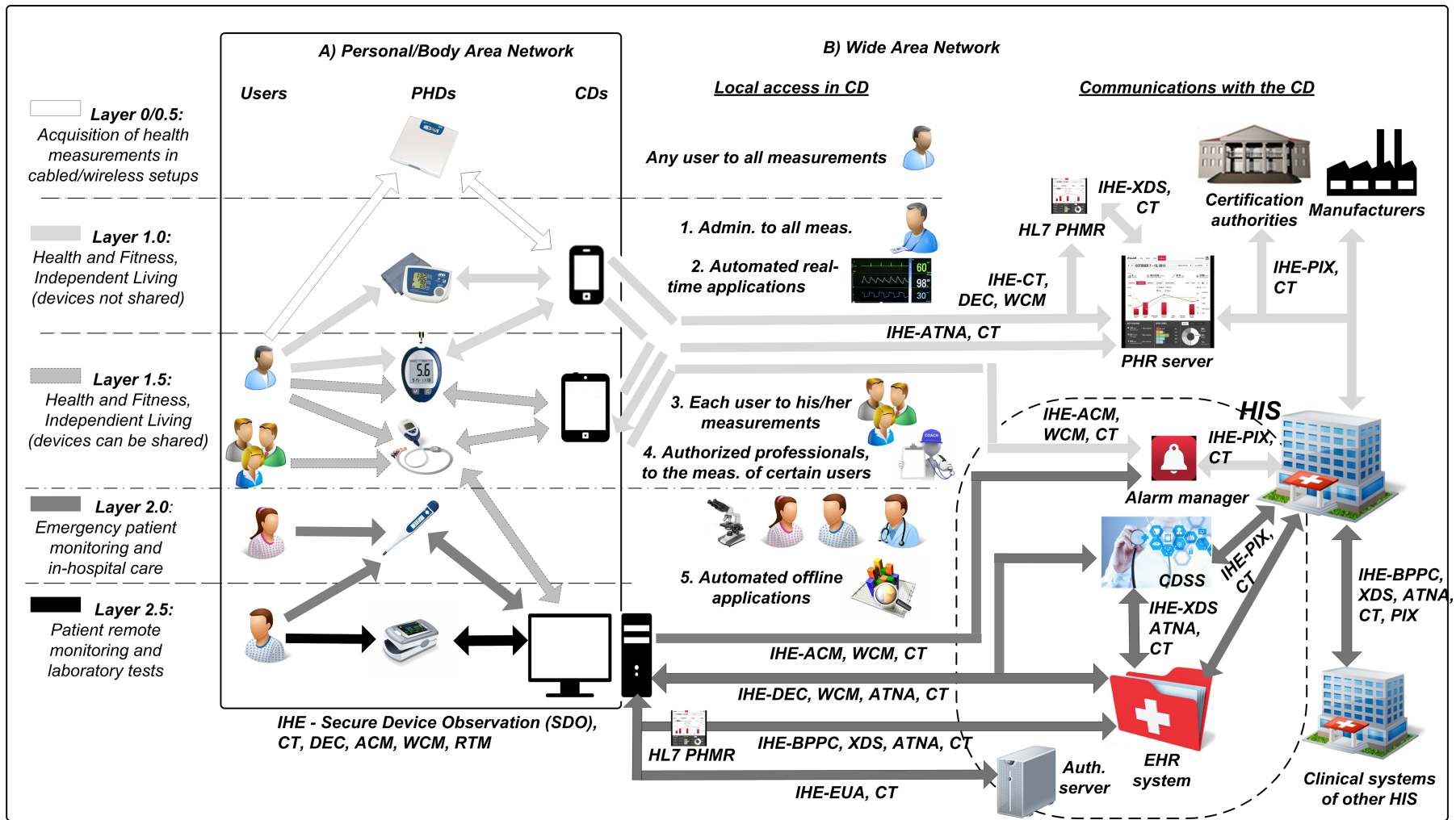


Figure 2.11: Layer-based proposal for a secure, cost-efficient, m-Health architecture.

### 2.6.3 Suggested algorithms for the SDO Profile

Various alternatives are available for performing the cryptographic functions required by the newly proposed IHE profile, Secure Device Observation. Those showing the best balance between security, complexity, overhead and free availability of the algorithm will be recommended. To assess security, the recommendations of the NIST are followed, regarding key lengths for long term use ( $>$  year 2030), summarized in Table 2.6, and crypto periods (time span during which a key is authorized for use), summarized in Table 2.7. In addition to this, priority of choice is given to algorithms not usually implemented by the transport technologies. This practice, implementing the same cryptographic functions at different levels with different algorithms, reduces the impact of attacks based on the vulnerability of some specific algorithm. The time complexity of the candidate algorithms, shown in Table 2.8, is estimated in cycles per operation (e.g. digital signature) or cycles per byte (e.g. in encryption), which is directly related with energy consumption and with delays, two major issues in BAN/PAN architectures [91]. With respect to space complexity, it is estimated by means of the overheads introduced, regarded as a fixed amount of bytes when calculating security items (challenge, hash, HMAC, DS or FP) and an estimation (half block length) when performing encryption, since the latter case is due to the addition of padding bytes to fit the cipher block length. It is worth noting that the overhead introduced by the algorithms will also have an impact on the energy consumption and delays of the architecture that implements them (due to the transmission of extra bytes) and hence on the demand of more powerful processors to enable real-time transmission. Finally, it is checked whether the algorithm is standard, under any restricting license, and if there are reliable free implementations available. This proposal includes the following:

- Symmetric encryption: Twofish [356], which is a suitable supplement to the Advanced Encryption Standard (AES [22]), usually implemented by secure transport technologies. This algorithm, designed by Bruce Schneier, was in fact one of the five finalists to become the AES [357], together with MARS, RC6 [358], Rijndael (chosen) and Serpent [359]. It can be considered very secure (third most voted after Rijndael and Serpent) and pretty fast (29.4 cycles/B), although slower than AES (12.6 cycles/B) and RC6 (17.3 cycles/B). Its mode is set to CTR (which is non-authenticated encryption), since it hinders cryptanalysis and does not require a previous padding of the plain text to the block size of the cipher. Regarding overheads, the three produce the same since their block size and key length are equally set to 128 bits. The main advantage of Twofish over RC6 is that the former has not been patented and has a reference implementation in the public domain. Symmetric master keys (MK) will be renewed every year. Symmetric keys for encrypting frames, S, will be

renewed every session and symmetric keys for encrypting stored data have a single use. If Twofish were to be compromised in the future, the order of preference for replacement would be Serpent, RC6, MARS and AES.

- **Asymmetric encryption:** RSA ( $\geq 2048$ ) [360] is the algorithm recommended for the exchange of master secrets, which supplements DH/ECDH [341], implemented by most secure transport technologies. RSA and elGamal [361] are the alternatives, but the former is preferred for being standard and less similar to DH. Nonetheless, RSA2048 introduces more overheads than ECDH (block length 2048 bits vs 256) and performs more slowly (11.41 Mcycles vs 5.17). Asymmetric encryption keys will be renewed every 1-2 years. If RSA were to be compromised in the future, elGamal would be recommended as a replacement.
- **Challenges generation:** The standardized SHA-512 [362], which produces longer challenges (512 bits) than other hash functions and ciphers, and thus reduces the possibilities of repetitions. In addition, it does not imply extra overheads since challenges are protected with RSA2048, resulting in 2048 bits regardless of the fact that the initial length is less. Another advantage is its performance (17.7 cycles/B), very close to the fastest cipher (RC6, 17.3 cycles/B). To obtain a challenge, a secret seed stored in the device is concatenated with the current time (at its maximum resolution) and hashed. If SHA-512 were to be compromised in the future, Whirlpool [363] would be recommended as a replacement.

Table 2.6: Cryptographic key length recommendations by NIST [355]

Date	Minimum of strength	Symmetric algorithms	Factoring modulus	Discrete logarithm Key	Discrete logarithm Group	Elliptic curve	Hash(A) <sup>1</sup>	Hash(B) <sup>2</sup>
2010 (Legacy)	80	2TDEA	1024	160	1024	160	SHA-1 to SHA-512	SHA-1 to SHA-512
2011- 2030	112	3TDEA	2048	224	2048	224	SHA-224 to SHA-512	SHA-1 to SHA-512
>2030	128	AES-128	3072	256	3072	256	SHA-256 to SHA-512	SHA-1 to SHA-512
>>2030	192	AES-192	7680	384	7680	384	SHA-384 SHA-512	SHA-224 to SHA-512
>>>2030	256	AES-256	15360	512	15360	512	SHA-512	SHA-256 to SHA-512

<sup>1</sup> Hash(A): Digital signatures and hash-only applications.

<sup>2</sup> Hash(B): HMAC, key derivation functions and random number generation.



Table 2.7: Cryptoperiods recommended by NIST for different types of key uses [355]

Key type	Cryptoperiod	
	Originator usage period (OUP)	Recipient usage period
Private signature key	1-3 years	
Public signature key	Several years (depends on key size)	
Symmetric authentication key	$\leq 2$ years	$\leq \text{OUP} + 3$ years
Private and public authentication keys	1-2 years	
Symmetric data encryption and key wrapping keys	$\leq 2$ years	$\leq \text{OUP} + 3$ years
Symmetric and asymmetric RNG keys	Upon reseeding	
Symmetric master key	About 1 year	
Private key transport key	$\leq 2$ years	
Public key transport key	1-2 years	
Symmetric key agreement key	1-2 years	
Private and public static key agreement keys	1-2 years	
Private and public ephemeral key agreement keys	One key agreement transaction	
Symmetric, private and public authorization key	$\leq 1-2$ years	

- Hashing: RIPEMD-256 [364], which performs faster (11.1 cycles/B) than other reference functions such as SHA-256 [362] (15.8 cycles/B) or Whirlpool (30.5 cycles/B). RIPEMD-256 and SHA-256 introduce less overhead than Whirlpool [363] (512 bits), while fulfilling the recommendation of the NIST (256 bits). Although Tiger operates faster (8.1 cycles/B), its key length (192 bits) is not secure enough. Furthermore, RIPEMD-256 will never be patented and reference implementations can be found in the public domain. If RIPEMD-256 were to be compromised in the future, the order of preference for replacement would be Whirlpool and SHA-256.
- HMAC with counter: The standardized Secure Hash Algorithm (SHA)-1 [365] is sufficient to implement these codes, since they do not need to be as secure as regular hashes. Part of the original content, a key SA, is unknown to the attacker, which minimizes the odds of finding collisions. Among the SHA family of standards, SHA-1 is the fastest (11.9 cycles/B) and most compact (160 bits). The counter is a 2-byte number, used to avoid a replay attack by re-sending frames gathered from the current session. SA will be renewed every session.

- Digital signature, fingerprints and certificates: The standardized Elliptic Curve Digital Signature Algorithm  $\geq 224$  (recommended 256) [366], which performs signature-verification slightly faster (3.92-6.56 Mcycles) than the other two algorithms authorized by the NIST, DSA [367] and RSA [360] with 2048-bit key length. DSA was replaced by ECDSA because the latter operates with smaller numbers, and thus it is hard to find implementations of DSA supporting 2048 bits. On the other hand, RSA2048 has a similar overall performance (11.06-0.29 Mcycles), but ECDSA produces a much shorter signature (512 bits vs 2048) with a roughly similar security level. Digital signature keys will be renewed every 1-3 years. If ECDSA were to be compromised in the future, the order of preference for replacement would be DSA  $\geq 2048$  and RSA  $\geq 2048$ .

Table 2.8: Performance of relevant cryptographic functions [368]

Algorithm	MiB/s	Cycles per byte	$\mu$ s to setup key and IV	Cycles to setup key and IV
3DES/CTR	13	134.5	27.317	49989
AES/CTR	139	12.6	0.698	1277
Twofish/CTR	59	29.4	7.716	14121
Serpent/CTR	32	54.7	1.197	2191
RC6/CTR	101	17.3	2.802	5128
MARS/CTR	47	37.2	3.516	6435
Blowfish/CTR	58	30.0	62.683	114710
Whirlpool	57	30.5		
Tiger	214	8.1		
MD5	255	6.8		
SHA-1	153	11.4		
SHA-256	111	15.8		
SHA-512	99	17.7		
RIPMD-128	153	11.4		
RIPMD-160	106	16.5		
RIPMD-256	158	11.1		
HMAC(SHA-1)	147	11.9	0.509	932

Operation	ms/Operation	Mcycles/Operation
RSA 2048 encryption—decryption	0.16—6.08	0.20—11.12
RSA 2048 signature—verification	6.05—0.16	11.06—0.29
DH 2048 key-pair generation with precomputation	2.14	3.92
DH 2048 key agreement	3.84	7.03
ECDH over GF(p) 256 key-par generation with precomputation	2.19	4.01
ECDH over GF(p) 256 key agreement	2.82	5.17
ECDSA over GF(p) 256 signature—verification with precomputation	2.14—3.58	3.92—6.56

### 2.6.4 Integration of signal-based protection within biomedical standards

This Section details an example of implementation of the Signal-Based Protection component of the newly proposed Secure Device Observation profile (SDO:SBP). Particularly, it is introduced a new file format based on DICOM that enables the efficient segmentation of an echocardiogram frame into regions in order to, on the one hand, enhance storage capacity and on the other, to enable a security-enhanced anonymization process. Basically, once the information to be anonymized is extracted, the process of anonymization is carried out through a signal-based security technique, called keytagging (introduced in Section 4.5), which meets essential requirements for the integration with DICOM: security, transparency to the image, cost-efficiency and fully compliance with JPEG2000. The following paragraphs explain this processes involved in detail.

#### Segmentation based on echocardiogram characteristics

On the whole, echocardiogram images have three different regions, as shown in Figure 2.12: the ultrasound image (white solid line), auxiliary images (green dotted line) and text (yellow dashed line). The ultrasound image is the most important because it contains the most relevant information for the diagnosis. The ultrasound is always present and only appears once in each frame. The auxiliary images surround and complement the ultrasound region. These are, for example, the ECG, the color label, other ultrasound images to supplement the information of the main ultrasound image and some symbols regarding the configuration. The text is always present in all the images and contains information such as patient data, date, time and configuration details of the acquisition session or measurements derived from the study, as shown in Figure 2.12. It is worth highlighting that certain text regions can contain very relevant information for the diagnosis.

An ultrasound study can be composed of one or several frames. The studies with multiframe, acting as a video sequence, show a temporal evolution — e.g. the B mode of echocardiograms represent the heart movement. The typical number of frames that needs to be stored for accurate diagnosis is 16, but there may be as many as 64 frames, as commented in the introduction. For multiframe studies, it is worth noting that the only region that change over time is the ultrasound region, the rest remain invariant. For each echocardiogram acquisition device, the distribution and the size of the regions, the number of auxiliary regions and the text engraved are different. Another difference is that some image regions contain color information that is relevant for the diagnosis while others not — e.g. the Doppler modes include relevant information in color in the ultrasound image and in the color scale.

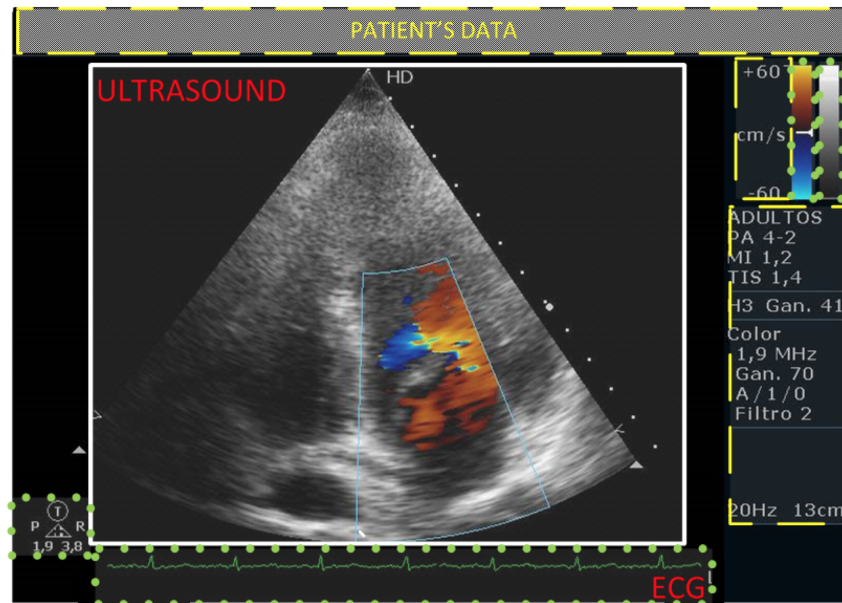


Figure 2.12: Echocardiogram regions of the color Doppler mode. The white solid line contains the US, the green dotted the auxiliary images, and the yellow dashed the text.

### New Storage Format based on DICOM

Basically, a DICOM file contains a header and the image. It is proposed creating a new image format, to be included in the DICOM standard, which takes advantage of the segmentation capabilities already incorporated in acquisition devices — and also available in certain postprocessing software. The final file, which the device shall provide, is a DICOM file (Section 2.1.4) and consequently has two parts: the DICOM header and the image coded according to the the proposed image format. These parts are described below.

- *DICOM header*: The header composition for each image type is listed in Part 3 of the DICOM standard. The header fields included in a file depend on the image type and on the acquisition device. Nevertheless, it always stores certain mandatory data, such as the width, height, bit depth, color type and image format. The format of the image part is defined by means of the “Transfer Syntax Unique Identifier” header field, included in Part 5 of the DICOM standard. The header also contains information about the patient, such as the patient’s name, and other information regarding the echocardiogram test, such as the type of scan, position, acquisition device and number of frames. An important field of the DICOM header, included in the ultrasound image, is the calibration of the regions. It defines regions on the ultrasound image with different calibrations and the calibration parameters, which is of use to perform measurements in the ultrasound regions. To this regard, no changes are needed in the DICOM header in order to integrate the proposed image format

in the DICOM standard. It is only necessary to define a “Transfer Syntax Unique Identifier” for the proposed format, to permit its specification and implementation in DICOM files.

- *Proposed image format:* DICOM can use either lossless or lossy compression, and the codecs supported are specified in Part 5 of the standard. Among them, JPEG2000 has been selected for this format given its efficiency and compatibility with the image-based security technique chosen (Section 4.5). It has been designed an image compression format that separates the image into regions. First, the acquisition device provides the regions and their types: ultrasound, auxiliary or text, as shown in Figure 2.12. Then, the acquisition device generates the image format, which consists of two parts: an Extensible Markup Language (XML) file, where the information related to the regions configuration is included, and the coded regions. The XML format is proposed because it is extremely portable and similar to the DICOM headers system. This file shall encode the text efficiently but without losing quality, since it can contain relevant information for the diagnosis. With respect to the independent storage of echocardiogram regions, it facilitates the addition of information for the diagnosis and the removal (or edition) of the least relevant regions for enhanced compactness.

*XML File:* Figure 2.13 shows a common XML implementing this file format. The XML file contains the following information, including the corresponding XML fields between brackets:

- The size of the whole image (tsize: w, h), as a copy of the corresponding fields contained in the DICOM header.
- The regions configuration (region), one per region present in the image. The types are: ultra-sound or ROI (roi), auxiliary image (img) and text (text).
- The position of the regions (pos). The initial position (x0, y0) has to be defined for all types of region and also the final position (x1, y1), except for the text region since its size is adjusted to the space available. All the regions have a rectangular shape.
- The image codec (cod) may be indicated for the ultrasound and image regions, the default codec is JPEG2000.
- The sizes of the ultrasound (size) and image (L) regions, in bytes.
- In the case of having several frames, the ultrasound is the only region that changes in every frame, so only one region (roi) has to be indicated in the XML file. The number of frames is indicated in the ultrasound region (frames). The

field size (size) of every ultrasound frame can be added in the case that the size changes for each one, otherwise it only needs to appear once.

- The text regions (text) include their contents in the XML file. The acquisition device shall provides the XML file, as it already does with similar headers in the DICOM file — e.g. the file size or the calibration regions.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE configuration SYSTEM "roistorageformat.dtd">
<format>
  <tsize w="512" h="256"/>
  <region>
    <pos x0="44" y0="75" x1="564" y1="597"></pos>
    <roi><size>33893</size></roi>
  </region>
  <region>
    <pos x0="0" y0="0"></pos>
    <text>PATIENT'S DATA</text>
  </region>
  <region>
    <pos x0="77" y0="574" x1="615" y1="573"></pos>
    <img L="149"></img>
  </region>
</format>
```

Figure 2.13: Example of XML file to support the new image format.

*Encoded regions:* The second part corresponds to the encoded regions, except the text, which is included in the XML file. The role of the XML respect to these regions is to specify the order of the regions and the codec and compression quality for each individual region, which can be adjusted according to criteria such as their diagnostic relevance. This coding process would not add complexity if integrated in DICOM-compliant acquisition devices.

### Security mechanism

The new DICOM-based format, which stores the echocardiogram information in differentiated regions, facilitates the implementation of image-based security techniques (e.g. steganography, watermarking, keytagging). The following paragraphs describe how the best fitting technique, keytagging, can enhance the levels of security of the echocardiogram. For the sake of clarity, a brief summary of the main principles of the keytagging algorithm is provided below.

Keytagging is a novel technique intended for the protection of medical image-based tests, thus, including echocardiograms. Complete details about this technique can be found in Section 4.5. Basically, it relies on the association of tags (any type of binary content,  $T$ ) to stable, semistable or volatile features of the image, producing access keys (called keytags,  $KT$ ) that depend on both the image and the tag content. Once the keytagging of an image  $I$  is done, the keytags  $KT$  shall replace the original content of the tags  $T$  associated to the  $I$ , being  $KT$  and  $I$  — the latter may have undergone some modification(s) — necessary to retrieve  $T$ .

Going to the multiframe case, the first step is to select the frame(s)  $I$  and the content(s)  $T$  to be associated by means of keytags  $KT$ . Multiframe images can include up to 64 frames and any of them can be selected for keytagging. Although a frame may be composed by more than one image region,  $T$  shall be linked to the main image region, the  $ROI$ . To perform the association of  $KT$ , the keytagging algorithm transforms the  $ROI$  into grayscale, performs the Cohen-Daubechies-Feauveau (CDF) 9/7-tap wavelet transform of the grayscale ROI, extracts stable, semistable and volatile features from the wavelet coefficients — these features correspond to certain bits of relevant coefficients belonging to selected wavelet subband — and efficiently encodes  $T$  based on these features. The use of the CDF 9/7-tap wavelet transform, used by JPEG2000, guarantees high compliance of keytagging with this DICOM-compliant compressor — which is extensible to the standard.

It is worth noting that, unlike other image-based security techniques (e.g. steganography, traditional watermarking), keytagging can associate information to the most stable features of the image without distorting it. As a consequence, this method preserves the clinical content of the image without the need for assessment, prevents eavesdropping and collusion attacks, and obtains a substantial capacity-robustness tradeoff with simple operations. Furthermore, another very relevant feature is that the strength of the link between  $I$  and  $T$  through  $KT$  can be adjusted. If a  $T$  is linked to the image by means of a stable  $KT$ , the content is retrievable even from heavily modified (and distorted) versions of  $I$ ,  $\tilde{I}$ . By contrast, semistable  $KT$  only retrieve the original contents of  $T$  if the image modification(s) are mild (e.g. if  $\tilde{I}$  preserves its clinical content). Finally, volatile  $KT$  retrieve highly distorted  $\tilde{T}$  even if the modification(s) of  $\tilde{I}$  are mild, since they are intended to work only with the original  $I$ . Therefore, they have different applications in security — a complete description can be found in Section 4.7.1. For instance, stable keytags may be used to persistently associate relevant test IDs (e.g. the patient ID), semistable keytags are useful for associating information that will not be (by any means) retrievable if the image gets highly distorted (the test diagnosis) and volatile keytags to associate known patterns in order to detect, and even locate, tampered image areas.

### Integration of the keytags in the DICOM header

The keytagging algorithm permits associating information of interest  $T$  to the echocardiogram  $I$  by means of keytags  $KT$ . Any frame in the multiframe video — regardless its mode — is suitable to be  $I$ . So as to obtain a smooth integration in DICOM files, each  $KT$  is placed in the DICOM header replacing the corresponding  $T$  field. For instance, if  $T$  is the name of the patient and it is associated to frame 1 ( $I$ ) by means of a semistable  $KT$ , this  $KT$  replaces the actual patient's name in the corresponding field (0010,0010) of the DICOM header. Note that in order to identify which frame(s) and region(s) have been used as  $I$ , these details are included along with the  $KT$ . This schema permits the keytagging of frames/regions in an unambiguous way.

As regards to privacy, the DICOM fields may contain sensitive information. In this case, DICOM mandates their storage in digital envelopes protected with CMS. Therefore, all DICOM field(s) replaced with  $KT$  will be adequately protected with the cryptographic means implemented by DICOM. Any  $KT$  shall be placed in protected envelopes, digitally signed (with ECDSA  $\geq 224$ , DSA  $\geq 2048$  or RSA  $\geq 2048$ ), and encrypted if  $T$  (and thus  $KT$ ) is confidential, preferably using Twofish for the symmetric encryption and RSA  $\geq 2048$  for the asymmetric.

#### 2.6.5 Implications for IHE and its profiles

The main implication is the suggestion of SDO (Sections 2.6.2 and 2.6.3), a new IHE profile which would belong to the PCD domain and which would enable a standardized and secure communication in the first segment of DEC (alone or combined with WCM) — from the PCD to the Device Observation Reporter— and ACM (alone or combined with WCM) profiles —from the Alarm Source to the Alarm Aggregator—, which are currently not detailed. The hypothetical integration of SDO in IHE would imply the addition of new advisories in ACM, related with security issues —e.g. invalid certificate, unauthorized user trying to take his/her measurements— and would open up the possibility of recommending the use of the enhanced —SDO-compliant— version of ISO/IEEE 11073 in implementations of DEC, ACM and WCM.



*“Hackers are breaking the systems for profit. Before, it was about intellectual curiosity and pursuit of knowledge and thrill, and now hacking is big business.”*

Kevin Mitnick

*“For good ideas and true innovation, you need human interaction, conflict, argument, debate.”*

Margaret Heffernan

# 3

## Enhancement of the security of standard protocols for the exchange of biomedical information

This Chapter deals with the blocks of the proposal for a secure, cost-efficient, m-Health architecture that are surrounded in red in Figure 3.1. While Section 2.6 (blue block in Figure 3.1) proposed a solution consisting of a flexible structure that provides features tailored to the needs of different types of m-Health application — e.g. the identification of users by means of authentication elements to enable the sharing of PHDs and/or CDs with privacy, the cryptographic protection of the communications or the compliance with the IHE profiles implemented by EHRs and CDSS —, Chapter 3 addresses the extension and strengthening of weak biomedical standards according to it. Particularly, the two security extensions described herein are applied to the widespread standards ISO/IEEE 11073 PHD (X73PHD, Section 2.1.2), which covers the communications between a variety of PHDs and CDs, and to SCP-ECG (Section 2.1.3), which specifies conventions required for the storage and interchange of ECG information between ECG devices and host systems. The manner how the X73PHD models are extended and how X73PHD-compliant devices (PHDs acting as agents and CDs acting as managers) implement the IHE profiles included in the layered proposal is detailed in Section 3.1. In addition, Section 3.2 analyzes the security of this extension and its associated costs: implications for X73PHD and impact on the X73PHD-IHE architecture and on its surrounding framework. Similarly, Section 3.3 defines the extension for the security enhancement of SCP-ECG files, Section 3.4 assesses the security of this extension and its associated costs and Section 3.5 presents a proof of concept. Finally, the main conclusions from this research are drawn in Section 3.6.

Table 3.1: Operators and notation of the extensions of X73PHD and SCP-ECG

Operators	Meaning
$[x,y]$	Concatenate strings x and y
$x=y$	x takes the value of y
$x==y$	Returns the result (true or false) of comparing x and y
$x\{y\}$	Cipher or decipher string y using key x
$f(x,y)$	Execute function f with parameters x and y
Notation	Meaning
X	Entity. It could refer to an agent (A), a manager (M), a user (U), an administrator (Ad) or a manufacturer (Mf)
Ch1	Challenge used by a manager to authenticate an agent
Ch2	Challenge used by an agent to authenticate a manager
$h(x)$	Hash of string x
MK	Symmetric master key to derive symmetric session keys (S, SA)
S	Symmetric session key for encryption of frames
SA	Symmetric session key for authentication of frames
CEX	Certificate for encryption of entity X
PrEX	Private key for encryption of entity X
PbEX	Public key for encryption of entity X
CSX	Certificate for signature of entity X
PrSX	Private signature key of entity X
PbSX	Public signature verification key for entity X
Fi	Frame in clear text to be exchanged between agent and manager after C&A function
$HMAC(Fi,SA)$	Message authentication code of frame Fi using key SA
$C\&A(Fi,S,SA) = [S\{Fi\}, HMAC(S\{Fi\},SA)]$	Frame i exchanged between an agent and a manager, using session key S for encryption and session key SA for authentication
d	Medical measurement(s)
D	d concatenated with identification or authentication strings
$DS(D,PrSX)$	Digital signature of frame D performed by entity X
ID(X)	In case of devices, this is the EUI-64. In case of users, this is the PersonID
$FP(D,X) = [ID(X),DS(D,PrSX)]$	Fingerprint of frame D performed by entity X. It includes the identity (ID) of X and its DS
StAi	Symmetric key i for encryption of data to be stored in an agent
StMi	Symmetric key i for encryption of data to be stored in a manager
RFID-T	Radio Frequency Identification Token
BC	Bar code
SC	Smart Card

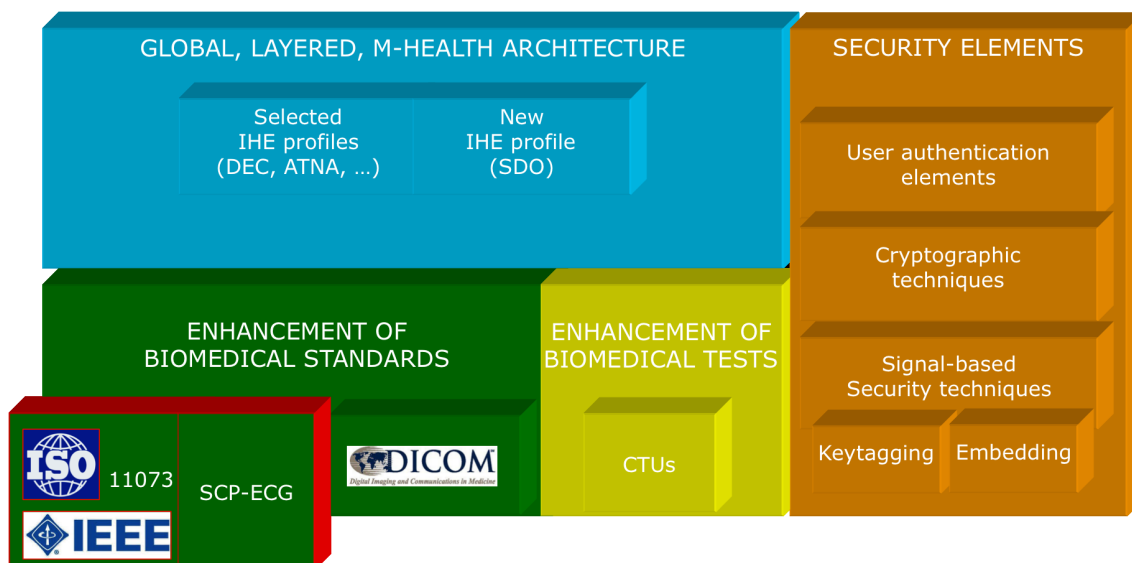


Figure 3.1: Building blocks for a secure, cost-efficient, m-Health architecture. Contents addressed in Chapter 3 surrounded in red.

### 3.1 Enhancement of the security of ISO/IEEE 11073 Personal Health Devices

This section depicts in detail the extended X73PHD-IHE framework and also the role of the entities involved in the implementation of the IHE profiles included in the global, layered-based security scheme — see Section 2.6.2. The notation to interpret this proposal is summarized in Table 3.1. Focusing first on the enhancement of the X73PHD architecture, the series of steps proposed to carry out this task —by including compliance with the SDO, DEC, ACM, WCM and RTM profiles— are defined in Tables 3.2-3.4, and related with the layer(s) that implement it and with the corresponding IHE profile(s). Furthermore, an example with the steps of the first connection between an agent and a manager in Layer 2.5 is included in Figure 3.2. Complementarily, the Finite State Machine (FSM) of the extended X73PHD is illustrated in Figure 3.3 and the new and modified frames and attributes are specified in Tables 3.6-3.8. Regarding the peripheral processes that integrate the X73PHD-IHE framework, the manufacturing and initial configuration of the devices are addressed in Table 3.2, and the local consultation of measurements and the forwarding to the appropriate healthcare systems — according to the illustration in Figure 2.11 — are guaranteed through the implementation of the IHE profiles listed in Section 2.1.1 in the manner described below.

- *CT*: The manager shall connect, as time client, to a NTP/SNTP [182, 211] server to obtain the current time.

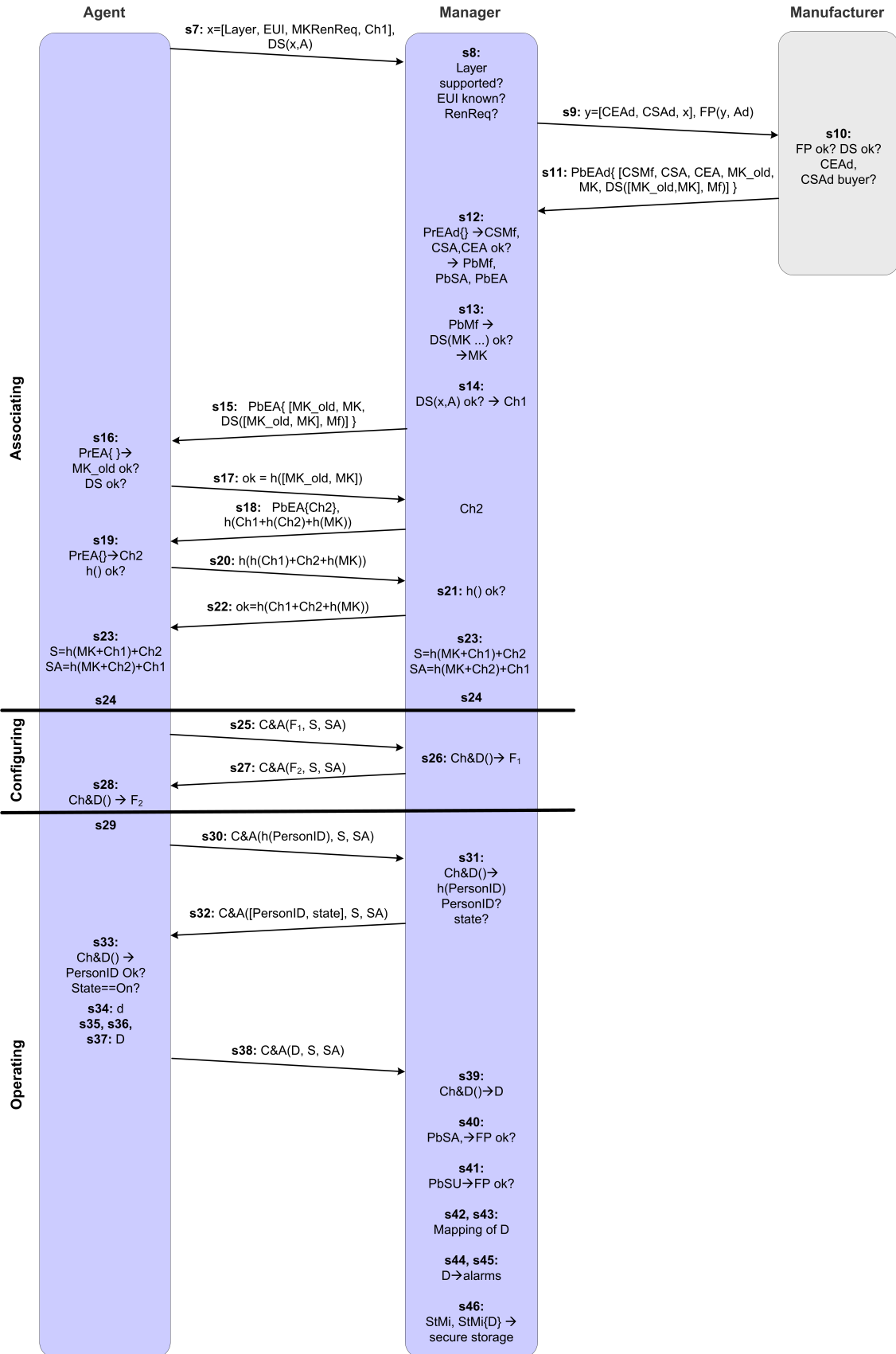


Figure 3.2: Illustration of a successful first connection between an agent and a manager in Layer 2.5 of the extended X73PHD.

- *DEC and WCM*: The manager shall act as the Device Observation Reporter, which forwards the acquired measurements to Device Observation Consumers, such as PHR, EHR or CDSS, by means of a subscription mechanism that enables their filtering by means of Device Observation Filtering actors.
- *ACM and WCM*: The manager shall act as the Alert Reporter —whose alerts may have their origin in the agent— communicating with an Alert Manager which notifies Alert Communicator(s) such as the smartphone of the administrator —e.g. for advisories regarding security issues—, or nurses and next of kin —for physiological and technical alarms.
- *ATNA*: The manager and the healthcare systems (e.g. PHR, EHR, CDSS, alert system) shall implement a secure node, so that they can authenticate users and authorize them to consult stored measurements. The events of acquisition of measurements —as they reach the manager, PHR, EHR, CDSS or alert system— and access of users to them are recorded in an audit repository to which these entities connect to.
- *XDS and BPPC*: When the manager stores the measurements acquired by agents as documents, it may become a XDS-compliant Document Source for PHR and EHR systems that shall implement a Document Repository for persistent, secure and reliable storage. Both PHR and EHR systems may implement a Document Registry to facilitate easier retrieval of these documents for Document Consumers (e.g. a CDSS). BPPC shall be implemented by XDS actors to implement policies of private access based on user consent, that is to say, a type of access to personal biomedical data that is constrained by the consent of the user.
- *EUA*: The manager shall act as a Client Authentication Agent, which connects to a centralized Kerberos Authentication Server of the HIS to get user authentication —based on either RFID-T or SC— and service tickets, enabling further kerberized secure communications. In addition, a specific system filters any meaningful command that a malicious user may try to introduce as a password through the Authentication Agent.
- *PIX*: The HIS takes the role of Patient Identity Source —providing patient identity feed based on the user's demographic data and on his/her personID (e.g. extracted from RFID-T, BC and SC), which is registered as patientID—, and also the role of PIX Manager —in charge of the cross-referencing— and the entities with access to user measurements (e.g. PHRs, EHRs, CDSS, alert systems) shall act as PIX Consumers —for homogeneous referencing.

Table 3.2: Steps for a successful first connection between an agent and a manager in the extended X73PHD (I)

Step	Layer(s)	Entity	Action(s)	IHE profile(s)
<i>State: processes of device(s) manufacturing and initial configuration (related to X73PHD framework)</i>				
1	1.5+ 2.0+ 2.5	Mf	Providing the agent with a BC reader and a passive RFID sensor, and each user with a BC or a RFID-T —e.g. as bracelets, as personal cards. Providing the manager with a RFID sensor and a SC reader Providing the agent with a port that enables the attachment of a SC card reader with its corresponding keypad.	SDO, DEC, ACM EUA SDO, DEC, ACM
2	1.0+	Mf	Generating, signing and holding the CEA and CSA certs of the agent. These contain the agent’s EUI-64, and respectively, its public encryption key, PbEA, or its public signature verification key, PbSA. CEA and CSA are stored in a public repository and their paired private keys, PrEA and PrSA, are stored inside the agent.	SDO:SEC
3	1.0+	Mf Ad	Repeating the actions of step 2 in the manager — if off-the-shelf — with CEM (only in Layers 2.0+) and CSM. Repeating the actions of step 2 in the manager — if not off-the-shelf — with CEM (only in Layers 2.0+) and CSM.	SDO:SEC
4	1.0+	Ad	Installing the admin’s CEAd and CSAd certs, bundled with their password-protected private key, in the manager.	SDO:SEC
5	1.0+  1.5+ 2.5	Ad	Based on the consent of the users, implementing a XACML-based policy setting which users (e.g. trainers, physicians) can access the measurements of others (e.g. clients, patients) after authentication (with password in Layer 1.0, with RFID-T/SC in Layers 1.5+). Configuring the manager to establish the RFID-T/BC of the users from which it is allowed to receive measurements. Storing a copy of the public encryption cert (CEU) of the users from which it is allowed to receive measurements.	EUA, ATNA, BPPC, SDO:SST SDO:CMA SDO:CMA
6	0.5+	Ad	Pairing/associating agent and manager with authentication (e.g. PIN, passkey, NFC) if the chosen transport technology supports it.	SDO:SEC
<i>State: associating with authentication process (related to X73PHD standard)</i>				
7	1.0+	A	Negotiating a security layer and launching its EUI (the manager may have requested it) together with a fresh challenge, Ch1. Signing this frame, x, with PrSA –to enable further verification– and sending it to the manager.	SDO:CBA
8	1.0+	M, A	The manager receives the frame and checks whether the security layer is supported. If it is not supported, the agent will attempt to establish an association with lower security requirements in s24. If the proposed security is supported, the manager consults its association table to check if there has been previous association to that EUI. If so, the manager knows MK and goes to step 14 — unless if frame x contains a request to renew some key or cert.	SDO:CBA
9	1.0+	M	Sending a frame to the agent’s manufacturer, including the administrator’s certificates CEAd, CSAd and x (from s7), concatenated with the admin’s fingerprint. To obtain the fingerprint, the admin is required to manually introduce the password of his/her private signature key, PrSAd.	SDO:SRC
10	1.0+	Mf	Verifying the fingerprint of y and the signature of x, and also that CSAd corresponds to the buyer of that agent.	SDO:SRC
11	1.0+	Mf	Sending its certificate CSMf, the agent’s certificates CSA and CEA and MK signed by the manufacturer. If x (from s7) contained a renewal request –which happens with a periodicity of 1-3 years–, both the old and the new key/cert requested will be attached and digitally signed. This entire frame is encrypted with the corresponding admin’s public encryption key, PbEAd.	SDO:SRC
12	1.0+	M	Decrypting the frame by using PrEAd. Then, verifying the certs by means of CRL or OCSP. If they are not valid, rejecting the connection — by means of a frame in s24 — and instructing the admin to contact the agent’s manufacturer. Otherwise, PbMf, PbSA and PbEA are obtained.	SDO:SRC, ACM
13	1.0+	M	Using PbMf to verify DS(MK,Mf), both decrypted in the previous step. If it is valid, obtaining MK.	SDO:CBA-SRC
14	1.0+	M	Using PbSA to verify the signature of frame x (from step 7). If it is valid, obtaining the challenge Ch1 and generating its own fresh challenge, Ch2.	SDO:CBA
15	1.0+	M	If x (from s7) contained a renewal request –which happens with a periodicity of 1-3 years–, sending to the agent both the old and the new key/cert requested and its digital signature — by the manufacturer —, all encrypted with its public encryption key, PbEA.	SDO:SRC

Table 3.3: Steps for a successful first connection between an agent and a manager in the extended X73PHD (II)

Step	Layer(s)	Entity	Action(s)	IHE profile(s)
<i>State: processes of device(s) manufacturing and initial configuration (related to X73PHD framework)</i>				
16	1.0+	A	Decrypting the frame with its private decryption key, PrEA. Next, checking that the signature of the frame is valid and that the old cert/key is correct.	SDO:SRC
17	1.0+	A	Accepting or rejecting the update of the key/cert (based on the previous step) by means of a frame sent to the manager. Destroying the old key/cert in case of acceptance and sending a warning message to the admin otherwise.	SDO:SRC, ACM
18	1.0+	M	Sending an authentication frame, composed of PbEA{Ch2} and h(Ch1 + h(Ch2) + h(MK)), to the agent.	SDO:CBA
19	1.0+	A	Decrypting Ch2 by using PrEA. Using it, Ch1 and MK to check that the received h(Ch1+h(Ch2)+h(MK)) is valid. Authenticating the manager if the verification is successful.	SDO:CBA
20	1.0+	A	Calculating h(h(Ch1)+Ch2+h(MK)) and sending it to the manager.	SDO:CBA
21	1.0+	M	Authenticating the agent if the verification of the frame received is successful.	SDO:CBA
22	1.0+	M	Confirming the authentication to the agent, by sending the frame h(Ch1+Ch2+h(MK)).	SDO:CBA
23	1.0+	A, M	Deriving session keys for encryption, S = h(MK + Ch1) + Ch2, and authentication, SA = h(MK + Ch2) + Ch1.	SDO:SRC-SEC
24	1.0+	A, M	Aborting the connection if the certs of the agent are not valid (s12) or to negotiating a lower security layer that both agent and manager support (s8). The frames exchanged between agent and manager from here on are encrypted and authenticated.	SDO:CBA-SRC
<i>State: configuring process (related to X73PHD standard)</i>				
25	1.0+	A	Sending the frame Fi, encrypted with S, to establish the further transmission of measurements. This frame is concatenated with a Hash Message Authentication Code, HMAC(S{Fi}, SA), dependent on both the encrypted frame, and on the session key for authentication SA. The resulting frame, [S{Fi}, HMAC(S{Fi}, SA)], is denoted as C&A(Fi, S, SA), named after “CIPHERING & AUTHENTICATION”.	SDO:SEC
26	1.0+	M	Using SA to verify the HMAC of Fi. If it is valid, then the manager decipheres the frame with S and interprets it. This process, inverse to that in s25, is denoted as Ch&D(C&A(Fi, S, SA)) named after “CHECKING HMAC & DECIPHERING”.	SDO:SEC
27	1.0+	M	Sending the frame C&A(Fj, S, SA) to continue with the configuration process.	SDO:SEC
28	1.0+	A	Using SA to verify the HMAC of Fj. Steps 25-28 may be repeated several times, until all configuration frames have been exchanged.	SDO:SEC
<i>State: data measurement and transmission processes (related to X73PHD standard and its framework)</i>				
29	1.5-2.0	U	Swiping his/her RFID-T/BC through the passive sensor of the agent.	SDO:UID, DEC:RFID-T or BC
	2.5		Inserting his/her SC in the slot of the agent and introducing his/her PIN/password.	SDO:UID, DEC:SC
30	2.0+	A	Applying C&A() to a frame Fi = h(PersonID) and sending C&A(Fi, S, SA) in order to find out if the manager knows the user corresponding to h(PersonID).	SDO:CMA
31	1.5+	M	Applying Ch&D() to the received frame and obtaining Fi = h(PersonID). Checking that the admin had configured a PersonID whose hash is precisely the received h(PersonID). Otherwise, requesting the admin to do it now. If he/she does nothing, rejecting the association.	SDO:CMA SDO:CMA ACM
	2.5		Checking that the admin had stored the public certificate whose PersonID hash is precisely the received h(PersonID). Otherwise, requesting the admin to do it now. If he/she does nothing, rejecting the association.	SDO:CMA ACM
	1.5+		If the connection has not been rejected, checking the state of the ID credentials of that user (enabled or disabled). If it is disabled, sending a warning message to both the user and the admin.	SDO:CMA ACM

Table 3.4: Steps for a successful first connection between an agent and a manager in the extended X73PHD (III)

Step	Layer(s)	Entity	Action(s)	IHE profile(s)
32	1.5+	M	Sending C&A([PersonID, state], S, SA) to the agent.	SDO:CMA
33	1.5+	A	Calculating Ch&D(C&A([PersonID, state], S, SA)). Subsequently, checking that the PersonID of the user identified in the agent matches the PersonID received from the manager. If the state of the credentials is disabled, the acquisition session is not started, go back to step 29	SDO:CMA, ACM
34	0+	U	Taking his/her measurements “d” by means of the agent.	DEC, WCM
	1.5+	A	Logging off the user 10-seconds after he/she takes his/her last measurement.	SDO:CMA
	0+	A	Going back to step 29 to begin a new acquisition session — unless agent and manager were disassociated for some reason.	SDO:CMA
35	1.5-2.0	A	Adding the PersonID, provided by his/her RFID-T or BC, to d. D= [d, PersonID].	SDO:UID, DEC: RFID-T or BC, WCM
	2.5		Adding the user’s fingerprint, provided by his/her SC, to d. D= [d, FP(d, U)].	SDO:UID-UDS, DEC:SC, WCM
36	1.0+	A	If it does not know the user (checked in step 31), generating a symmetric key for storage, StAi, calculating and storing StAi{D} and PbEM{StAi} in the PM-Store. Next, wiping properly the variables and buffers storing the plain D and StAi, and going back to step 29.	SDO:SST
37	2.0+	A	Adding its own fingerprint to D, D=[D, FP(D,A)]	SDO:MV, DEC, WCM
38	1.0+	A	Sending C&A(D,S,SA) to the manager.	SDO:SEC, DEC, WCM
39	1.0+	M	Calculating Ch&D(C&A(D,S,SA)).	SDO:SEC, DEC, WCM
40	2.0+	M	Verifying the agent’s fingerprint in D with its associated public signature verification key, PbSA. If it is not valid, refusing D.	SDO:MV, DEC, WCM
41	2.5	M	Verifying the user’s fingerprint in D, with its associated public signature verification key, PbSU. If it is not valid, refusing D.	SDO:MV, DEC, WCM
42	2.0+	A	If steps s38 or s39 fail, getting notified and storing D in the PM-store, as in step 33 — the data rejected. Instructing the admin to check the certificates CSA and CSU, and rejecting the association.	ACM
43	1.0+	M	Mapping the acquired measurements D for its representation with IHE-harmonized syntax and semantics.	RTM, DEC, WCM
44	1.0+	M	The measurements D are readily available for applications that need to process them online (e.g. real-time displaying).	
45	1.0+	M	Generation of physiological alarms, if the value(s) of D are far out of a healthy range (e.g. systolic blood pressure $\geq$ 180 mmHg, the user did not take several pills of his/her medications), and also technical alarms, if the values of D are inconsistent (e.g. constant zero).	ACM, WCM
46	1.0+	M	Secure standard storage of D: Creation of a symmetric key StMi for encrypting StMi{D} of D. Storage of StMi{D} in a HL7 Personal Healthcare Monitoring Report (PHMR). Wiping properly the variables and buffers storing the plain D and StMi. The securely stored D are available for those users authorized by the XACML policy —implemented in step 5— after an authentication process that will filter any attempt of code injection.	SDO:SST



## 3.2 Evaluation of the security-enhanced ISO/IEEE 11073 PHD

This section begins assessing the security of the proposal in Section 3.1, by analyzing the countermeasures that each security layer implements against different threats, in Section 3.2.1. Then, the implications that this extension would have for the X73PHD models are laid out in Section 3.2.2. Next, Section 3.2.3 evaluates the performance of the extension, by measuring the impact that the implementation of each layer produces on the X73PHD architecture — in terms of overheads and delays — and on its surrounding framework. Finally, the potential limitations of this proposal are summarized in Section 3.2.4.

### 3.2.1 Risk assessment

The risk assessment is depicted in detail in Table 3.5. Columns 1-2 summarize the risk assessment of the X73PHD architecture —as described in Section 2.5— and columns 3-4 the measures against those threats depending on the layer implemented —based on the proposal described in Section 3.1. Table 3.5 shows that the preexisting Layer 0 implements no security and that the preexisting Layer 0.5 puts emphasis only on the secure pairing of devices (which on the other hand might be counterfeits or have been hacked) and on secure wireless communications between them. Layers 1.0+ add security measures to both agent and manager to detect counterfeiting, to impede hacking and undue local access to measurements, and new countermeasures for private and authenticated communications. Layers 1.5+ include the possibility that several users share agents and managers with privacy, by means of secure identification/authentication with BC/RFID tokens or smart-cards, automatized user log-off, remote activation/deactivation of identification credentials and checking that the user is known by the manager before he/she takes his/her measurements. In addition, these layers also implement audit trails of measurements acquisition, transmission (e.g. to EHR systems) and access to guarantee data traceability and user accountability. Layers 2.0+ add mandatory timestamps and fingerprints in the measurements for a strengthened verification in the manager. Finally, Layer 2.5 improves the identification of users in the agent (by requiring a smartcard and a password), and includes the digital signature of the user in his/her measurements to prevent their repudiation.

The chosen algorithms, their key sizes and crypto periods (Section 2.6.3) are considered secure until 2030, regardless of the layer. Furthermore, the key management policy (described in Section 3.1) is oriented towards Perfect Forward Secrecy. This implies that in the unlikely case that a session key is cracked, the damage is confined to that session

Table 3.5: Security analysis of the architecture of the layer-based, enhanced-X73PHD

Threats		Countermeasures	Layer: 0	0.5	1.0	1.5	2.0	2.5			
USER	User impersonation by credential theft or no request of identification/authentication credentials	Use of physical tokens for user identification/authentication				✓	✓	✓			
		Use of an additional password for user identification in the agent						✓			
		Use of an additional password for user authentication in the manager						Op.	Op.		
		Remote activation/deactivation of identification credentials —used in the agent— and user warnings					✓	✓	✓		
	Exploitation of open sessions	User log-off 10s after taking user measurements					✓	✓	✓		
	DoS by wrong user identification in the agent	BC/RFID token requested					✓	✓	✓		
		Smartcard requested							✓		
	Repudiation of user measurements	Including the PersonID attribute with all the measurements						✓	✓	✓	
		Including a digital signature of the user in his/her meas.							✓		
		Including a timestamp with meas. from agent's PM-store		✓	✓	✓	✓	✓	✓		
Extending the timestamp to freshly acquired measurement							✓	✓			
AGENT	Device counterfeiting	Device certificate, signed by manufacturer, requested					✓	✓	✓	✓	
		Authentication by manager					✓	✓	✓	✓	
	Device hacking to deliver wrong measurements	Fingerprints in measurements						✓	✓		
		Manager verifies fingerprints						✓	✓		
	Data theft by local access	Asymmetric encryption of the PM store: decryption possible only in the manager					✓	✓	✓	✓	
		Proper wiping of critical variables/buffers					✓	✓	✓	✓	
Sending measurements to a wrong manager	Checking if the user is known by the manager					✓	✓	✓			
AGENT-MANAGER	Injection of commands	Secure transport					✓	Op.	Op.	Op.	Op.
		Frames with HMACs					✓	✓	✓	✓	
	Cracking of cryptographic keys	Use of secure algorithms, complementary to those of the secure transport layer					✓	✓	✓	✓	
		Key sizes recommended by NIST					✓	✓	✓	✓	
		Keys are renewed (and the previous ones are destroyed) before expiration or if they are revoked					✓	✓	✓	✓	
		Perfect Forward Secrecy					✓	✓	✓	✓	
	Eavesdropping	Secure transport					✓	Op.	Op.	Op.	Op.
		Frames encryption					✓	✓	✓	✓	
	Replay attack	Secure transport					✓	Op.	Op.	Op.	Op.
		Fresh challenges and counter in frames					✓	✓	✓	✓	
Man in the middle attack	Secure device pairing (PIN, PBC, NFC, etc.)					✓	Op.	Op.	Op.	Op.	
	Agent-manager authentication					✓	✓	✓	✓		
DoS by injecting noise	HMACs and retrials					✓	✓	✓	✓		
	Report to admin, secure storage of meas. in PM-store					✓	✓	✓	✓		
MANAGER	Counterfeiting to associate to a rightful agent	Admin and agent's manufacturer authorization requested to managers.					✓	✓	✓	✓	
		If ad-hoc device, cert. requested —signed by its manufacturer							✓	✓	
		Authentication by agent					✓	✓	✓	✓	
Hacking to corrupt the measurements	Audit trails of measurements acquisition, transmission and access					✓	✓	✓			
Data theft by local access	Single-use keys and asymmetric encryption of measurements: authenticators required for decryption					✓	✓	✓	✓		
	Proper wiping of critical variables/buffers					✓	✓	✓	✓		
Access of authorized users to unintended measurements	Role-based access control: regular users, professionals, admin, automatized online and offline applications					✓	✓	✓			
Injection of malicious codes	Command filtering in the authentication system					✓	✓	✓			

and the attacker will only be able to read those frames (if he/she discovers S) or to authenticate forged frames (if he/she discovers SA). To minimize the likelihood that the master key is discovered, it is used only to derive session keys that protect the transmission of frames. But even if at some point an attacker discovers MK and some session keys, frames exchanged in previous sessions will be safe since session keys are derived from MK and another random secret, Ch2, which is protected by the public key of the agent. Finally, the measurements from an acquisition session are protected with symmetric keys of single use protected with asymmetric cryptography.

### 3.2.2 Implications for ISO/IEEE 11073 PHD

The implications that the proposal suggested in Section 3.1 would have for X73PHD can be seen through the modifications involving its service, communication and domain information models. This is mainly illustrated in Tables 3.6-3.8 — service model and, eventually, DIM — and Figure 3.3 — communication model and, incidentally, service model. The four columns on the left in Tables 3.6-3.8 show the four modified and four newly-created frames to meet the proposals suggested in Section 3.1. The modified frames and attributes are shown in shaded cells, while the newly created ones appear in unshaded cells. Additionally, an explanation of the frame or attribute can be found in the second to the right column, which is linked to the proposals in Section 3.1. The layers involved in every modification are shown in the far right column. A few of them are required only in Layers 2 and 2.5. Regarding the — MDER [74] — data types of the attributes, those with a fixed numeric value — indicated between brackets — are INT-U16, and the rest of them — hashes, HMACs, FingerPrints, etc. — are OCTET STRING. The types CHOICE and SEQUENCE (concatenation) are used to represent the combination of two or more attributes.

Similarly, a complementary illustration of the implications is provided in Figure 3.3. The figure shows a conveniently modified FSM of both agents and managers. Thus, it includes the existing states frames and attributes, along with the newly suggested sub-state (authenticating), and the new frames and attributes. The links between the new frames and the steps (noted as sX and suggested in Tables 3.2-3.4) are also shown in Figure 3.3. To differentiate existing and newly proposed states, frames and attributes, the latter are written in italics.

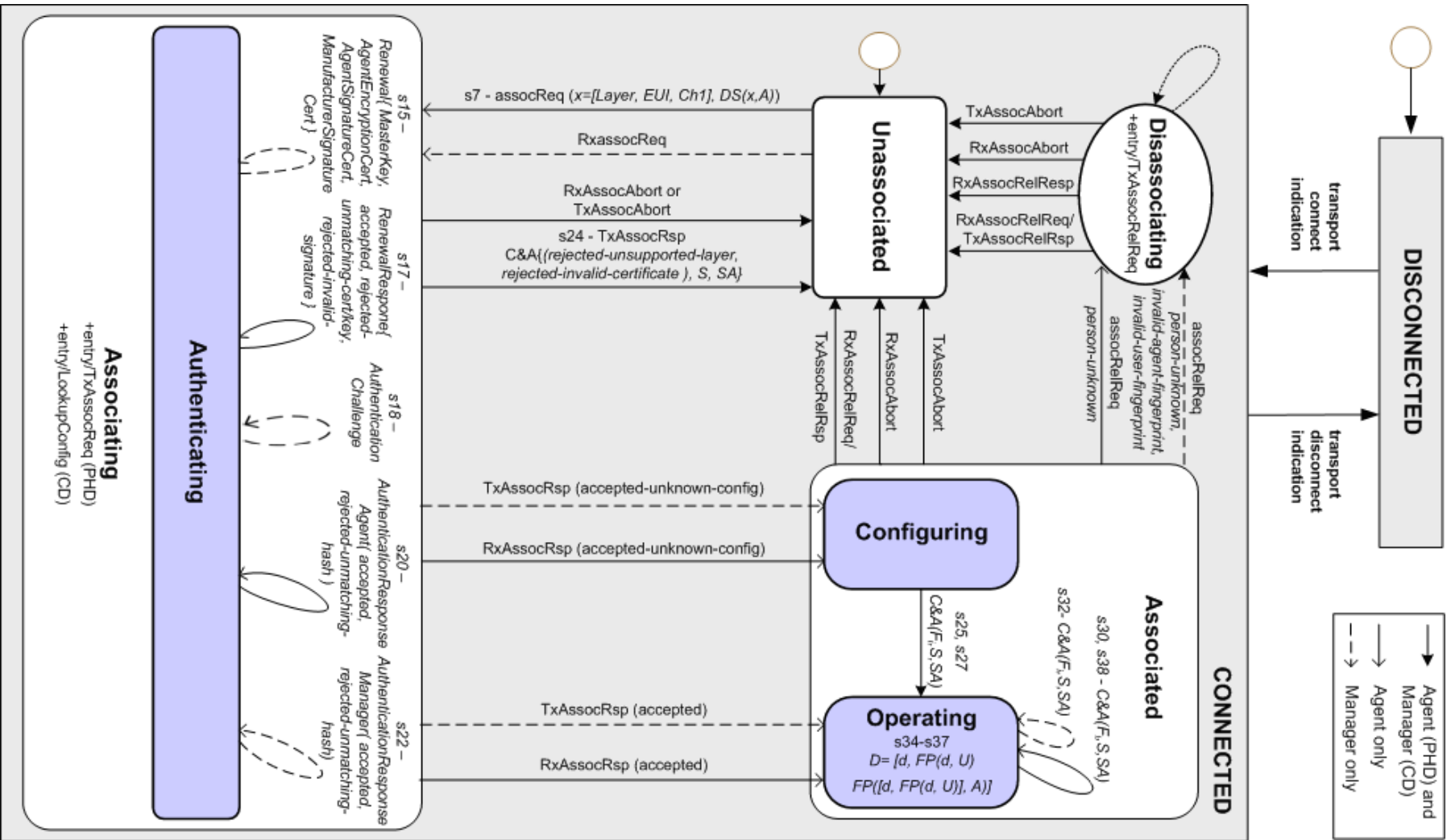


Figure 3.3: Proposed Finite State Machine (FSM) for both agents and managers, including the states frames, and attributes existing in the current approved version of X73PHD, along with the newly suggested sub-state (authenticating sub-state), and the new frames and attributes.

Table 3.6: Generic structures (lightly shaded cells), modified (shaded cells) and newly created (unshaded cells) frames and attributes in the extended X73PHD (I)

Frame	Sub-Frame (level 1)	Sub-Frame (level 2)	Sub-Frame (level 3)	Additional information	Security Layers	
AarqApdu	PhdAssociationInformation	ProtocolVersion	protocol-version4(3)	This bit shall be set if the extended version of 11073-20601 is supported.	0+	
		option list	RegCertDataList	It is recommended adding auth-body-IHE(3) to the AuthBody compliance list.	0+	
		Layer		This indicates the layer of the extended version of 11073-20601.	0+	
			zero(0)		0+	
			zero-and-a-half(1)		0+	
			one(2)		0+	
			one-and-a-half(3)		0+	
			two(4)		0+	
			two-and-a-half(5)		0+	
		RenewalRequest		Request to renew z, the master key and/or certain certificates, {MK, CEA, CSA, CSMf}.	1+	
			MasterKey(0)		1+	
			AgentEncryptionCert(1)		1+	
			AgentSignatureCert(2)		1+	
			ManufacturerSignatureCert(3)		1+	
			Challenge 1		This is the agent-to-manager challenge, Ch1.	1+
			DigitalSignature		Signature by the agent, DS(PhdAssociationInformation, PrSA).	1+

Table 3.7: Generic structures (lightly shaded cells), modified (shaded cells) and newly created (unshaded cells) frames and attributes in the extended X73PHD (II)

Frame	Sub-Frame (level 1)	Sub-Frame (level 3)	Additional information	Security Layers
RerqApdu			This is a manager-to-agent frame, encrypted with the public encr. key of the agent, PbEA.	1+
	Renewal{MasterKey, AgentEncryptionCert, AgentSignatureCert, ManufacturerSignatureCert}		[z_old, z]. Purpose: updating an old key/certificate with a new one.	1+
	DigitalSignature		Signature by the manufacturer, DS(Renewal{...}, PrSMf).	1+
RereApdu			This is an agent-to-manager frame.	1+
	ResultRenewal{MasterKey,	accepted	$h([z\_old, z])$ . Purpose: to approve the update of a key/cert.	1+
	AgentEncryptionCert,	rejected-unmatching- {key/cert}	$h([z, z\_old])$ . Purpose: to reject the update of a key/cert, z, because the value of the current key/cert in RerqApdu, z_old, was not correct.	1+
	AgentSignatureCert,	rejected-invalid-signature	$h([z, z\_old, z\_old])$ . Purpose: to reject the update of the key/cert because the signature in RerqApdu was invalid.	1+
	ManufacturerSignatureCert}			
AucApdu	AuthenticationChallenge		This is a manager-to-agent frame. It contains the manager-to-agent protected challenge, PbEA{Ch2}, concatenated with $h(Ch1+h(Ch2)+h(MK))$ . Purpose: to allow the agent verify that the manager knows MK.	1+
AurApdu			This could be both an agent-to-manager and a manager-to-agent frame.	1+
	AuthenticationResponseAgent		This is an agent-to-manager frame, based on hashes to hinder its manipulation.	1+
		accepted	$h(h(Ch1)+Ch2+h(MK))$ . Purpose: to verify positively AucApdu.	1+
		rejected-unmatching-hash	$h(h(Ch1)+h(Ch2)+h(MK))$ . Purpose: to indicate that AucApdu does not match the value calculated by the agent.	1+
	AuthenticationResponseManager		This is a manager-to-agent frame, based on hashes to hinder its manipulation.	1+
		accepted	$h(Ch2+1+h(MK))$ . Purpose: to verify AuthenticationResponseAgent positively.	1+
		rejected-unmatching-hash	$h(Ch2+2+h(MK))$ . Purpose: to indicate that AuthenticationResponseAgent does not match the value calculated by the manager.	1+

Table 3.8: Generic structures (lightly shaded cells), modified (shaded cells) and newly created (unshaded cells) frames and attributes in the extended X73PHD (III)

Frame	Sub-Frame (level 1)	Sub-Frame (level 2)	Sub-Frame (level 3)	Additional information	Security Layers
AareApdu	AssociateResult			Encrypted with session key S if Layer requires so.	1+
			rejected-unsupported-layer(9)		1+
			rejected-invalid-certificate(10)		1+
		HMAC		Hash Message Authentication Code, HMAC(AssociateResult, SA). Purpose: to authenticate AssociateResult.	1+
RlrqApdu	ReleaseRequestReason			ReleaseRequestReason travels encrypted with session key S if Layer requires so.	1+
			person-unknown(3)	This could be both an agent-to-manager and a manager-to-agent frame. Purpose: it is sent by the manager when it does not know the person to whom the data pertain, and by the agent when it checks that the manager does not know that person.	2+
			invalid-agent-fingerprint(4)	This is a manager-to-agent frame. Purpose: to indicate that the agent's fingerprint is invalid.	2+
			invalid-user-fingerprint(5)	This is a manager-to-agent frame. Purpose: to indicate that the the user's fingerprint is invalid.	2.5
		HMAC		HMAC(ReleaseRequestReason, SA).	1+
PrstApdu	DataApdu			DataApdu travels encrypted with session key S if Layer requires so.	1+
		Message	personID	If Layer $\leq 1.0$ , this is the PersonID as defined in 11073-20601 <sup>TM</sup> -2014 (16b). If $1.5 \leq \text{Layer} \leq 2.0$ , then PersonID takes the same value as the EUI-64 RFID-T/BC (64b). If Layer == 2.5, then PersonID is the Subject Unique Identifier of the X.509 CU (64b).	1+
			knownPerson	This is the hash of PersonID in agent-to-manager frames and PersonID otherwise.	2+
			FingerPrint	This is necessary if measurement data are present inside the frame.	2+
		Counter and HMAC		HMAC(DataApdu, SA).	1+

The creation of additional DIM attributes supporting the new security features could be useful for better modeling of PHDs. However, this is not imperative because not all transmitted information is modeled in the DIM. For example, within the PhdAssociationInformation frame, there is the ProtocolVersion information which is used to communicate acceptable X73PHD versions. ProtocolVersion is not modeled in the DIM, even though it provides information of what the agent is. The newly proposed Layer provides comparable information and therefore, according to the DIM definition it could be incorporated to the DIM but not necessarily. Similarly, in the PhdAssociationInformation frame, the RenewalRequest — defining requests to update some important keys or certificates — and the Challenge 1 could be added to the DIM if a new, security-enhanced version of the standard were to be created, but not compulsorily.

### 3.2.3 Impact on the ISO/IEEE 11073 PHD architecture and on its framework

This is evaluated in Table 3.9 by means of three reference examples, carefully chosen to cover a broad range of information transmission cases when using X73PHD. They have very different frame sizes —which affects the relative overhead— and may require real-time transmission —which is influenced by delays:

- Case 1: sending a discrete measurement, a weight represented with a frame of 36 bytes.
- Case 2: sending a continuous signal, a 3-lead ECG divided into 1-second blocks, sampled at 200 Hz and represented with 16 bits per sample. That is to say, blocks of 9600 bits. It is worth noting that this is a concrete —although rather common— set of parameters for ambulatory ECGs. Nonetheless, ECGs may range from a few seconds —e.g. 10 seconds in a resting ECG test— to several hours —e.g. in a Holter test. Regardless of their duration, the analysis of the features in the transmission of the security-enhanced signals at global scale is the same as per each individual signal block when real-time transmission is guaranteed [369]. Therefore, it is necessary to obtain an estimation of the computational power required to guarantee real-time operation.
- Case 3: sending measurement(s) in a frame whose size is the maximum allowed in X73PHD (63 KBytes). In this case, there is no real-time transmission involved. It consists of one large frame being transmitted in one go. It is worth noting that this is an extreme case.



Table 3.9: Absolute and relative overhead and delays of the new and modified frames proposed in Tables 3.6-3.8

Frame(s)	Entity	Case	Original size (b)	Absolute overhead (b)	Relative overhead	Delay (Mcycles)
s7, s8	A, M	1-3	54	16+64+512+512=1104	20.44	3.92
s14, s18	M	1-3	—	2048+256=2304	—	6.86
s19-s20	A	1-3	—	256	—	11.12
s21-s22	M	1-3	48	256-48=208	4.33	>0.01
s23	A, M	1-3	—	—	—	> 0.01
s25/s27	A/M	1-3	var	$\approx 128/2+176=240$	var	>0.01
s26/s28	M/A	1-3	—	—	—	>0.01
s30	A	1-3	—	256+176=432	—	>0.01
s31-32	M	1-3	26	128-26+176=278	10.69	>0.01
s33	A	1-3	—	—	—	>0.01
s35-s41, s46 — Layer 2.5 —	A, M	1, 2, 3	x= 288, 9600, 516096	1424, 1456, 1456 — $\text{ceil}((x+2 \cdot (64+512)+64)/128) \cdot 128+176-x$ —	4.94, 0.15, >0.01	22.73, 22.86, 29.95
s35-s40, s46 — Layer 2.0 —	A, M	1, 2, 3	Idem	912, 944, 944 — $\text{ceil}((x+2 \cdot 64+512+64)/128) \cdot 128+176-x$ —	3.17, 0.10, >0.01	12.25, 12.38, 19.47
s35, s38, s39, s46 — Layer 1.5 —	A, M	1, 2, 3	Idem	272, 304, 304 — $\text{ceil}((x+64)/128) \cdot 128+176-x$ —	0.94, 0.03, >0.01	0.89, 1.02, 8.11
s35, s39, s46 — Layer 1.0 —	A, M	1, 2, 3	Idem	272, 176, 176 — $\text{ceil}(x/128) \cdot 128+176-x$ —	0.94, 0.02, >0.01	0.31, 0.44, 7.53

The proposed extension of the protocol consists of 46 steps, described in Section 3.1. Nonetheless, only 16 of these steps introduce some overhead or delay, which are calculated based on the data provided in Section 2.6.3. The results in Table 3.9 show that the maximum overhead introduced by one step is 2304 bits. Although this can be considered as high (in relative terms) when the original frame is short (e.g. s7), it is almost negligible when protecting ECG signals or long measurements for transmission (Layers 1.0-2.5, cases 2 and 3). It is also worth noting that the relative overhead grows significantly with the layer when protecting short measurements (Layers 1.0-2.5, case 1), varying from 0.94 in Layer 1 to 4.94 in Layer 2.5. This is mainly due to the addition of the fingerprints of the user (s35) and the agent (s37). Regarding delays, each operation has either a fixed delay (a certain amount of cycles) or a variable delay, which depends on the input data size (e.g. in encryption). The latter is calculated by multiplying the speed of the operation and the data size. Some steps involve two or more sequential operations —e.g. those denoted as C&A()— and in that case their individual delays will be added. Therefore, the cells in the delay column are calculated by summing the delays produced by all operations involved for each row. It is observed that steps s35-s41 contribute most to the overall delay, which grows notably with each layer implemented. Short measurements and ECG signals (cases 1 and 2) obtain similar results (<1 Mcycle in Layers 1.x, about 12 Mcycles in Layer 2.0, about 23 Mcycles in Layer 2.5), while the same evaluation with the maximum frame size (case 3) obtains approximately 7 extra Mcycles.

One of the most demanding real-time application that can currently be supported by X73PHD is the transmission of ECGs, as in our case 2. Table 3.9 shows an associated delay of 22.86 Mcycles when implementing Layer 2.5, the most secure and complex, to protect the ECG block and access it. On the other hand, real-time ECG applications usually require that the overall delay, starting when the acquisition of the block begins and finishing when the block can be interpreted, is approximately  $\leq 2s$  [369]. Since the block length is 1s, there is 1s (disregarding the transmission delay) to execute 22.86 Mcycles in real-time. Assuming that the transport technology introduces low/moderate overhead and that it is able to transmit the protected ECG block (11056 bits) with a negligible delay, it is enough that the agent and the manager operate at approximately 23 MHz. If the manager features a much faster processor (e.g. >1 GHz), which is very typical in smartphones or tablets, the requirement for the agent can be dropped to 9 MHz. This happens because the selected algorithm, ECDSA, performs the signature (in the agent) with fewer operations than the signature checking (in the manager, which is usually a more powerful device). It is worth noting that, for these estimations, it has been assumed a throughput of 1 MIPS/MHz (1 million instructions per second per megahertz), which is a reasonable ratio in off-the-shelf 8-bit microcontrollers (e.g. the Atmel ATmega328). A simple 8-bit microcontroller was chosen as reference for the following reasons: a) an 8-bit

microcontroller is powerful enough to run a X73PHD agent [370, 371], b) manufacturers of medical devices look for cost-effective implementations, and c) by choosing an 8-bit architecture for the estimations, we are positioned in a scenario with limited processor capability (considering the current state-of-art), i.e. if the architecture is changed (e.g. a manager running in a mobile phone, which has for example an ARM Cortex micro, which is a much more powerful processor), the processor would have a larger MIPS/MHz throughput, which implies the capability of executing more instructions per clock cycle, and so the situation would be more favorable.

Regarding the impact of the X73PHD extension on its framework, a simple initial setup is required. As detailed in Section 3.1, an administrator installs his/her certificate in the manager (s4) and implements a XACML-based privacy policy setting out which users are authorized to take and/or consult measurements (s5). He/she may also pair/associate the agent and the manager with the most secure method implemented by the transport technology (s6). In addition to this, certain layers of the enhanced X73PHD —see Table 2.5— demand items to identify/authenticate users —which requires extra hardware—, the implementation of reliable PHRs in the manager and the implementation of IHE profiles to enable communications with healthcare systems. Nevertheless, the proposed enhancement of X73PHD does not hamper the automatic verification, access and processing of the acquired measurements and it would facilitate its integration with PHRs, EHRs and CDSS, and the triggering of alarms at abnormal values. Furthermore, when an authorized user accesses this data with his/her regular software, additional information about its associated features (layer, validity of timestamps and fingerprints) may be displayed.

With respect to the agent implementation, it is suggested a programming language featuring a reduced computational load, such as ANSI C. It is worth noting that the delays presented in Table 3.9 have been calculated based on the data in Table 2.8, corresponding to a speed benchmark of cryptographic algorithms coded in C++. Nevertheless, the programming language choice for the agent implementation falls directly on the developer (or the manufacturer), who would assume the inherent trade-off between scalability/easiness and computational efficiency. Managers, on the other hand, could be developed using a different programming language —e.g. Java in an Android-based manager. Java has the advantages of being highly portable and abstract but it is —generally speaking— less computationally efficient. However, since managers are, at the same time, more powerful devices, their performance would not be greatly affected.

### 3.2.4 Potential limitations

Although the proposal presented herein has several advantages over the regular non-extended standard, there are also some challenging caveats to be considered. In the first place, it is necessary to keep track of the discovery of potential vulnerabilities in the security algorithms implemented, so that the compromised algorithms can be replaced with the second options proposed in Section 2.6.3 (or by new, more secure algorithms that might be created in the future). Also, users of the system have to be appropriately trained in security practices, e.g. choice of strong passwords, remote activation/deactivation of identification credentials. Additionally, a reference implementation — which has not been carried out at the moment of writing — would be useful for testing purposes. In fact, a pilot evaluation comprising a variety of potential users (e.g. fitness enthusiasts, elderly people, hospital patients, physicians and systems administrators) would certainly be a reliable source for learning valuable lessons about the possible technical enhancements and potential social issues (e.g. reluctance to use personal authentication means) as well as the benefits of deploying and using this security framework in daily practice. Moreover, it would be mandatory to keep track of new versions of the standards and norms on which our proposal relies. Should a new version of the X73PHD standard or the IHE profiles be published, this security proposal must be revised to guarantee flawless adaptation to them. Finally, since there is ongoing work towards the inclusion of remote control in X73PHD personal health devices [372], it would be mandatory to review this eventual final document for two main reasons. First, it is necessary to check whether the new remote control feature compromises the security framework proposal. If so, the proposal must be modified to cover the new potential security breaches. Second, the new feature could be used to extend the security framework so that administrators can send security commands to personal health devices (e.g. force the device to use 256-bit key size — instead of 128-bit — in symmetric encryption, so that all devices comply with an eventual new recommendation of NIST, without the need for physical access to the device to update it).

### 3.3 Enhancement of the security of SCP-ECG

This section addresses the security enhancement of the SCP-ECG standard (Section 2.1.3), which specifies rules for the storage and exchange of ECG information — signal data, ECG measurement (e.g. the onset/offset of particular ECG wave-points such as the QRS), interpretation results and specific patient’s data — between ECG PHDs and CDs/HS. SCP-ECG is composed of a well defined and compact file format and a messaging part. Given that this standard has been successfully harmonized with the standard X73PHD [195], whose layer-based security extension has been addressed in Section 3.1, and that the messaging part of SCP-ECG is informative (but not normative), this proposal includes extending the SCP-ECG file format for its security enhancement and reusing the security-enhanced X73PHD (Section 3.1) for the exchange of ECG information. As illustrated in Figure 3.4, the ECG information would be acquired by the ECG PHD and sent to the CD (or directly to the HS) by using the extended X73PHD-IHE standard, where it would be stored according to the extended SCP-ECG format, which can be forwarded to HS (or to an end user) through secure channels. Therefore, it can be considered that this proposal extends the previous X73PHD-IHE framework — which implements the layered model defined in Section 2.6 — to a X73PHD-SCP-IHE framework. Moreover, this common framework aligns the security of both extensions and provides X73PHD with a secure and standardized storage format for ECG information and SCP-ECG with a secure and standardized communication protocol.

It is worth noting that the compliance of the SCP-ECG extension with the X73PHD-IHE framework can only be guaranteed if the former implements the newly-created IHE profile SDO:SST (Secure Device Observation – Secure Standard Storage), which is mandatory for Layers 1.0+ (Table 2.5) and corresponds to step 46 in Table 3.4. To fulfill this requirement, the protection policy for SCP-ECG files relies on cryptography and implements three basic and interrelated measures, explained in Section 3.3.1: role-based access control based on privacy profiles, adequate encryption of contents and addition of digital signatures. The formal security extension of regular SCP-ECG files addressing this protection policy is defined in Section 3.3.2.

#### 3.3.1 Privacy profiles for Role Based Access Control (RBAC)

As explained in Section 2.1.3, a SCP-ECG file may be divided into four parts with different sensitivity levels: **A**, identification of the patient and the elements involved in the ECG acquisition session; **[B]**, general patient data, health status and medication; **C**, ECG signal and **[D]**, ECG measurements and interpretation. In addition to this, it is worth noting that a SCP-ECG file can be requested for different purposes (see Figure 3.4), to

wit teaching, research, examination, diagnosis and storage. Both classification, parts of a SCP-ECG file and possible uses, have been taken into account for the definition of a RBAC policy that preserves the principles of data processing and purpose binding of privacy. The following privacy profiles, which include different privacy measures and access privileges (see Figure 3.5), were defined after consultation with three independent cardiologists:

0. *Teaching/research*

- Use: to disclose those parts useful for teaching/research (*[B]*, *C* and *[D]*).
- Privacy: *[B]*, *C* and *[D]* are in plaintext and *A* is replaced by a template with bogus values.
- Privileges: reading.

1. *Examination*

- Use: to allow clinicians caring for the patient to read the whole SCP-ECG.
- Privacy: all the parts are encrypted.
- Privileges: reading.

2. *Diagnosis*

- Use: to complement the file with additional data, such as the delineation of ECG fiducial points or the diagnosis of the cardiologist who interprets the ECG.
- Privacy: all the parts are encrypted.
- Privileges: reading all the parts, writing *[D]* and *tags 15, 17, 19-20* of part *A*, which identify the analyzing device, department, institution and physician.

3. *Storage*

- Use: secure storage.
- Privacy: encryption of all the parts.
- Privileges: making protected exact copies of the file, with no permission to interpret, write or modify the plaintext.

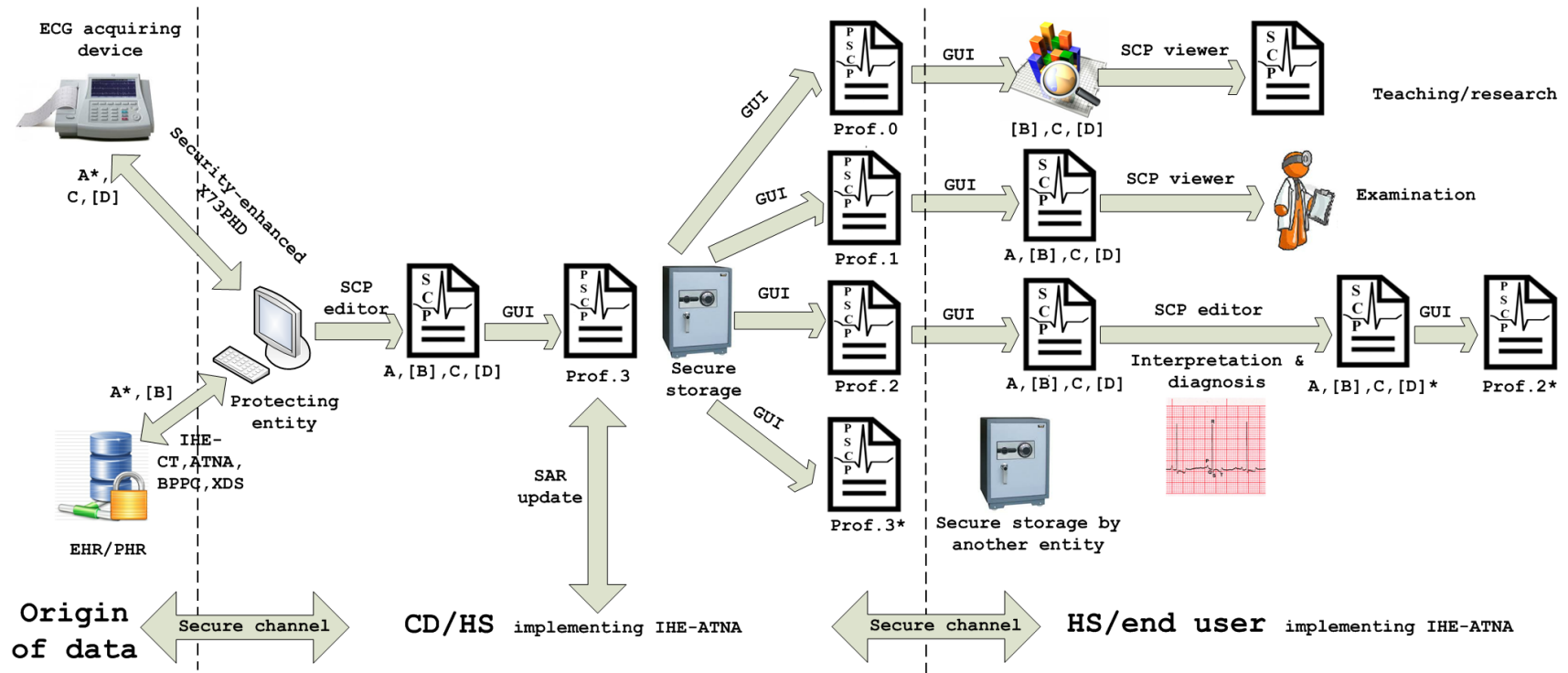


Figure 3.4: A scenario of use for the SCP-ECG security extension. Regular and security-enhanced SCP-ECG files are depicted in detail in Figures 2.3 and 3.5.

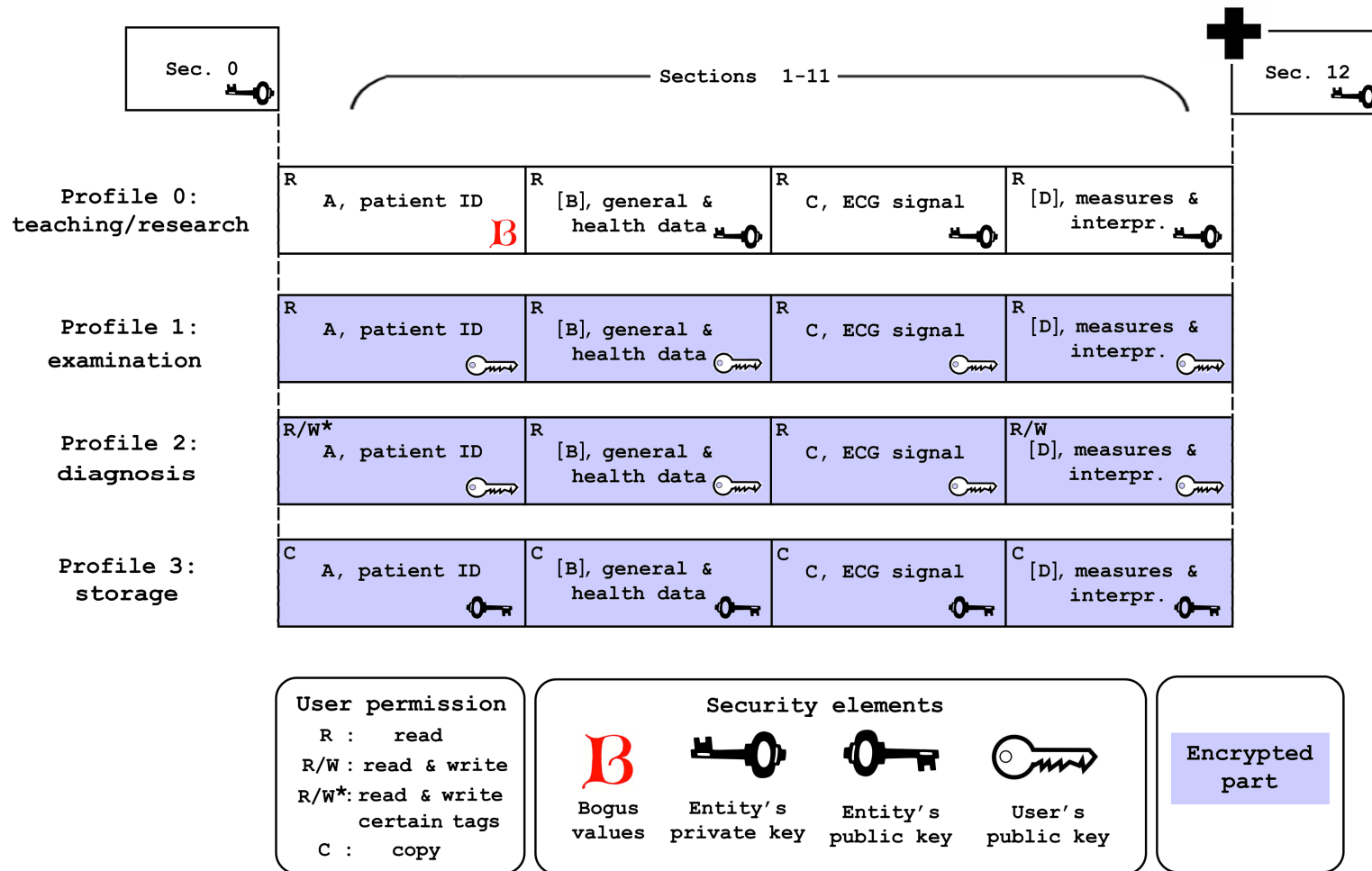


Figure 3.5: Security-enhanced SCP-ECG file types depending on its profile (Section 3.3.1). It shows which security element ultimately protect each part and which access privileges correspond to the intended *user(s)*. Section 0, parts *A*, *[B]*, *C* and *[D]* defined in Figure 2.3, section 12 defined in Table 3.10.



These privacy profiles implement part-level encryption in a manner similar to that of the Context Envelopes defined by DICOM. The content of the parts is sealed by means of encryption and the syntax to make them verifiable and retrievable to the targeted user(s) is placed in a new section (Section 3.3.2). As in the X73PHD extension, this proposal combines symmetric encryption, asymmetric encryption and digital signatures for an optimal security-performance tradeoff, and it follows the suggestions for the choice of algorithms of the SDO profile (Section 2.6.3). As regards to supporting several profiles in a single SCP-ECG, this is not recommended since it would lead to too large an increase in the size of the syntax with respect to the average size of a SCP-ECG file. In summary, each security-enhanced SCP-ECG file is generated on demand in the CD — it could also be generated in other points of the architecture, such as in the HS to protect already stored regular SCP-ECG files — from its regular counterpart, choosing the best-fitted privacy profile according to the information retrieved from the IHE profile XDS and BPPC — implemented by CDs and HS integrated in the X73PHD-SCP-IHE framework.

### 3.3.2 SCP-ECG extension

The SCP-ECG is a well defined protocol, which can be extended by defining new sections (numbers 12 to 127 and those above 1023, see [212]) or employing existing free spaces. Since security is not addressed in any existing section, it is proposed dedicating an entirely new section to enhance the security of SCP-ECG files according to the proposal in Section 3.3.1. The notation regarding cryptographic elements of this extension is contained in Table 3.1. To avoid confusion with regular files we call this new format security-enhanced (or protected) SCP-ECG. The files are given the extension `.pscp` for easy distinction.

#### Section 12 structure

Like the rest of the SCP-ECG sections, this is divided into two parts:

- The **Section ID Header**, which is common to all the sections in this standard (Figure 2.3) and precedes the Data Part. It is composed of:
  - Bytes 1 to 2: 16 bit **CRC-CCITT** over the entire section (excluding these two bytes).
  - Bytes 3 to 4: **Section ID number**.
  - Bytes 5 to 8: **Section length** including the Section ID header (in bytes).
  - Byte 9: **Version Number of the Section**.
  - Byte 10: **Version Number of the Protocol**.

- Byte 11 to 16: **Reserved**.
- The **Data Part** (Table 3.10), which adopts the structure corresponding to Section 1 to allow the flexible storage of several fields of variable length. Each field details the options (e.g. privacy profile, cryptographic algorithms and parameter values) to set up a security-enhanced SCP-ECG file. These are described by:
  - The corresponding **tag**: a specification byte which indicates the field we refer to. It would be possible to use up to 255 different tags, although only 7 are required.
  - The **length**: a 2-byte specification indicating the length of the field value (in bytes). The maximum possible length described by 2 unsigned bytes is 65535 bytes, but in practice this value is much lower.
  - The **parameter data**: the content of the field, an element to provide security. If *length* == 0, the *parameter data* of the corresponding *tag* is empty.

Finally, it is necessary to add the corresponding pointer in Section 0 (Figure 2.3) to address the new section, indicating: section ID number (2 bytes): 12, section length (4 bytes) and index to section (4 bytes).

### Section 12 content

The tags included in Section 12 (Table 3.10) enable the security measures under this extension:

- **Role-Based Access Control** by means of privacy profiles (RBAC, Section 3.3.1).  
Tag involved:
  0. Specifies the professional role of the user, the ECG file is protected accordingly.
- **Digital signature** (DS) to verify the reliability of the ECG signal and the rest of the data — thus, protecting against forgery and manipulation. Tags involved:
  1. CSE, identifies the entity generating the security-enhanced SCP-ECG file and contains his/her public key for signature, PbSE.
  2. Specifies which hash function has been used, taking as input the whole file.
  3. Stores the DS, resulting from the encryption of the hash with the private key of the protecting entity, PrSE.
- **Part-level encryption**: which maintains confidentiality according to the consent of the patient. Tags involved:

Table 3.10: Structure and content of the Section 12 Data Part of a security-enhanced SCP-ECG file

Tag	Length	Value (parameter data)				
0	1 byte	<b>Privacy profile</b>	Value	Type		
			0	Teaching/research		
			1	Examination		
			2	Diagnosis		
			3	Storage		
1	length	<p><b>Certificate of the entity generating the security-enhanced file</b> (PEM coding):                      The certificate shall be X.509 type. Three different public key algorithms are allowed for signature: <b>ECDSA</b> (<math>\geq 224</math>, recommended <b>256</b>), <b>DSA</b> (<math>\geq 2048</math>) and <b>RSA</b> (<math>\geq 2048</math>). See Table 3.11 for certificate sizes.</p>				
2	1 byte	<b>Hash function ID</b>	Value	Algorithm		
			0	<b>RIPEMD-256</b>		
			1	Whirlpool		
			2	SHA-256		
3	length	<p><b>Digital signature</b>, <math>DS(pSCP - ECG, PrSE)</math>                      This is the encryption of the hash using the private key for signature of the entity generating the file (<math>PrSE</math>, initially <math>DS = \text{blank}</math>). At the user's end the <math>DS</math> is used to verify the integrity and authenticate the file. The length of the <math>DS</math> depends on the type of entity's certificate for signature (tag 1), see Table 3.11.</p>				
4	1 byte	<b>Symmetric encryption algorithm ID</b>	Value	Algorithm		
			0	<b>Twofish</b>		
			1	Serpent		
			2	RC6		
			3	MARS		
			4	AES		
5	length	<p><b>Encrypted symmetric key(s)</b>, <math>encrypt(S, Tag\ 4, PbEU)</math>                      The symmetric encryption key(s) <math>S</math> — to be used for encrypting the confidential sections — are generated with a secure random function and encrypted with the public key specified in the user's certificate, <math>PbEU</math> (entity's certificate in profile 3). Thus, the length of this field depends on the user's certificate type, see Table 3.11. This field is not present in profile 0 (tag 0), since there is no encrypted parts.</p>				
<b>Secure access record, SAR.</b>						
6	25-n bytes	Each entry is:	Byte	Name	Type	Notes
			1 to 15	<b>Certificate issuer, Common Name</b>	ASCII	
			16 to 20	<b>Certificate serial number</b>	Integer	
			21	<b>Type of access</b>	Integer	Allowed values: 0 to 3
			22 to 25	<b>Request date</b>	Integer	Seconds since January 1, 1970, 00:00:00 GMT
For profiles 0-2 there is only one entry, for profile 3 there may be several.						

0. Indicates which parts of the file are private (Section 3.3.1).
4. Specifies which symmetric cipher is used to encrypt the content of the private parts.
5. Stores the symmetric key(s), randomly generated and protected by the public key of each authorized user.

Only the intended user can recover the symmetric key(s) and decrypt the confidential parts of the file, for which he/she needs to load his/her private key.

- **Secure Access Record (SAR)**, which reinforces the implementation of the ATNA profile in the provision of transparency to the patient. Tag involved:

6. Has a double mission: to identify publicly and uniquely the intended user for privacy profiles 0-2 and to keep an updated copy of all granted accesses for profile 3. The protecting entity can immediately export this list for patient consultation.

## 3.4 Evaluation of the security-enhanced SCP-ECG

This section begins evaluating the security of the proposal in Section 3.3 against different threats (Section 3.4.1). Next, the implications of this extension for the SCP-ECG file format and its performance are analyzed (Section 3.4.2). Finally, the potential limitations of this proposal are summarized (Section 3.4.3).

### 3.4.1 Risk assessment

The security-enhanced format for SCP-ECG files, to be managed by CDs and HS (maybe also by PHDs) in secure m-Health architectures, involves cryptographic elements, publicly stored in the newly created Section 12 of these extended files. In this proposal, it is considered that plain SCP-ECG files will be totally replaced by their security-enhanced counterparts, that the variables created in the processes of protection and access will be thoroughly cleaned and that the private keys involved will be managed adequately. Therefore, the possibility that an attacker accesses a CD or a HS and finds unprotected SCP-ECG files, relevant ECG information or private keys — e.g. in the hard drive, in the RAM memory or in cache — is excluded. Regarding the security-enhanced SCP-ECG files, they cannot be considered as hard to obtain always since their transmission in the BAN/PAN may be wireless — with a security configuration that may be inadequate — and because some patients may cooperate in granting access (with their informed consent) to

their biomedical tests (or part of them) for certain m-Health applications — e.g. research — under strict RBAC, which increases the number of requests for SCP-ECG files (and the number of potential opportunities for attackers accordingly).

An attacker with access to security-enhanced SCP-ECG files may try to perform certain attack(s). The following risk assessment analyzes attacks depending on the actions intended by the attacker and the cryptographic elements he/she needs access to.

- Unauthorized reading of confidential parts from security-enhanced SCP-ECGs. Its Section 12 contains the syntax to read the contents that are confidential, and given its relevance, it is protected with asymmetric encryption. Breaking this encryption or obtaining the private key(s) from an authorized user is considered highly unlikely. Therefore, the only opportunity for an attacker is attempting a brute-force attack on each individual confidential section — since they are encrypted with independent symmetric encryption keys —, which has a low success likelihood.
- Generation of forged security-enhanced SCP-ECG files. Anyone can create his/her own security-enhanced SCP-ECG files, since the procedure is public. However, attempting to forge the origin of the biomedical test requires generating a legitimate digital signature from a trusted entity (e.g. a rightful CD). To do so, the attacker would need to break or steal the private key of a trusted entity — which is highly unlikely if appropriately protected.
- Malicious removal of legitimate contents from security-enhanced SCP-ECG files. An attacker may remove certain parts of a legitimate file. Nonetheless, this would lead to a failed verification of the digital signature embedded in its Section 12, which will alert authorized users about the tampering.
- Malicious edition of legitimate security-enhanced SCP-ECG files. This is a combination of the previous types of attack. It requires knowing the plain contents of the file (thus, breaking the encryption of the confidential parts), editing certain part(s) (as intended by the attacker) and re-protect the SCP-ECG file. The last step includes re-encrypting the confidential parts of the file and replacing the previous signature with a new valid one, the latter requiring the private key of a trusted entity — which is highly unlikely to obtain.

Therefore, this analysis demonstrates that extended SCP-ECG files feature adequate levels of security.

Table 3.11: Typical size (KB) of Section 12 fields of a security-enhanced SCP-ECG file

Entity's certificate type	Tag 1	Tag 3	User's certificate type	Tag 5
ECDSA 224	0.6	0.06		
ECDSA 256	0.6	0.06	RSA 2048	0.26
DSA 2048	1.6	0.05	RSA 4096	0.51
DSA 4096	2.6	0.05		
RSA 2048	1.1	0.26	Tags 0, 2, 4	Tag 6
RSA 4096	1.8	0.51	0.003	$0.025 \cdot \#entries$

### 3.4.2 Implications for SCP-ECG and impact on its architecture

The main implications for this standard are the addition of the new Section 12, the encryption of confidential contents — which depends on the privacy profile implemented — and the coordination with the security-enhanced ISO/IEEE 11073 PHD standard for the exchange of ECG information. The use of encryption has a severe distortion effect on confidential SCP-ECG parts. This effect has been evaluated on 30 SCP-ECG files from [www.openecg.net](http://www.openecg.net), by calculating the normalized cross correlation,  $corr \in [0, 1]$ , between all pairs of metadata and signals from different files. Related signal pairs, such as leads from the same patient record, obtained  $corr$  values higher than 0.6 while unrelated signal (and metadata) pairs obtained values close to 0. As expected, the  $corr$  values between pairs of original signals/metadata and their encrypted counterparts were also close to 0, showing the decorrelation power of encryption.

On the other hand, the security extension of SCP-ECG files also results in a different file size and access time:

- *File size.* The addition of Section 12 implies dealing with bigger files, which will increase the size of the file database and the time used for the transmission of these files. As shown in Table 3.11, the main factors are the certificate type of the entity generating the protected file (Tag 1), which also determines the length of the DS (Tag 3), and the user's certificate type, which fixes the encrypted symmetric key(s) length (Tag 5). They account for approximately 95%-99% of the section size. The contribution of the rest of the fields (hash function ID, symmetric encryption ID, etc.) is very low.

For security-enhanced SCP-ECG files implementing privacy profile 3 the number of

entries in Tag 6 may grow substantially, so it is proposed limiting this field to the last 40 accesses (1 KB). Notice in Table 3.10 that Tag 5 is not included for profile 0. The section size ranges from 0.66 (profile 0 with ECDSA 224/256 entity's cert, — Tag 5 is empty, 1 entry in Tag 6) to 4.16 KB (profile 3 with RSA 4096 entity's cert for encryption in Tag 5, DSA 4096 entity's cert for signature in Tags 1, 3 and 40 accesses in Tag 6). Since the size of a typical SCP-ECG file is 31 KB (Section 2.1.3), the typical overhead is within  $0.66/31 - 4.16/31 \simeq 2 - 13.4\%$ . When taking the minimum file size (7.4 KB), the overhead ranges from  $0.66/7.4 \simeq 9\%$  to  $4.16/7.4 \simeq 56.2\%$ . These results show the importance of choosing ECDSA certificates to reduce the overhead without security degradation. Finally, the overhead for the maximum file size (355 KB) ranges from  $0.66/355 \simeq 0.2\%$  to  $4.16/355 \simeq 1.2\%$ .

- *Protection-access time.* This is the average delay introduced by the operations described in Section 3.3.2 through a software implementation (Section 3.5):
  - Security enhancement of a regular SCP-ECG file: typically 0.5-1 s.
  - Access to the contents of a security-enhanced SCP-ECG file: typically 0.5-1 s.
  - Generation of a security-enhanced SCP-ECG file (profiles 0-3) from another security-enhanced SCP-ECG file (profile 3, Figure 3.4): typically 1.5-2.5 s.

The last procedure takes longer because it implies accessing the confidential contents and protecting again twice (one time to update the secure access record in the file of the protecting entity and add a new signature, and another to produce the whole user's file). Comparing the time to generate the contents of a SCP-ECG file ( $\simeq 10-30$  s) and the delay to protect it, the latter is only  $\simeq 2-10\%$ . Comparing the delay to access a security-enhanced file to the time to represent its contents and interpret them ( $\geq 1$  min), the former represents only  $\leq 5\%$ .

To provide a reference of the performance, all the tests were executed on an Intel Core 2 CPU E850 at 3.16 GHz running Windows XP.

### 3.4.3 Potential limitations

Given the simplicity of this format extension, the only potential limitations might come from the discovery of vulnerabilities in the algorithms implementing the cryptographic functions used. Since the choice of algorithms falls directly in the newly proposed SDO (IHE) profile (Section 2.6.3), any related issue shall be solved from there, by updating periodically the list of algorithms — including novel, highly secure algorithms and removing those vulnerable or less secure.

### 3.5 Proof of concept

It has been built a simple graphical user interface (Figure 3.6) that implements the procedures depicted in Figure 3.4 in order to provide users (clinicians, researchers, hospital system administrators, etc.) with a way to protect their SCP-ECG files and access them easily. Thus, this GUI guarantees the compliance of the extension proposed with regular SCP-ECG equipment and software (viewers, editors, parsers). If this extension is adopted officially, ECG devices will be able to provide security-enhanced SCP-ECG files and SCP-ECG viewers will be able to show their contents using the software principles already implemented in this GUI.

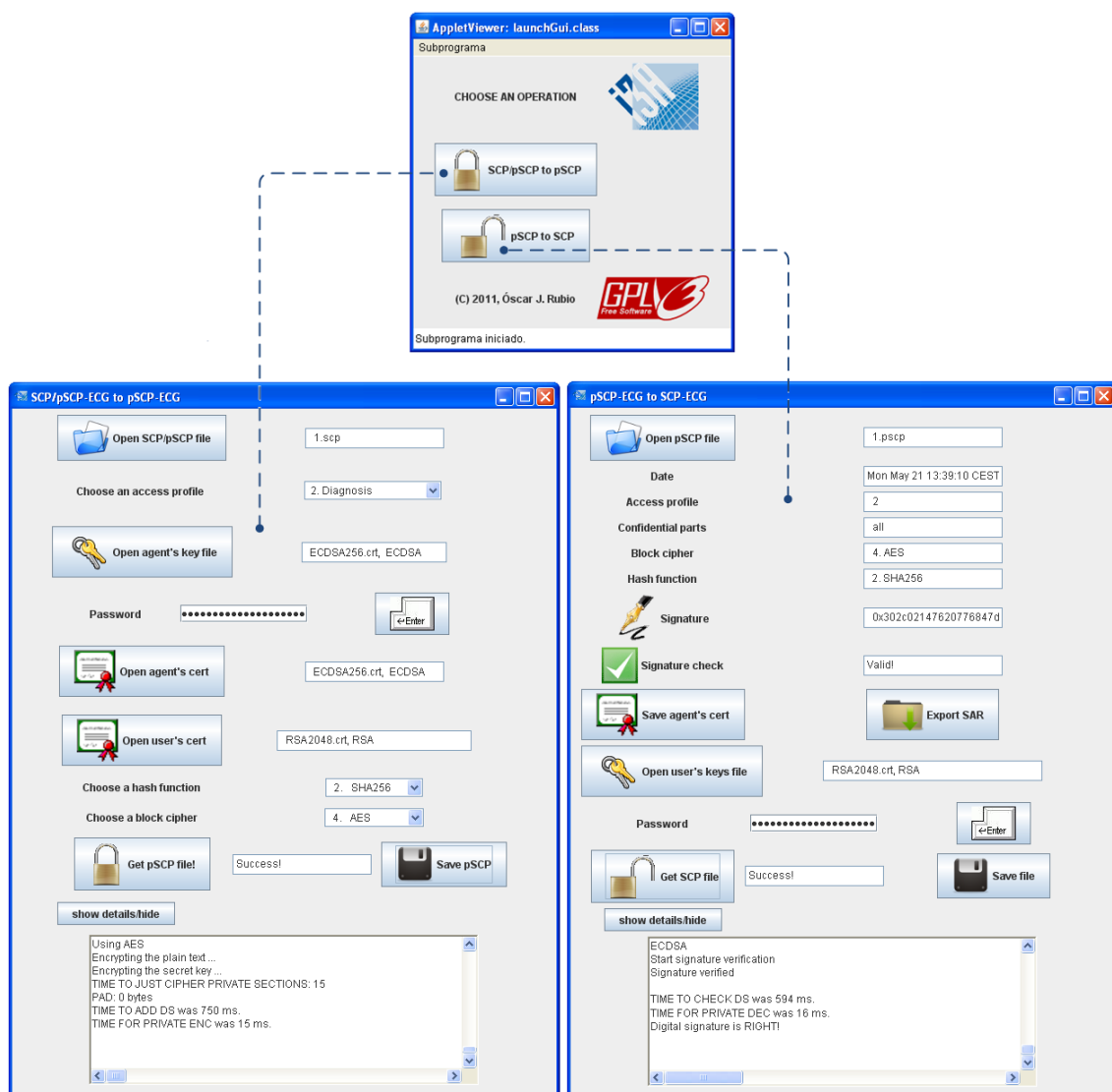


Figure 3.6: SCP-ECG ↔ Security-enhanced SCP-ECG graphical user interface. A scenario of use for this GUI is illustrated in Figure 3.4.



All the operations of encryption, decryption, writing and checking are carried out by the application. Nevertheless, some interaction is required:

- With the entity that protects the regular SCP-ECG file — he/she shall (1) set the privacy profile, (2) choose the symmetric cipher and (3) the hash function, (4) load his/her certificate, (5) his/her private key and (6) the users' certificates. The set [symmetric encryption algorithm ID, hash function ID, protecting entity's certificate and protecting entity's private key] can be fixed to save time. It is recommended using [Twofish, RIPEMD-256, ECDSA  $\geq$  256 for signature].
- With the user that accesses a security-enhanced SCP-ECG file — to access the confidential parts in the protected file he/she shall load his/her private key (not necessary for profile 0).

This GUI is openly available at <http://sourceforge.net/projects/pscp/>, also as an *applet* for integration in web pages.

## 3.6 Conclusions

The main objective of this Chapter was to illustrate the procedures and considerations involved in the security extension of biomedical standards according to the global, layer-based proposal in Chapter 2. Furthermore, this chapter has exemplified the extension of two well-known standards that previously featured an insufficient enforcement of basic security requirements: X73PHD and SCP-ECG. The main conclusions regarding these extensions are summarized below:

- The proposal and evaluation of the security-enhanced version of X73PHD indicates that it not only maintains, but also augments, the defining features of the original X73PHD. In fact, the agent can persistently store the acquired measurements, with security; the manager can establish associations with different agents at the same time, by negotiating differentiated layers, and it can also communicate with PHRs, EHRs, alert managers and CDSS; the manager is able to access and process all the information without human intervention and also to show authorized users additional information regarding security and interoperability features. The security assessment demonstrates that the implementation of any layer proposed includes at least one countermeasure against each threat affecting the m-Health applications intended for that layer, and that the number of countermeasures grows with the layer implemented. As regards to the costs involved, it can be considered that the modification that this extension produces in the three models defining X73PHD are moderate. It is not required extending the DIM with new attributes; the new service

model adds four new frames and extends another four with new sub-frames (most of them common to all layers); and the communication model only adds one new sub-state, ‘Authenticating’. Furthermore, the enhanced X73PHD architecture can be considered lightweight since an agent with a simple 9 MHz processor (assuming a throughput of 1 MIPS/MHz) can implement the top layer and transmit a 3-lead ECG in real-time to a manager with a one-core processor at 1 GHz (also assuming the same throughput). As regards to the surrounding framework, it is required that an administrator initially configures the agent and the manager, that users sharing these devices have tokens for identification/authentication, and that managers implement certain IHE profiles to enable their integration with healthcare systems.

- The security enhancement of SCP-ECG relies on the extension of its file format and on the exchange of ECG data through the security-enhanced X73PHD. The design of this security extension prioritizes its robustness and the ease of use for clinicians caring for the patient, cardiologists who interpret ECGs, researchers, teachers and hospital system administrators, who can keep using their regular SCP-ECG devices, editors and viewers. The intermediate software developed in this work to protect SCP-ECG files and access the protected files is openly available. An adequate level of resistance to attacks against the security of the files and the privacy of the personal health information is achieved by means of cryptography. Since this is an evolving field, the list of cryptographic algorithms proposed (and the order of preference) are specified in the SDO profile, which will be updated periodically. The costs required to perform the security-enhancement of the files and the further access to the contents are low or moderate: typically 2 – 13.4% of overhead with respect to the size of a regular file, 2 – 10% extra delay to protect a newly generated SCP-ECG file and  $\leq 5\%$  extra delay to access it for interpretation. Thus, a good level of availability of the test is technically feasible. Finally, this extension follows the guidelines for security standardization since it implements role-based access control, digital signature, part-level encryption and registry of accesses to carry out the secure storage of (ECG-related) biomedical contents, which correspond to the SST part of the SDO profile.

To sum up, these two interrelated proposals follow the guidelines of the global security proposal and provide efficient and standardized solutions for the acquisition, exchange and storage of biomedical information — mainly in the BAN/PAN part of the m-Health architecture. Moreover, it can also be considered that these extension of X73PHD and SCP-ECG achieve security levels in line with those of reference biomedical standards, such as DICOM and HL7, with low or moderate costs.

*“Innovation distinguishes between a leader and a follower.”*

Steve Jobs

*“Doubt is not a pleasant state of mind, but certainty is absurd.”*

François-Marie Arouet Voltaire

*“The most important thing in science is not so much to obtain new facts as to discover new ways of thinking about them.”*

Sir William Bragg

# 4

## Enhancement of the security of biomedical tests through their associated signals

This Chapter deals with the blocks of the proposal for a secure, cost-efficient, m-Health architecture that are surrounded in red in Figure 4.1. Once the layer-based security scheme has been designed (blue block in Figure 4.1) and weak biomedical standards have been extended according to it (dark green block in Figure 4.1), there is still room for enhancing the security of biomedical tests, which may be managed by means of biomedical standards but may also be handled out of these formats — given its intrinsic clinical value. Since the protection of biomedical standards is entirely based on cryptographic resources, the application of another type of resources (which may be combined with traditional cryptography), relying on different security principles, seems the most adequate to strengthen the protection of biomedical tests. Particularly, the two security techniques described herein are based on signals, which are the core components of most biomedical tests. The first technique enables an efficient and secure coding of biomedical test by embedding their periodic measurements and contextual information into their biomedical signals (Section 4.1). Its performance — signal distortion, embedding capacity, delays, bandwidth requirements — is thoroughly evaluated, by means of various ECG and EEG-based tests (Section 4.2), and implemented as a proof-of-concept (Section 4.3). Next, it is proposed the implementation of various secure m-Health applications based on this coding (Section 4.4). Then, the second signal-based technique, called keytagging, details a procedure for the association of information to images in a secure, cost-efficient and non-distorting manner (Section 4.5). The major features of keytagging — robustness-

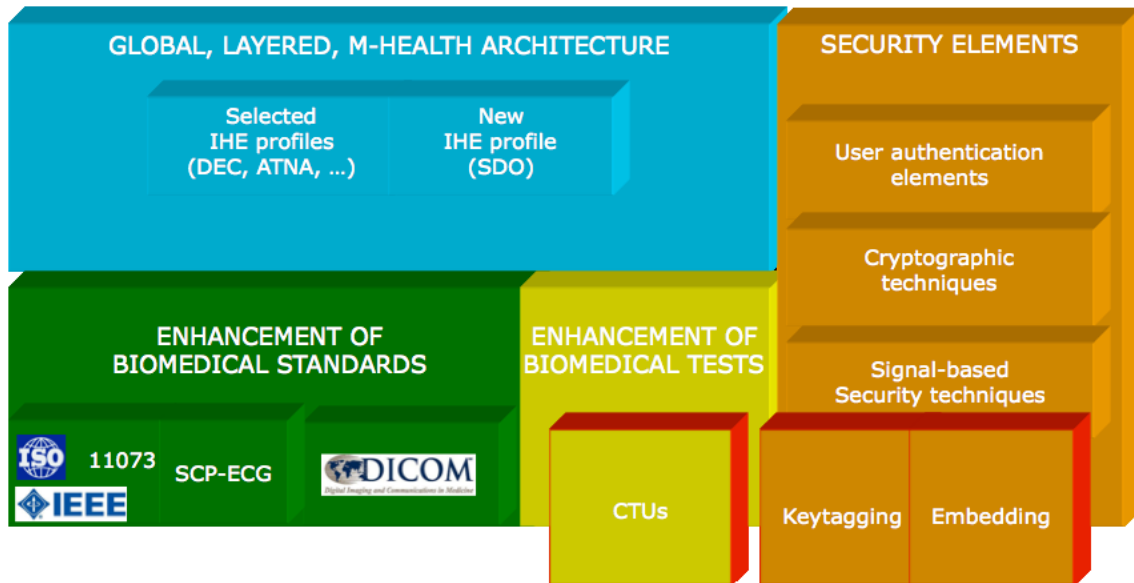


Figure 4.1: Building blocks for a secure, cost-efficient, m-Health architecture. Contents addressed in Chapter 4 surrounded in red.

capacity tradeoff, specificity, compliance with compression, runtime cost, scalability — are experimentally tested (Section 4.6) and taken into account to define the operating parameters of a variety of keytagging-based security measures (Section 4.7). Finally, the main conclusions of this Chapter are drawn (Section 4.8).

## 4.1 Novel coding for biomedical tests

The first signal-based security technique developed in this Thesis, a novel coding for biomedical tests based on embedding, is presented, analyzed and evaluated throughout Sections 4.1-4.4 and 4.8. Its notation is summarized in Table 4.1. The outline of the new cryptosteganographic coding for biomedical tests composed of signals (e.g. ECGs), periodic measurements (e.g. oxygen in blood, body temperature) and contextual data (e.g. allergies, medication of the user) is formally defined in Algorithms 1-2, illustrated in Figure 4.2 by means of an example and explained in detail in Sections 4.1.1-4.1.3. It is worth mentioning that this coding is mainly intended for Personal/Body Area Networks, being the biomedical test acquired by a device with multiple interfaces and sensors connected to it. The acquiring device will encode this information with this novel coding, which fulfills the requirements in Section 1.2.2 by integrating appropriate methods for signal compression, embedding of additional metadata — contents of the test and elements to provide security and privacy — and partial encryption of the signal. Real-time coding/decoding is feasible since the coder works with length-adjustable signal blocks to

Table 4.1: Operators and notation of the algorithm for coding biomedical tests

Notation	Meaning
$output(s) \leftarrow f(input(s))$	Assignment of value to one or several outputs from a function or operator $f()$ with one or several inputs.
$[ ]$	Concatenation operator.
$\oplus$	Binary XOR operator.
$\{X\}$	Set of elements of type $X$ , each element $i$ represented as $X\{i\}$ .
$\#X$	Number of elements that compose the set $X$ .
$V(i : j : k)$	Vector derived from a vector $V$ , corresponding to a subset of its elements, $[V(i), V(i + j), V(i + 2 \cdot j), \dots, V(k)]$ .
$S$	Vector corresponding to a signal associated to a biomedical test.
$Th$	Distortion threshold allowed after the processing of $S$ .
$contents$	Vector corresponding to periodic measurements and/or contextual information associated to a biomedical test.
$CTU$	<i>Coded Test Unit</i> , see Figure 4.2.
$CTU_p$	Plain (not partially encrypted) <i>Coded Test Unit</i> , see Figure 4.2.
$RC$	<i>Recovery Container</i> , defined in Table 4.2.
$lengthNoise$	Length of the noisy vector to be hosted between two consecutive <i>containers</i> in order to hide their locations.
$IV$	<i>Initialization Vector</i> , to be used for the partial encryption of a $CTU_p$ .
$w_{coef} \leftarrow WT(S)$	Function that performs the wavelet transformation of a signal $S$ and returns the resulting coefficients, $w_{coef}$
$SPIHT_b, pointer \leftarrow compress(S, SPIHT, Th)$	Wavelet transformation of $S$ and encoding of the resulting coefficients with the SPIHT coder, which returns a bitframe $SPIHT_b$ that truncated at $pointer$ and reconstructed returns $S$ with a distortion of $Th$ .
$S \leftarrow decompress(SPIHT_b, SPIHT)$	Reconstruction of a signal $S$ from its $SPIHT_b$ bitframe. The former will have some degree of distortion if the latter has been truncated.
$w_{SPIHT}, LIS, LIP, LSP \leftarrow decodeWavelet(SPIHT_b)$	Reconstruction of the wavelet coefficients, $w_{SPIHT}$ , of the $SPIHT_b$ bitframe. It can also return the three lists involved in the decoding, $LIS$ , $LIP$ and $LSP$ .
$w_{added} \leftarrow decodeWavelet(SPIHT_b, index1, index2, LIS, LIP, LSP)$	Reconstruction of the wavelet coefficients corresponding to the segment of $SPIHT_b$ from $index1 + 1$ to $index2$ . The process can be boosted by providing the $LIS$ , $LIP$ and $LSP$ of the reconstruction of $SPIHT_b(1 : index1)$ .
$Sk$	Secret key used for symmetric encryption-decryption.
$PrU$	Private key to be used by user $U$ for asymmetric decryption of data or for its signature.
$PbU$	Public key of user $U$ , used by any user for asymmetric encryption of data intended for $U$ , or to verify any signature issued by $U$ .
$DS(D, Alg, PrU)$	Digital signature of $D$ using the algorithm Alg and the private key of $U$ .
$checkDS(D, Alg, PbU)$	Verification of the $DS$ of $D$ by using the algorithm Alg public key of $U$ .
$encrypt(Plaintext, Alg, K)$	Encryption of <i>Plaintext</i> using the algorithm Alg and the key $K$ .
$decrypt(Ciphertext, Alg, K)$	Decryption of <i>Ciphertext</i> using the algorithm Alg and the key $K$ .

constrain the delays, producing *Coded Test Units (CTUs)*. As shown in Figure 1.5, within the m-Health scenario these *CTUs* may be sent from the acquiring-coding device to one or several concentrator devices (e.g. aggregators), which in turn may re-forward them to other systems (e.g. PHRs and/or EHRs). Regardless the device/system storing *CTUs*, the access to the signal(s), measurements and data that they contain is limited according to the professional role(s) of the consulting user(s). Particularly, access to the signal can be provided to any user (under the consent of the patient) by providing the plain *CTU*, which would be decompressed as a whole — maintaining the secrecy of the metadata embedded. Complementarily, users who know the coding of *CTUs* can always access their authorized contents and detect if there is corruption. Furthermore, this coding is designed to prevent unauthorized users/attackers from accessing contents, not only by encrypting them, but also by hiding their locations within the *CTUs*.

#### 4.1.1 Signal compression

The signal compression process appears in Algorithm 1: line 2. As detailed in Sections 2.2.1-2.2.2, the combination of the wavelet transform and the 1D SPIHT coder is well tailored for the compression of 1D biomedical signals. It offers a good compression-distortion tradeoff and counts with noteworthy features, such as progressive lossy to lossless coding, low complexity (use of simple operators), moderate memory usage and symmetric coding-decoding. Precisely the SPIHT decompression of the signal appears in Algorithm 2: line 11. Another outstanding property of this coder is that large amounts of data can be embedded and retrieved from truncated SPIHT bitframes with simplicity and secrecy. To enable real-time operation and reduce memory demanding, the signal is divided into short, non-overlapping and equal-length blocks  $S$ , prior to compression. In offline mode, longer block lengths are recommended, since the content of the lower frequencies grows and the compression becomes more efficient. Adequate block length values, balancing bandwidth requirements and delays, are discussed in Section 4.2.3.

The 1D SPIHT uses a temporal orientation tree structure to define the temporal parent-offspring relations in the wavelet domain, across consecutive layers. The set partitioning rule creates subsets of subband coefficient indices to create and update three related lists. The returned stream interleaves bits corresponding to wavelet coefficient values, called refinement bits, and instructions to update the lists and continue the decoding, called significant bits. The stream bits are ordered according to their significance, and it can be truncated at any point to enable compression with distortion under a threshold that preserves the signal diagnostic value.

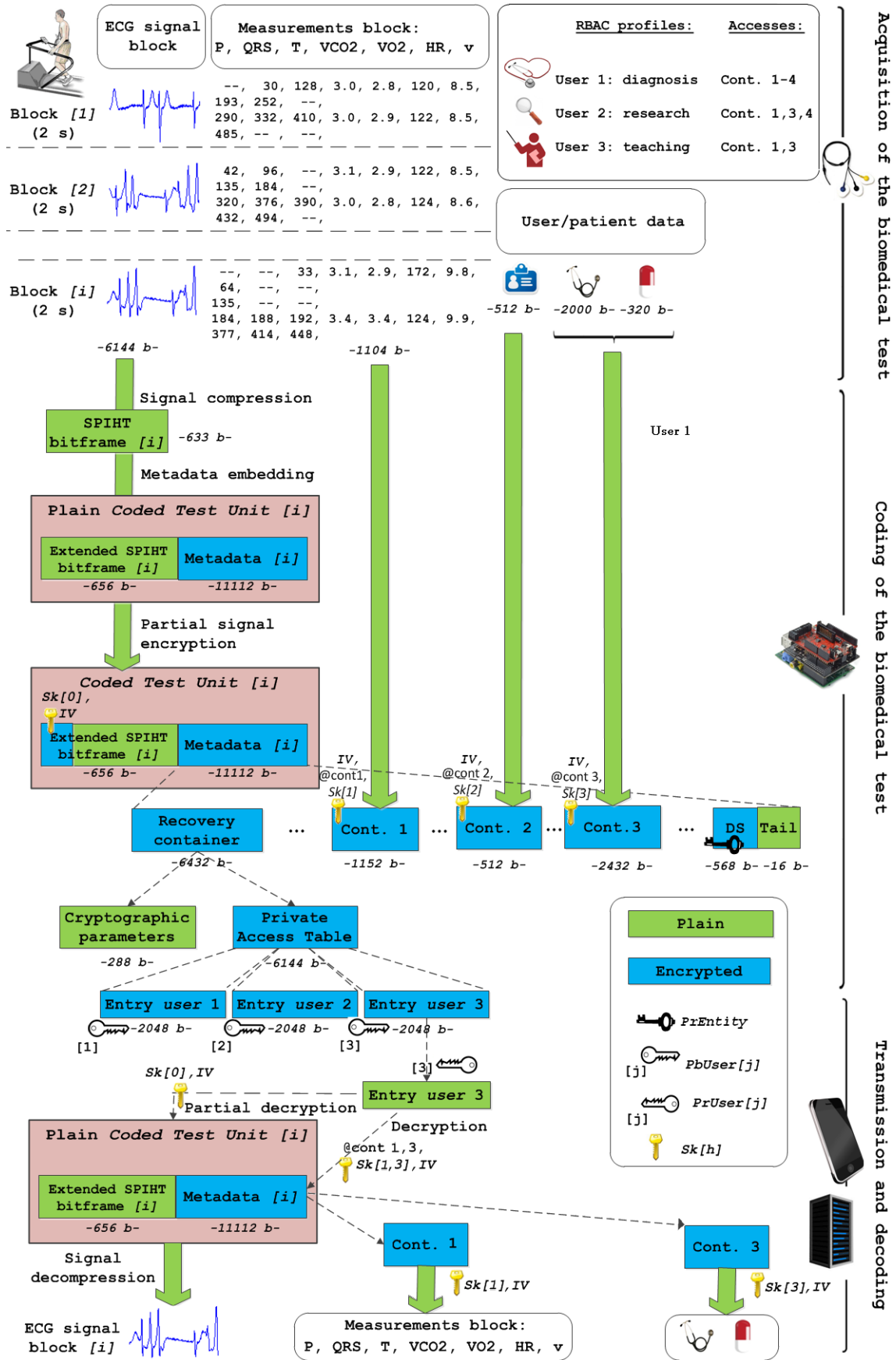


Figure 4.2: Proposed coding (and decoding) for 1D biomedical tests in m-Health architectures.

**Algorithm 1** Coding of biomedical tests as *CTUs*


---

```

1: procedure BIOCODING( $S, Th, \{contents\}, RC, \{Sk\}, \{lengthNoise\}, IV, PrEntity$ )
2:    $SPIHT_b, pointer \leftarrow compress(S, SPIHT, Th)$   $\triangleright$  SPIHT-based compression of  $S$ 
3:    $metadata \leftarrow preparationOfMetadata(\{contents\}, RC, \{Sk\}, \{lengthNoise\})$ 
4:    $CTU_p, tail \leftarrow embedding(S, SPIHT_b, pointer, Th, metadata)$   $\triangleright$  To embed  $metadata$  with coded  $S$ 
5:    $CTU \leftarrow symPartialSignalEncryption(CTU_p, Sk\{0\}, IV)$   $\triangleright$  Partial encryption of coded  $S$ 
6:    $CTU \leftarrow [CTU, DS([CTU, tail], readSignatureAlg(RC), PrEntity), tail]$   $\triangleright$  To close the  $CTU$ 
7:   return  $CTU, CTU_p(1 : 128)$   $\triangleright$  The first 128 bits of  $CTU_p$  are the  $IV$  to encode the next  $CTU$ 

8: procedure PREPARATIONOFMETADATA( $\{contents\}, RC, \{Sk\}, \{lengthNoise\}$ )
9:    $containers \leftarrow \{\}$ 
10:  for  $i$  in 1 to  $\#contents$  do  $\triangleright$  Each  $content$  will result in a  $container$ 
11:    if  $isConfidentialContainer(RC, i)$  then  $\triangleright$  If the  $container$  is confidential
12:       $containers\{i\} \leftarrow encrypt(contents\{i\}, readSymEncAlg(RC), IV, Sk\{i\})$   $\triangleright$  Sym. encr.
13:       $randomNoise\{i\} \leftarrow createRandomVector(lengthNoise\{i\})$   $\triangleright$  To hide its position
14:    else  $\triangleright$  If the  $container$  is public
15:       $containers\{i\} \leftarrow contents\{i\}$   $\triangleright$  Content in plaintext
16:       $randomNoise\{i\} \leftarrow createRandomVector(lengthNoise\{i\})$ 
17:     $metadata \leftarrow RC$ 
18:    for  $i$  in 1 to  $\#containers$  do  $\triangleright$  Introduction of random vectors between  $containers$ 
19:       $metadata \leftarrow [metadata, randomNoise\{i\}, containers\{i\}]$   $\triangleright$  to hide their locations
20:    return  $metadata$ 

21: procedure EMBEDDING( $S, SPIHT_b, pointer, Th, metadata$ )
22:    $CTU_p \leftarrow [SPIHT_b(1 : pointer), metadata]$   $\triangleright$  See Figure 4.2
23:    $w_S \leftarrow WT(S)$   $\triangleright$  Wavelet coefficients for perfect reconstruction of  $S$ 
24:    $w_{CTU_p}, LIS, LIP, LSP \leftarrow decodeWavelet(CTU_p(1 : pointer))$   $\triangleright$  Wavelet coefficients for a
25:    $pointer2 \leftarrow 0$   $\triangleright$  distortion of  $Th$  when reconstructing  $S$  with  $CTU_p(1 : pointer)$ 
26:   while  $distortionWavelet(w_S, w_{CTU_p}) > Th$  do  $\triangleright$  This loop extends  $CTU_p$  with bits from
27:      $pointer2 \leftarrow pointer2 + 1$   $\triangleright$   $SPIHT_b$  until the distortion of the  $S$  reconstructed from  $CTU_p$ 
28:      $CTU_p \leftarrow [SPIHT_b(1 : (pointer + pointer2)), metadata]$   $\triangleright$  is below  $Th$ 
29:      $w_{compensation} \leftarrow decodeWavelet(CTU_p, pointer, end, LIS, LIP, LSP)$ 
30:      $w_{CTU_p} \leftarrow w_{CTU_p} + w_{compensation}$ 
31:    $tail \leftarrow pointer + pointer2$   $\triangleright$  Point in  $CTU_p$  where the bits from the original  $SPIHT_b$  end
32:   return  $CTU_p, tail$ 

33: procedure SYMPARTIALSIGNALENCRIPTION( $CTU_p, sk, IV$ )  $\triangleright$  It only requires a double  $\oplus$ 
34:    $CTU \leftarrow CTU_p$ 
35:    $CTU(1 : length(sk)) \leftarrow CTU_p(1 : length(sk)) \oplus sk \oplus IV$ 
36:   return  $CTU$ 

```

---



**Algorithm 2** Decoding of *CTUs* to biomedical tests

---

```

1: procedure BIODECODING(CTU, PrUser)
2:   metadata  $\leftarrow$  readMetadata(CTU)            $\triangleright$  It reads the tail of CTU and extracts metadata
3:   RC  $\leftarrow$  readRC(metadata)  $\triangleright$  Extraction of RC, located at the beginning of metadata, see Tab. 4.2
4:   if checkDS(RC, readSignatureAlgorithm(RC), readPublicKeyEntity(RC)) then
5:     if checkDS(CTU, readSignatureAlgorithm(RC), readPublicKeyEntity(RC)) then
6:       {contents}, Sk{0}, IV  $\leftarrow$  readAuthorizedContents(RC, PrUser)            $\triangleright$  See Figure 4.2
7:       if IsConfidentialSignal(RC) then
8:         CTUp  $\leftarrow$  symPartialSignalEncryption(CTU, Sk{0}, IV)  $\triangleright$  To decrypt, Alg. 1: line 33
9:       else
10:        CTUp  $\leftarrow$  CTU
11:        S  $\leftarrow$  decompress(CTUp, SPIHT)            $\triangleright$  Reconstruction of S with a distortion of Th
12:      else
13:        Warning caused by invalid signature of CTU
14:      else
15:        Warning caused by invalid signature of RC
16:   return S, {contents}            $\triangleright$  The information contained in CTU of authorized access to the user

```

---

Bounding distortion using SPIHT is a simple task if we use the fact that the Euclidean norm, which is used to measure the error, is invariant to the wavelet transform (since it is a unitary transformation). Thus, guaranteeing reconstruction quality can be easily done by controlling the value of the coded coefficients and calculating some distortion measure to stop the coding process when the desired distortion level is reached [373, 374]. This is detailed in Section 4.2.2.

The tolerance to errors (inversion of bit value) of the SPIHT depends on the position of the wrong bits in the stream and on their types (refinement or significant). Wrong bits at the beginning of the stream will cause higher damage in the signal reconstruction since they carry more important information. Nonetheless, while wrong refinement bits cause a constant error in the signal, even one only wrong significant bit causes the desynchronization of the remaining decoding, producing a much more significant damage.

#### 4.1.2 Embedding metadata within the signal

The embedding and retrieval of metadata (e.g. additional measurements recorded during the test, contextual information, security items), formally defined in Algorithm 1: lines 4 and 21-32 and Algorithm 2: line 2, are steganographic procedures to achieve a certain degree of privacy. These are performed in the SPIHT domain given the remarkable advantages: high capacity, very low complexity and controllable signal distortion.

Before embedding the metadata, the signal is compressed (Section 4.1.1) guaranteeing

that the distortion is below a distortion threshold —  $Th$ . This compression implies that the bitframe is truncated, from a given point to the right, which corresponds to small details of the signal and noise — as the bitframe is ordered by significance. As illustrated in Figure 4.2 and Algorithm 1: line 22, to produce the plain *CTU*, the truncated bits are replaced with metadata, which results embedded within the signal. These bits are kept for signal reconstruction, providing a common access to the signal regardless whether the user knows the test coding method (thus, the presence of additional contents) or just the signal compression algorithm — see Algorithm 2: line 11. Nevertheless, those metadata bits added after the truncation point are interpreted by the SPIHT decoder as actual significant and refinement bits. Thus, they will produce wrong decoding from the truncation point, introducing small levels of random noise in the reconstructed signal block (Section 4.2.3). This leads to two possible results:

- $distortion > Th$ , the most common case, when the added random noise increased the distortion of the signal. To bypass this issue, extra SPIHT bits from the original, untruncated bitframe bits will be added between the truncation point and the metadata bits, until  $distortion \leq Th$  — see Algorithm 1: lines 26-30. Those extra bits introduce certain overhead — see Figure 4.2.
- $distortion \leq Th$ , when the added random noise was overall close to certain details in the original signal block. Since the distortion of the signal with the metadata is lower, it preserves its clinical value without the need of adding extra bits from the original SPIHT.

It is worth noting that during the embedding there is no need to reconstruct the signal in the time domain to update the distortion when extending the SPIHT. This is feasible in the transform domain since the wavelet is a unitary transformation — see Algorithm 1 lines 26 and 29-30, and practical because the wavelet coefficients are calculated only once — see Algorithm 1: 23-24.

### Metadata encoding, protection and access

Organizing and protecting appropriately the metadata to be embedded within plain *CTUs* (see Figure 4.2) are basic requirements to guarantee that the corruption of the signal or the metadata can be detected and that access to the latter is suitably controlled. Although Cryptographic Message Syntax [151] (implemented by DICOM) provides the means to digitally sign, digest, authenticate or encrypt any digital content, it presents disadvantages that the *CTUs* must avoid: the syntax to protect each piece of data is not separated from it, control the access of different users is costly and it produces too much overhead.

The proposed coding is depicted in Figure 4.2, by means of an example, and in Algorithm 1: lines 3 and 8-20. At the end of each *Coded Test Unit (CTU)* there is a tail, composed of two bytes, which points at the beginning of the *metadata* to allow its retrieval — see Algorithm 2: line 2. The *metadata* is composed of:

- a *Recovery Container (RC)*, mandatory in the first *CTU*, which includes the syntax necessary to make the signal and the content of each data *container* retrievable to targeted users (or to everybody);
- data *containers* (1-6, optional), which include periodic measurements and/or context-related metadata about the test (see Section 4.4); and
- a digital signature (DS, mandatory), which allows the detection of tampering/forgery in the *CTU*.

The *Recovery Container*, depicted in Table 4.2, details the symmetric (*tag 3*) and asymmetric elements (*tag 0-2*) combined in the protection scheme to obtain an optimal security-performance tradeoff. *Tags 4-5* indicate the position of *container 1* to enable public access (when permitted by the user/patient) and *tag 6* contains the Private Access Table, which regulates private access to the *containers*.

The **data containers**, as illustrated in Figure 4.2 and Algorithm 1: line 19, are placed one after another, with noisy bytes preceding each container to hide their locations within the *CTU* — thus, increasing the cost of an attack due to the secrecy of their locations. In addition to this, confidential *containers* are encrypted independently with symmetric cryptography (a secret key,  $Sk[h]$ , and a initialization vector,  $IV$ , are used), which operates very fast. The recommendations from the (IHE) SDO profile (Section 2.6.3) are followed for the choice of the cryptographic algorithms. The symmetric ciphers suggested are listed in Table 4.2: tag 3 — Twofish, Serpent, RC6, MARS or AES, operating in counter mode (CTR), which makes cryptanalysis more difficult and does not require extra bytes for padding. The preferred cipher is Twofish (128), expected to remain secure beyond 2030 (according to NIST, see Table 2.6) and the second fastest in generation of keys and encryption (see Table 2.8). Asymmetric cryptography, which is safer and does not need previous key arrangements to begin operation, is used to protect the symmetric encryption elements and also the location (position and length) of the confidential *containers* (Table 4.2: tag 6). This uses a key pair ( $PbUser[j]$ ,  $PrUser[j]$ ) for encryption and decryption. Regarding algorithms, only the widespread RSA ( $\geq 2048$ ) [360] is recommended, since its major competitor, elGamal, is not a standard and encrypts more slowly. The access procedure is as follows:

- For public **containers** (indicated in Table 4.2: tag 4), they are in plaintext and their locations are publicly available in Table 4.2: tag 5.

Table 4.2: Structure and content of a *Recovery Container*

Tag <sup>1</sup>	Length <sup>1</sup>	Value (parameter data)																								
<b>Certificate of the coding entity</b> (PEM encoding):																										
0	length <sup>2</sup>	This is the certificate for signature of the person, software or acquiring device that generates the <i>Coded Test Unit</i> . It must be X.509 type and three signature algorithms are allowed: <b>ECDSA</b> $\geq 224$ (recommended <b>256</b> ) [366], DSA $\geq 2048$ [367] and RSA $\geq 2048$ [360].																								
<table border="1"> <thead> <tr> <th></th> <th>Value</th> <th>Algorithm</th> </tr> </thead> <tbody> <tr> <td rowspan="3">1</td> <td rowspan="3">1 byte</td> <td><b>0</b>    <b>RIPEMD-256</b></td> </tr> <tr> <td>1      Whirlpool</td> </tr> <tr> <td>2      SHA-256</td> </tr> </tbody> </table>				Value	Algorithm	1	1 byte	<b>0</b> <b>RIPEMD-256</b>	1      Whirlpool	2      SHA-256																
	Value	Algorithm																								
1	1 byte	<b>0</b> <b>RIPEMD-256</b>																								
		1      Whirlpool																								
		2      SHA-256																								
<b>Digital signature</b> , $DS(RC, \underline{Tags} : 0, 1, PrEntity)$																										
2	length <sup>2</sup>	This is the encryption of the hash of the <i>RC</i> using the private key of the coding entity (initially DS = blank). At the user's side the DS is used to verify the integrity of the <i>RC</i> and authenticate the coding entity. The length depends on the signature algorithm: DSA or ECDSA.																								
<table border="1"> <thead> <tr> <th></th> <th>Value</th> <th>Algorithm</th> </tr> </thead> <tbody> <tr> <td rowspan="5">3</td> <td rowspan="5">1 byte</td> <td><b>0</b>    <b>Twofish</b></td> </tr> <tr> <td>1      Serpent</td> </tr> <tr> <td>2      RC6</td> </tr> <tr> <td>3      MARS</td> </tr> <tr> <td>4      AES</td> </tr> </tbody> </table>				Value	Algorithm	3	1 byte	<b>0</b> <b>Twofish</b>	1      Serpent	2      RC6	3      MARS	4      AES														
	Value	Algorithm																								
3	1 byte	<b>0</b> <b>Twofish</b>																								
		1      Serpent																								
		2      RC6																								
		3      MARS																								
		4      AES																								
<b>Binary mask of contents(s)</b> — 0-bits for confidential, 1-bits for public.																										
4	1 bytes	The leftmost bit corresponds to the signal, the next to the first container and so on. The rightmost bit indicates if the first container is present in the following <i>CTUs</i> (0) or not (1).																								
5	$(4 + 3) \cdot n$ bytes	<b>Position and length of the <math>n</math> public container(s)</b> , see Tag 4.																								
<table border="1"> <thead> <tr> <th></th> <th>Length<sup>1</sup> (bytes)</th> <th>Content</th> </tr> </thead> <tbody> <tr> <td rowspan="10"><b>Private Access Table (PAT)</b></td> <td>6</td> <td>Date of coding (seconds since January 1, 1970, 00:00:00 GMT)</td> </tr> <tr> <td>6</td> <td><i>PbU1</i> (first bytes)</td> </tr> <tr> <td>1</td> <td>RBAC profile (n) — see Section 4.4</td> </tr> <tr> <td>length</td> <td>encrypt(entr<sub>y</sub> for user 1, Alg, <i>PbU1</i>)</td> </tr> <tr> <td>...</td> <td>...</td> </tr> <tr> <td>...</td> <td>...</td> </tr> <tr> <td>...</td> <td>...</td> </tr> <tr> <td>...</td> <td>...</td> </tr> <tr> <td>...</td> <td>...</td> </tr> <tr> <td>...</td> <td>...</td> </tr> </tbody> </table>				Length <sup>1</sup> (bytes)	Content	<b>Private Access Table (PAT)</b>	6	Date of coding (seconds since January 1, 1970, 00:00:00 GMT)	6	<i>PbU1</i> (first bytes)	1	RBAC profile (n) — see Section 4.4	length	encrypt(entr <sub>y</sub> for user 1, Alg, <i>PbU1</i> )	...	...	...	...	...	...	...	...	...	...	...	...
	Length <sup>1</sup> (bytes)	Content																								
<b>Private Access Table (PAT)</b>	6	Date of coding (seconds since January 1, 1970, 00:00:00 GMT)																								
	6	<i>PbU1</i> (first bytes)																								
	1	RBAC profile (n) — see Section 4.4																								
	length	encrypt(entr <sub>y</sub> for user 1, Alg, <i>PbU1</i> )																								
	...	...																								
	...	...																								
	...	...																								
	...	...																								
	...	...																								
	...	...																								
6	length <sup>2</sup>	<table border="1"> <thead> <tr> <th></th> <th>Length<sup>1</sup> (bytes)</th> <th>Content</th> </tr> </thead> <tbody> <tr> <td rowspan="10">each entr<sub>y</sub> is</td> <td>16</td> <td><i>IV</i>, initialization vector</td> </tr> <tr> <td>16</td> <td><i>Sk</i>[0], secret symmetric key for the signal</td> </tr> <tr> <td>4</td> <td>Position of <i>container</i> 1 (bytes)</td> </tr> <tr> <td>3</td> <td>Length of <i>container</i> 1 (bytes)</td> </tr> <tr> <td>16</td> <td><i>Sk</i>[1], secret symmetric key for <i>cont.</i> 1</td> </tr> <tr> <td>...</td> <td>...</td> </tr> <tr> <td>4</td> <td>Position of <i>container</i> 6 (bytes)</td> </tr> <tr> <td>3</td> <td>Length of <i>container</i> 6 (bytes)</td> </tr> <tr> <td>16</td> <td><i>Sk</i>[6], secret symmetric key for <i>cont.</i> 6</td> </tr> </tbody> </table>		Length <sup>1</sup> (bytes)	Content	each entr <sub>y</sub> is	16	<i>IV</i> , initialization vector	16	<i>Sk</i> [0], secret symmetric key for the signal	4	Position of <i>container</i> 1 (bytes)	3	Length of <i>container</i> 1 (bytes)	16	<i>Sk</i> [1], secret symmetric key for <i>cont.</i> 1	...	...	4	Position of <i>container</i> 6 (bytes)	3	Length of <i>container</i> 6 (bytes)	16	<i>Sk</i> [6], secret symmetric key for <i>cont.</i> 6		
	Length <sup>1</sup> (bytes)	Content																								
each entr <sub>y</sub> is	16	<i>IV</i> , initialization vector																								
	16	<i>Sk</i> [0], secret symmetric key for the signal																								
	4	Position of <i>container</i> 1 (bytes)																								
	3	Length of <i>container</i> 1 (bytes)																								
	16	<i>Sk</i> [1], secret symmetric key for <i>cont.</i> 1																								
	...	...																								
	4	Position of <i>container</i> 6 (bytes)																								
	3	Length of <i>container</i> 6 (bytes)																								
	16	<i>Sk</i> [6], secret symmetric key for <i>cont.</i> 6																								

<sup>1</sup> The fields Tag and Length are represented with 1 and 2 bytes respectively.<sup>2</sup> The length of these fields is specified in Table 4.3.

- For confidential *containers* (indicated in Table 4.2: tag 4), their symmetric keys ( $Sk[h]$ ), initialization vector ( $IV$ , which is common for the signal and all the *containers* in a  $CTU$ ) and locations make private entries in the Private Access Table (PAT, Table 4.2: tag 6), encrypted with the public RSA key of the intended user(s). As shown in Algorithm 2: line 6, each user decodes his/her entry in the PAT using his/her private key.

It is worth noting that *container1* is intended for periodic content(s) that are associated to each signal block – and thus to all the  $CTU$ (s), not only in the first one. The presence of this *container*, either continuous or limited to the first  $CTU$ , is indicated in Table 4.2: tag 4.

The **Digital Signatures (DS)** included in each  $CTU$  (Figure 4.2) and in the  $RC$  (Table 4.2: tag 2) are used to check their integrity and authenticity, see Algorithm 2: lines 4-5. Again, the recommendations from the (IHE) SDO profile (Section 2.6.3) are followed for the choice of the cryptographic algorithms involved. The DS are calculated by combining a safe hash function (Table 4.2: tag 1 - RIPEMD 256, Whirlpool or SHA 256) which makes a digest of the  $RC/CTU$ , with a public-key algorithm, which encrypts the digest with the private key of the entity who encodes the test — a person, a program or the test acquisition device itself. At the user's side, each DS is verified by calculating the hash of the received  $RC/CTU$  and comparing it with the original hash, decrypted with the public key of the coding entity (extracted from his/her digital certificate, Table 4.2: tag 0). If they match the  $RC/CTU$  is valid, otherwise all  $CTUs$ /that  $CTU$  are refused. Regarding algorithms, RSA [360] is allowed but discouraged, since the signatures are lengthy, DSA [367] is permitted since its signature is very compact (see Section 4.2.3), and ECDSA [366] is the preferred option since for a similar security level the signature length is the same as DSA and its key, and consequently its digital certificate, is much shorter (see Table 4.3).

### 4.1.3 Partial signal encryption

The partial encryption of the signal is applied to plain  $CTUs$ , obtaining the corresponding  $CTUs$ . This process is performed in the compressed domain, which saves a number of operations with respect to encrypting the original signal block. The reasons why partial encryption can be easily implemented are two: the SPIHT bitframe is ordered by relevance and the first changed significant bit produces the desynchronization of the decoding from that position. Therefore, it is enough to encrypt the first 128 bits of the bitframe, which include many significant bits, to produce a very high distortion that makes it uninterpretable. The signal block can only be reconstructed if the first 128 bits are retrieved,

either decrypting with the corresponding key or by brute-force searching, with a success probability of 1 in  $2^{128} \sim 10^{39}$  in the latter case.

Table 4.3: Typical size (KB) of the containers in a *Secure Frame*

<i>Recovery container (RC)</i> , defined in Table 4.2			Rest of <i>containers</i>			
<b>Entity's cert</b>	<i>RC</i> -Tag 0	<i>RC</i> -Tag 2	<i>CTU</i> DS	<b>Database</b>	<b>Block length</b>	<i>Cont. 1</i>
ECDSA 224	0.6	0.06	0.06	Arrhythmia (ECG)	512	0.053
ECDSA 256	0.6	0.06	0.06	Compression (ECG)	512	0.076
DSA 2048	1.6	0.05	0.05	SCCN (EEG)	512	0.012
DSA 4096	2.6	0.05	0.05	Arrhythmia (ECG)	4096	0.421
RSA 2048	1.1	0.26	0.26	Compression (ECG)	4096	0.606
RSA 4096	1.8	0.51	0.51	SCCN (EEG)	4096	0.098
<i>RC</i> -Tags 1, 3-5	<b>User's cert</b>	<i>RC</i> -Tag 6	<i>Containers 2-6</i>			
0.007	RSA 1024 (legacy)	$0.13 \cdot \#users$	3-10			
	RSA 2048	$0.26 \cdot \#users$				
	RSA 4096	$0.51 \cdot \#users$				

## 4.2 Experimental evaluation of the coding for biomedical tests

The methods selected for signal compression (Section 4.1.1) and metadata embedding (Section 4.1.2) depend on several parameters (e.g. signal distortion threshold, signal block length, wavelet decomposition level, DS type) which are studied and set up to guarantee a) user satisfaction: signal fidelity, low runtime costs (to allow real-time operation), ease of use of the implementation (see Section 4.3) and b) optimal system features: low bandwidth requirements, low overhead of the security elements and enough embedding capacity to include data produced in m-Health services.

A variety of electrocardiograms (ECGs), commonly used for the detection and diagnosis of heart disease, and electroencephalograms (EEGs), relevant in applications such as brain-computer interfaces and the study of epilepsy and sleep disorders (insomnia, circadian rhythm disorders, parasomnia, etc) are used to carry out all the parts of this evaluation.

### 4.2.1 Evaluation setup

Two well-known ECG databases have been used. The first one is the Massachusetts Institute of Technology (MIT)-Beth Israel Hospital (BIH) Arrhythmia [375]. This ECG database consists of 48 two-lead ECG registers of 30 min duration. The sampling rate is 360 samples per second with a resolution of 11 bits per sample. Although the database was originally created as standard test material for the evaluation of arrhythmia detectors, this database is by far the most used to test and compare ECG compression algorithms. The second ECG database is MIT-BIH Compression [201]. It is composed of 168 two-lead ECG records of 20.48 s duration. The sampling rate is 250 samples(s) with a resolution of 12 bits per sample. This database was created to pose a variety of challenges for ECG compressors, in particular for lossy compression methods. Despite this fact, it is scarcely used to test the ECG compression algorithms, being relegated by MIT-BIH Arrhythmia. Since these ECG databases are composed of two-lead recordings, the entire evaluation was run on both leads and the results represent the average.

For testing with EEGs, it was chosen the STUDY dataset [376, 377] from the Swartz Center for Computational Neuroscience (SCCN), composed of 10 recordings from 5 different subjects, with 61 channels per frame, 820 frames per epoch and 220 to 235 epochs. The sampling rate of these recordings is 200 samples per second and the resolution is 11 bits per sample.

### 4.2.2 Bounding signal distortion in compression

Fidelity of a compressed signal is understood as the close similarity with respect to the original. In clinical applications, it is essential to measure the distance between both signals by means of some distortion measure and setting a quality threshold to regulate the compression process. Among the most widespread measures of signal distortion are:

- the *Root Mean Square error (RMS)*, defined as

$$RMS = \sqrt{\frac{(x(n) - \tilde{x}(n))^2}{N}}, \quad (4.1)$$

- and the *Percentage RMS Distortion (PRD)*, defined as

$$PRD = \sqrt{\frac{\sum_{n=1}^N (x(n) - \tilde{x}(n))^2}{\sum_{n=1}^N (x(n) - \bar{x})^2}} \cdot 100, \quad (4.2)$$

where  $x(n)$  is the original signal,  $\tilde{x}(n)$  is the reconstructed,  $\bar{x}$  the mean of the original signal and  $N$  its length.

It can be observed in Equation 4.1 how the amplitude range of the signal affects the measure: compressed signals constrained to lower amplitudes obtain lower  $RMS$  than those with higher amplitude and the same fidelity. The definition of  $PRD$  in Equation 4.2 overcomes this issue because it uses a normalization which is independent from the amplitude of the signal (and from its DC level). Thus, the choice as the measure of signal distortion is the  $PRD$ , since it allows much fairer comparisons.

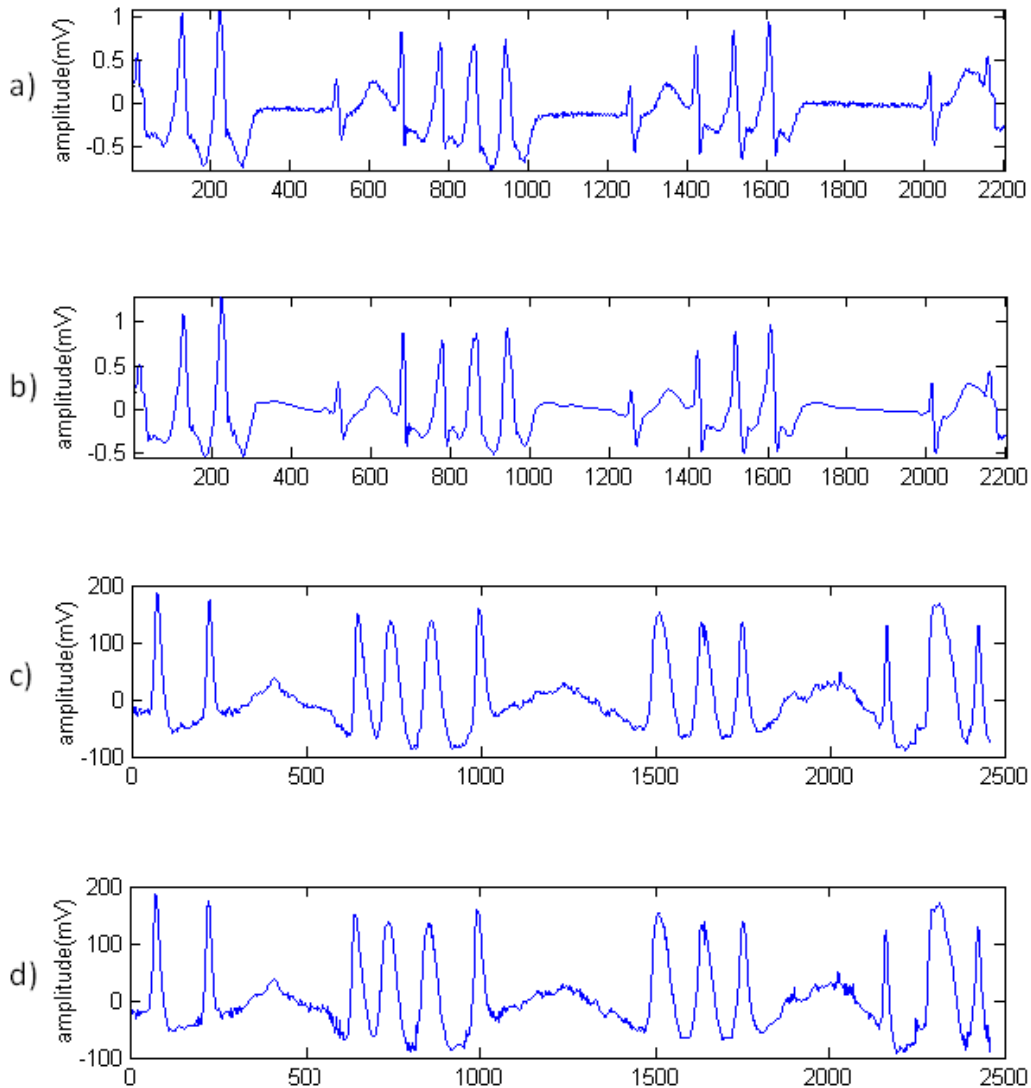


Figure 4.3: Signals a) 08730\_2 (lead 1) ECG from MIT-BIH Compression ( $bitrate 3000bps$ ), b) compressed with  $PRD = 9\%$  ( $bitrate 202bps$ ), c) Syn08-s254 EEG from SSCN ( $bitrate 2200bps$ ), d) compressed with  $PRD = 7\%$  ( $bitrate 240bps$ ). Additional parameters: block length = 512 samples, wavelet decomposition level = 6, SPIHT coding.



Furthermore, the correlation between the *PRD* and the mean opinion score (MOS) of expert cardiologists, obtained through blind and semi blind tests, was studied by Zigel in [378]. One of the conclusions of that work was that all tested signals with  $PRD < 9\%$  were considered as "good" or "very good" by the cardiologists. Thus, this value is used as quality threshold for ECG compression in this coding. Similarly, other works relate *PRD* to EEG quality. In [379] it is suggested limiting *PRD* to 7% to maintain 99.5% of the signal energy, while in [380] it is proposed rising to 30% since this value allows a seizure detection rate of 90% to be reached in epilepsy monitoring (using REACT, a state-of-the-art algorithm). Among these two values, 7% is preferred since EEG records may be used in applications requiring higher quality than seizure detection. Figure 4.3 shows two signals from these databases, an ECG and an EEG, which are compressed with the proposed thresholds and retain their main shapes accurately.

### 4.2.3 Runtime costs and bandwidth requirements

The runtime costs of the processes involved in the coding and decoding of biomedical tests are estimated in Table 4.5. The overall cost is mainly contributed by the latency of acquiring a signal block, expressible as:

$$block\ length(s) = \frac{block\ length\ (\#samples)}{sampling\ freq.\ (\#samples(s))}. \quad (4.3)$$

In fact, in all the configurations presented this delay is much greater than the sum of delays of the remaining processes (see Table 4.5: subtotal). This enables real-time operation on the condition of signal blocks as short as possible to maintain the delay at acceptable levels.

The bandwidth required for the transmission of coded ECG and EEG-based tests, embedding security elements (mandatory) and additional metadata (optional) is evaluated in Table 4.4. Four observations were made. First, using long signal blocks produces a decrease in signal bandwidth requirements which stops at 4096 samples/block for ECGs, in the case of EEGs higher values can improve the compression at the cost of very high delays ( $> 20.48$  s according to Equation 4.3). Long signal blocks allow more signal cycles to be included in a single block, lower frequencies obtain higher relevance and this benefits the sorting of the temporal orientation trees used by the 1D SPIHT, which increases the efficiency of the compression. Second, the signal bandwidth requirements increase slightly ( $\leq 4\%$ ) when embedding a big amount of metadata (three last columns in Table 4.4). Nevertheless this only happens in the first *CTU*, since the rest do not include *containers 2-6*. Third, using long signal blocks dramatically reduces the metadata bandwidth requirements since, in each *CTU*, the size of the security elements with respect to the

size of the coded signal block is lower. Fourth, the *CTU* compresses the original signal bandwidth (compression rate  $> 1$ ) despite of the embedding of security elements and other metadata. The only exception appears in the first *CTU* when using short signal blocks (512 samples/block) and embedding more than 3 KB in *containers 2-6*.

The size of the contents arranged in *Secure Frames* and subsequently embedded within *CTUs* for the bandwidth evaluation above are depicted in Table 4.3. The chosen certificate type for DS of the coding entity was ECDSA 256 and it was considered the case of 3 users, 2 with RSA 2048 certificates and 1 with a RSA 1024 (legacy) certificate, when embedding *containers 2-6*. For ECGs, the *container 1* included the signal delineation and additional measurements obtained from a stress test (VO<sub>2</sub>, heart rate, concentration of lactate in the blood, VCO<sub>2</sub> and speed of the treadmill). For EEGs, the *container 1* included a likelihood index for EEG seizure detection and additional monitoring measurements (NiBP, Temp, SPO<sub>2</sub>, CO<sub>2</sub> and heart rate). The ECG delineation consisted of the position of 15 fiducial points (wave onsets, peaks and offsets) per cardiac cycle, each point coded with 2 bytes. EEG seizure detection likelihood was estimated every second and coded using 1 byte. Each additional measurement was recorded at 1 sample/second and coded using 1 byte. For *containers 2-6* it was estimated that its overall size is around 3-10 KB. Although they store a variety of medical data, most of it can be described by means of IDs.

#### *Parameter tuning*

As regards to the adjustment of parameters, the length of the signal block establishes a tradeoff between the system overall delay and the bandwidth required for the transmission —this has been demonstrated above. Thus, two different values are recommended according to the application.

- 512 samples/block for **real-time transmission**, which yields acceptable delays (see Table 4.5: total) and low signal transmission rates (see Table 4.4): MIT-Arrhythmia (2 s, 409 bps/lead), MIT-Compression (2.7 s, 309 bps/lead), SCCN-EEG (3.3 s, 474 bps/channel).
- 4096 samples/block for **offline transmission**, which produces longer delays but more efficient signal transmission: MIT-Arrhythmia (12 s, 373 bps/lead), MIT-Compression (17 s, 282 bps/lead), SCCN-EEG (22.3 s, 389 bps/channel). Furthermore, the metadata transmission rate is reduced to one eighth with this configuration.

The signal compression, described in Section 4.1.1, begins with the wavelet transformation of the signal block. The Coiflet filter with 12 coefficients was chosen for this transformation, since it obtains higher compression efficiency than others (e.g. Daubechies

with 20 coefficients) and offers a good tradeoff between the number of operations and the quality of the reconstructed signal. The wavelet decomposition level was set to 6 because it was observed that the compression efficiency improves notably until this level but not in the following.

The protection scheme, described in Section 4.1.2, introduces overhead due to the need of including a digital signature (DS) in each *CTU* (see Figure 4.2). Several signature algorithms provide similar security with different DS length: ECDSA [366] ( $\geq 224$ , recommended 256) and DSA [367] ( $\geq 2048$ ) generate signatures sized in the range [0.05, 0.06] KB, while RSA [360] ( $\geq 2048$ ) signatures result much longer ( $\geq 0.26$ ) KB. To achieve good security with low overhead, ECDSA 256 is recommended.

Table 4.4: Bitrate required for the transmission of *Coded Test Units* including *metadata* with different elements

Parameters			Average <i>compressed signal</i> bitrate —bps/lead— + <i>metadata</i> bitrate —bps/lead— (overall compression ratio)					
Database	Block length	PRD	No <i>SF</i>	DS only	<i>Cont. 1</i> & DS	<i>RC, cont. 1,</i> <i>cont. 2-6</i> (3 KB) & DS	<i>RC, cont. 1,</i> <i>cont. 2-6</i> (6 KB) & DS	<i>RC, cont. 1,</i> <i>cont. 2-6</i> (10 KB) & DS
Arrhythmia —ECG—	512	9 %	409.4	409.7	410.6	422.0	422.5	422.2
			(9.67)	+ 368.9 (5.09)	+ 648.6 (3.74)	+ 2809 (1.23)	+ 4969 (0.73)	+ 7849 (0.48)
Compression —ECG—	512	9 %	309.2	307.7	308.2	317.1	316.8	317.0
			(9.70)	+ 256.0 (5.32)	+ 536.0 (3.55)	+ 2036 (1.27)	+ 3536 (0.78)	+ 5536 (0.51)
SCCN —EEG—	512	7 %	474.2	459.3	459.2	473.1	472.7	472.8
			(4.64)	+ 204.8 (3.31)	+ 252.8 (3.09)	+ 1453 (1.14)	+ 2653 (0.70)	+ 4253 (0.47)
Arrhythmia —ECG—	4096	9 %	372.5	372.7	372.8	387.7	387.6	387.5
			(10.63)	+ 46.1 (9.46)	+ 326.1 (5.67)	+ 596.1 (4.03)	+ 866.1 (3.16)	+ 1226 (2.45)
Compression —ECG—	4096	9 %	282.0	282.1	282.3	290.5	290.5	290.5
			(10.64)	+ 32.0 (9.55)	+ 312.0 (5.05)	+ 499.5 (3.80)	+ 687.0 (3.07)	+ 937.0 (2.44)
SCCN —EEG—	4096	7 %	388.6	386.6	386.3	395.2	394.8	394.9
			(5.66)	+ 25.6 (5.34)	+ 73.6 (4.78)	+ 223.6 (3.56)	+ 373.6 (2.86)	+ 573.6 (2.27)

Table 4.5: Runtime costs involved in the coding and decoding of *Coded Test Units*

Parameters			Delay <sup>1</sup> (ms)										
Database	Block length	PRD	<i>Block length(s)</i> , see Eq. 4.3	<i>Del./seiz. detection</i>	<i>Compres.</i>	<i>Cont.-level encryption</i>	<i>DS</i>	<i>Tr.</i>	<i>DS check</i>	<i>Decompres.</i>	<i>RBAC access</i>	Subtotal	Total
Arrhythmia (ECG)	512	9 %	<u>1422</u>	13	0.2	360	30	0.2	30	0.1	180	<u>613.2</u>	<u>2035.2</u>
Compression (ECG)	512	9 %	<u>2048</u>	13	0.3	360	30	0.2	30	0.1	180	<u>613.2</u>	<u>2661.2</u>
SCCN (EEG)	512	7 %	<u>2560</u>	156	0.3	360	30	0.4	30	0.1	180	<u>756.4</u>	<u>3316.4</u>
Arrhythmia (ECG)	4096	9 %	<u>11380</u>	37	2.4	360	30	1.3	30	1.2	180	<u>638.3</u>	<u>12018.3</u>
Compression (ECG)	4096	9 %	<u>16380</u>	37	3.2	360	30	1.8	30	1.5	180	<u>638.8</u>	<u>17018.8</u>
SCCN (EEG)	4096	7 %	<u>20480</u>	1248	3.0	360	30	3.1	30	1.4	180	<u>1851.1</u>	<u>22331.1</u>

Abbreviations:

*Del./seiz. detection* is ECG delineation/ EEG seizure detection,

*Compres.* is SPIHT compression,

*Cont.-level encryption* is *container*-level encryption,

*DS* is calculating the digital signature of the *Coded Test Unit* ,

*Tr.* is transmitting the *Coded Test Unit* using HSUPA at 5.76 Mbps,

*DS check* is checking the digital signature,

*Decompres.* is SPIHT decompression,

*RBAC access* is decrypting the *containers* allowed to the intended user.

#### 4.2.4 Embedding Capacity

The *Embedding Capacity* ( $EC$ ) is defined as the amount of metadata that can be embedded with the proposed coding method when using the same bandwidth as for transmitting the signal uncompressed. The  $EC_i$  (per lead/channel) of different ECG and EEG signals are shown in Table 4.6. In most cases the overall  $EC$  (e.g.  $\geq 77.7$  MB in ambulatory recordings — 25.9 MB·3 leads — or  $\geq 2.15$  MB in stress tests — 178.9 KB ·12 leads —) far exceeds the size that *containers* 1-6 require to enable m-Health services, estimated in Table 4.3. The difference is what is saved in transmission and storage, typically  $\simeq 70-80\%$  of the original size.

Table 4.6: Average *Embedding Capacity* ( $EC_i$ ) of *Coded Test Units* corresponding to various ECG and EEG-based tests

Test and duration	Signal database	Samples/block	$EC_i$
resting	Arrhythmia	512	66.5% (3.2 KB)
ECG,	Arrhythmia	4096	75.6% (3.7 KB)
10 s	Compression	512	63.0% (2.3 KB)
	Compression	4096	71.3% (2.6 KB)
resting	Arrhythmia	512	75.7% (11.0 KB)
ECG,	Arrhythmia	4096	84.8% (12.3 KB)
30 s	Compression	512	75.1% (8.3 KB)
	Compression	4096	83.5% (9.2 KB)
stress	Arrhythmia	512	80.1% (232.4 KB)
ECG	Arrhythmia	4096	89.2% (258.7 KB)
10 min	Compression	512	80.9% (177.8 KB)
	Compression	4096	89.2% (196.1 KB)
ambulatory	Arrhythmia	512	80.3% (33.6 MB)
ECG,	Arrhythmia	4096	89.4% (37.4 MB)
24 h	Compression	512	81.2% (25.7 MB)
	Compression	4096	89.5% (28.3 MB)
epilepsy detection	SCCN-EEG	512	69.7% (336.8 KB)
(EEG), 30 min	SCCN-EEG	4096	81.1% (392.2 KB)
polysomnographic	SCCN-EEG	512	69.8% (4.4 MB)
study (EEG), 6.5 h	SCCN-EEG	4096	81.3% (5.1 MB)

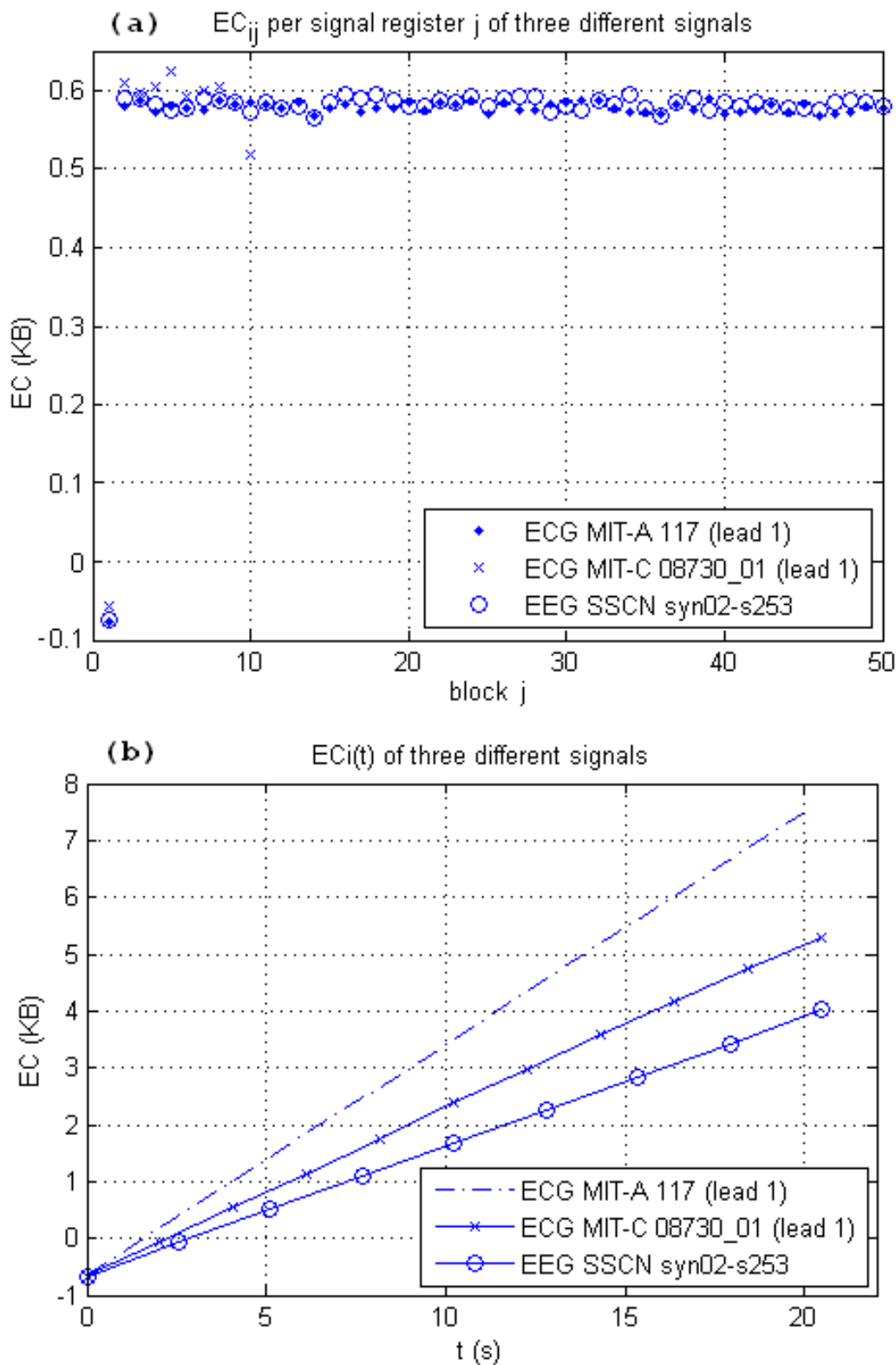


Figure 4.4: *Embedding Capacity* ( $EC$ ) per ECG register (a) and per lead (b) of two coded ECGs from MIT-Arrhythmia and MIT-Compression and a coded EEG from SSCN-EEG. ECGs compressed with  $PRD = 9\%$ , EEG with  $PRD = 7\%$ , block length = 512 samples, wavelet decomposition level = 6.

Each *CTU*  $j$  from a lead/channel  $i$  has its own embedding capacity,  $EC_{ij}$  (depicted in Figure 4.4-a), resulting from the difference between the sizes of the original signal block and the corresponding *CTU* (SPIHT bitframe, *SF* and tail). The  $EC_i(t)$  of a lead/channel  $i$ , illustrated in Figure 4.4-b, is the sum of the  $EC_{ij}$  of the blocks 1 to  $j$  transmitted/stored until  $t$ . The size of the *RC*, embedded in the first *CTU*, corresponds to the negative offset in Figure 4.4-b. The embedding capacity of a lead/channel can be approximated as:

$$EC_i(t) = (\text{sampling freq} \cdot \text{bit res.} - \text{compressed signal bitrate} - \frac{\text{size}(DS)}{\text{block length}}) \cdot t - \text{size}(RC). \quad (4.4)$$

To build Table 4.6, this approximation was used. The sampling frequencies of the signals and their resolutions were consulted in Section 4.2.1, the compressed signal bitrates in Table 4.4, the size of the DS (considering ECDSA 239) in Table 4.3 and the block length was calculated with Equation 4.3.

### 4.3 Proof of concept

The coding-decoding software implementing the processes defined in Algorithms 1-2 and illustrated in Figure 4.2 is openly available at <http://sourceforge.net/projects/pfmt/>. It is divided into two modules: a standard 1D SPIHT compressor-decompressor (Section 4.1.1), whose optimal parameters of (real-time/offline) operation were studied in Section 4.2.3; and a GUI to encode and decode plain *CTUs* (Section 4.1.2) and to perform partial encryption-decryption of *CTUs* (Section 4.1.3). As illustrated in Figure 4.5, the design of the GUI is rather simple and intuitive, to encourage users with little technical knowledge. It facilitates the coding of additional measurements and contextual information in the corresponding *containers*, the assignment of role-based access profiles to intended users (physicians, researchers, teachers, etc.) and the protection of the resulting *CTUs*. All the corresponding operations of encryption, decryption, signature and checking are carried out by the GUI. However, some interaction is required:

- With the entity that encodes the *CTUs*, he/she shall:
  1. load the signal SPIHT bitframes;
  2. load the content of the data *container*(s);
  3. load the certificates of the users and indicate their RBAC profiles (Section 4.4);
  4. load his/her digital certificate, if desired change the default hash function and the encryption algorithm;
  5. load his/her password-protected private key;
  6. save the resulting *CTUs*.

- With the user that accesses the *CTUs*, he/she shall:
  1. load the *CTUs*;
  2. export the private access table to check his/her RBAC profile (if desired);
  3. load his/her password-protected private key (only if he/she is allowed to access some content(s));
  4. save the plain *CTU(s)* and the *container(s)* that he/she is allowed to access.

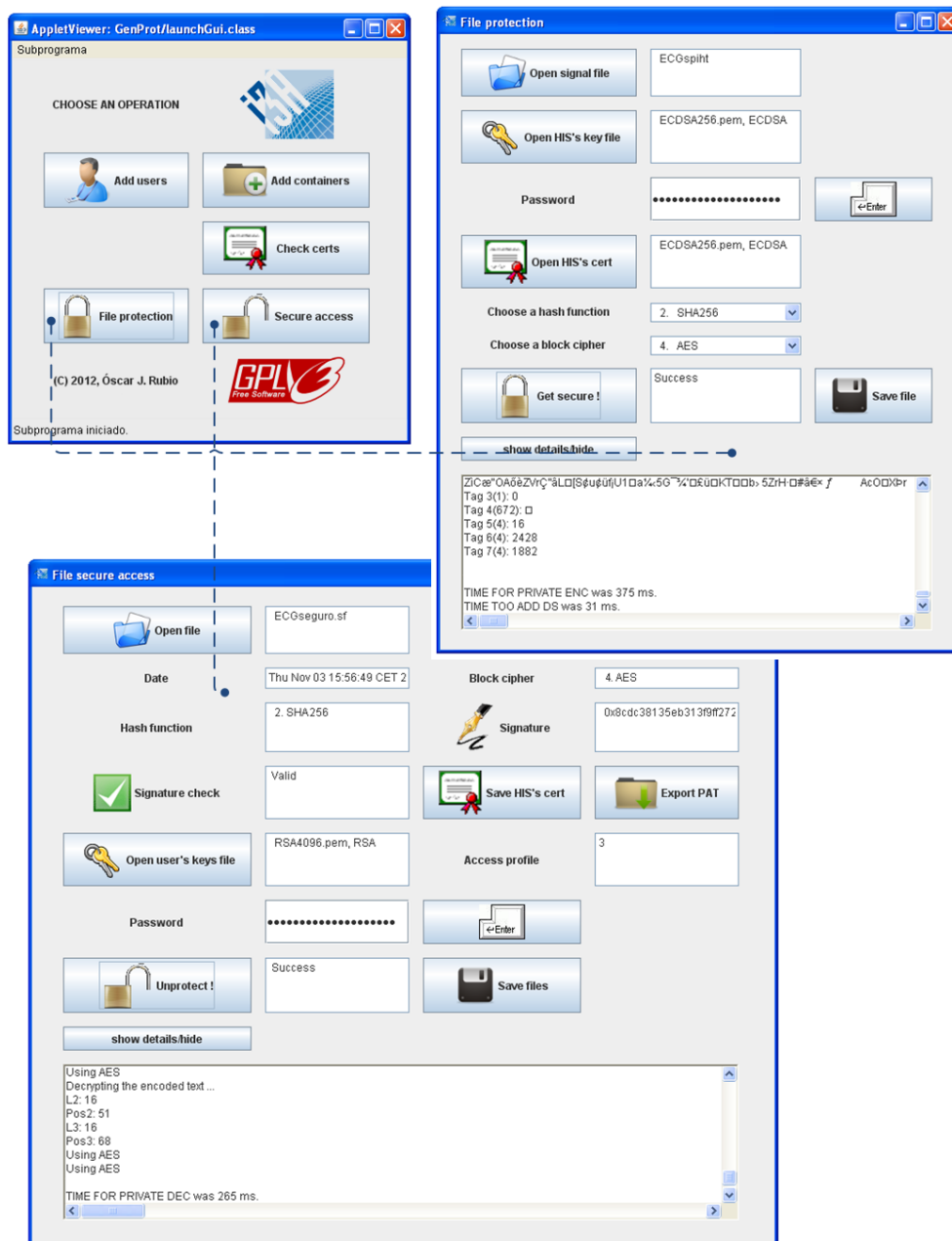


Figure 4.5: GUI to code and decode *Coded Test Units*, depicted in Figure 4.2.



These interactions with coding entities and users could be minimized by defining system configuration profiles. Due to the cryptographic operations involved, it is necessary that each coding entity and each user possess his/her own digital certificate (and the coupled password-protected private key). However, this requirement did not decrease the experience of the consulted physicians, who pointed out that the GUI was easy to handle. The certificates associated with electronic IDs are valid for this purpose.

## 4.4 Secure m-Health applications based on the novel coding

Since biomedical tests may be requested for different uses (e.g. diagnosis, research, teaching), the implementation of a RBAC policy defining different access profiles is a smart way to fulfill the privacy principles of necessity of data processing and purpose binding. In fact, these policies have gained attention in recent years and currently they are integrated in several medical standards (e.g. DICOM [144] and HL7 [146]). In addition to this, the security of this coding (Section 4.4.1) and its potential limitations (Section 4.4.2) shall also be analyzed.

The cryptosteganographic coding proposed enables the implementation of various m-Health applications by following three stages:

1. Establishing clearly the contents that each container shall store.
2. Defining m-Health application profiles and the content(s) that they allow to access.
3. Assigning m-Health, RBAC application profile(s) to each consulting user, according to his/her professional role(s).

The coding entity — person, program or acquisition device — will assign a RBAC profile to each intended user, according to his/her professional role, to establish the contents of the test that he/she is allowed to access. As shown in Figure 4.2, the proposed RBAC policy is defined on top of the formerly described *container*-level encryption, which already allowed several users to access various contents (placed into separated *containers*) of a *CTU*.

To illustrate with an example, a possible definition for the *containers*, integrating the most interesting contents included by major medical standards (DICOM [79], HL7 [77], SCP-ECG [76] and MFER [78]), may be:

- *Container 1*. This may include information concerning the acquisition session:
  - context-aware data (e.g. type of test: resting ECG, stress ECG, ambulatory ECG monitoring, intensive care monitoring);

- environmental parameters (e.g. positioning, humidity, temperature);
  - parameters of the signal (e.g. sampling frequency, quantization bits, amplitude multiplier, applied filters);
  - additional data extracted after signal processing (e.g. delineation of fiducial points in an ECG record, intervals of likely seizure in EEGs);
  - periodic measures acquired in intensive care monitoring (e.g. non-invasive blood pressure —NiBP—, temperature —Temp—, blood oxygen saturation —SPO2—, carbon dioxide —CO2—, heart rate);
  - periodic measures acquired in stress tests (e.g. maximal oxygen consumption —VO2—, heart rate, concentration of lactate in the blood, carbon dioxide production —VCO2—, speed of the treadmill/power of the bicycle).
- *Container 2.* This may include the identification of the patient (e.g. name, surname, Social Security Number, Personal Health Record identifier), the physician/technician who acquires the signal, the acquiring and analyzing devices and the institution (and/or department) that leads the test.
  - *Container 3.* This may include general data (e.g. age, height, weight) and health status of the patient (e.g. diseases, symptoms, previous diagnoses, observations).
  - *Container 4.* This may include the allergies and current medication of the patient.
  - *Container 5.* This may include sensitive diseases of the patient (e.g. AIDS, venereal diseases), not included in *container 3* for confidentiality reasons.
  - *Container 6.* This may include billing information of the medical test.

As regards to the RBAC profiles, the list below was compiled after consulting medical experts. It aims at covering the foremost applications of biomedical tests within the m-Health context:

0. Emergency care/surgery: access to signals, all personal and medical data of the patient, *containers 1-5*.
1. Diagnosis (by the physician who interprets the test): access to signals, all personal and medical data, excluding sensitive diseases not directly related with the current test, *containers 1-4*.
2. Research or examination (by another physician caring for the patient): access to signals and medical data of the patient preserving his/her anonymity, *containers 1, 3, 4*.

3. Teaching: access to signals and general health status of the patient to enable correlations, *containers 1, 3*.
4. Billing: access to signals and information about the costs of the acquisition session, *containers 1, 6*.
5. Signals consultation: access to signals and *container 1* only.

Nonetheless, it is worth highlighting that the proposed coding can work with different number and alternative definitions of *containers* and RBAC profiles, since it is not specifically intended for these examples only.

#### 4.4.1 Risk assessment

The coding method proposed, which is described in Section 4.1, involves different elements; including the corresponding Algorithms (1-2), the original biomedical test — signal(s), periodic measurements and/or contextual information — and the resulting *CTU*(s). Several considerations can be done about the character, either public or private, of these elements. As regards to the algorithm, Kerckhoff's principle states that the system shall be secure even if everything about it, except certain keys, is public knowledge. Therefore, it is proposed in Section 4.1 to make it public from the beginning. At first this may seem nonsense since the coding is steganographic, but what is hidden are the contents embedded within the signal, not the algorithm. With respect to the biomedical tests, it is assumed that the acquiring device(s) will thoroughly remove them after their encoding, since they are protected only in their coded form — as *CTU*(s). Thus, the possibility that an attacker accesses the device and finds copies of biomedical tests — e.g. in the RAM memory of the device — is excluded. Regarding the *CTUs*, they cannot be considered as hard to obtain always since their transmission in the BAN/PAN may be wireless and poorly protected and because some patients may cooperate in granting access (with their informed consent) to their biomedical tests (or part of them) for certain m-Health applications — e.g. teaching, research — under strict RBAC, which increases the number of accesses to the *CTU*(s) (and the number of potential opportunities for attackers accordingly).

An attacker with access to some of the aforementioned elements may try to perform certain attack(s) to interfere with the security of the m-Health applications described in Section 4.4. Thus, these applications cannot be considered as secure until performing a risk assessment in-depth, which includes all feasible attacks and the existing countermeasures. The following risk assessment analyzes attacks depending on the actions intended by the attacker and the system elements he/she needs access to.

- Unauthorized detection and reading of private biomedical contents from *CTU*(s). If

the first *CTU* transmitted is captured, the *RC* can be easily detected at the beginning of the embedded metadata. The *RC* contains the syntax to read the contents embedded with the signal, and given its relevance, it is protected with asymmetric encryption. Breaking this encryption or obtaining one or several private key(s) from authorized users is considered highly unlikely. Nevertheless, still some attacks can be attempted without knowing the content of the *RC*. Regarding the signal, it is known that the whole, plain *CTU* is used for its reconstruction through the SPIHT decoder. Therefore, if the plain *CTU* is transmitted, anyone can reconstruct the signal — because the corresponding user/patient permits the access to it. Otherwise, trying to break a regular, signal-encrypting *CTU* implies searching in a space of  $\simeq 10^{39}$  combinations and attempting to reconstruct the signal with each individual combination — with a very low success probability. As regards to the embedded contents, those stored in public *containers* can be read by anyone, since their location is known and they are unencrypted. On the contrary, confidential *containers* are independently encrypted with symmetric cryptography and their locations are secret, which increases the search space — and reduces the success probability of a brute-force attack.

- Generation of forged *CTU*(s). Anyone can create his/her own *CTU*(s), since the algorithm is public. However, attempting to forge the origin of the biomedical test requires generating a legitimate digital signature from a trusted coding device. To do so, the attacker would need to break or steal the private key of a trusted device — which is highly unlikely if appropriately protected.
- Malicious removal of legitimate contents from *CTU*(s). An attacker may remove certain parts of a legitimate *CTU*. If the removed part(s) were located at the beginning of the *CTU* (corresponding to the most important bits of the bitframe), the reconstructed signal will be highly distorted. If the removed part(s) were located in the middle or at the end of the *CTU*, certain contents embedded with the signal will disappear. In both cases the failed verification of the digital signature of the *CTU* will alert authorized users about the tampering.
- Malicious edition of legitimate *CTU*(s). This is a combination of the previous types of attack. It requires knowing the plain biomedical test (thus, breaking the cryptosteganographic protection of the *CTU*), editing the signal and/or the embedded content(s) total or partially (as intended by the attacker) and re-encode the *CTU*. The last step includes re-encrypting the *CTU* and replacing the previous signature with a new valid one, the latter requiring the private key of a trusted coding device — which is highly unlikely to obtain.

It can be concluded that the careful combination of cryptography and steganography, on the basis of an efficient biomedical signal compressor that returns a bitframe ordered by relevance, are the pillars supporting the security of this novel coding algorithm. The previous security assessment indicates that the only manner to weaken the security of this coding is by successfully attacking its manifold cryptographic protection — partial, symmetric and asymmetric. Therefore, the security of this coding cannot be considered as lower than the security of a solution based on cryptography only. In fact, the protection provided by the — symmetric — encryption of the *containers* is strengthened by hiding their locations in the *CTU*(s).

#### 4.4.2 Potential limitations

In short, it can be said that the test coding proposed guarantees that the biomedical signal is decoded with clinical quality, by means of the standard signal decoder, using as input the plain, coded signal attaching protected metadata. When the signal is partially encrypted (this is decided based on the consent of the user/patient), the information for its decryption is contained in the metadata, and thus the latter cannot be removed without losing the possibility of decoding the signal. However, when the signal is not partially encrypted, the protected metadata (or part of it) can be removed and the signal can still be decoded with clinical value. This can be seen as a potential limitation of the coding, since the removal of the metadata is detected (there is no valid signature anymore) but it does not impede the reconstruction of the signal. It would be desirable that the removal of the protected metadata destroys the clinical content of the signal, guaranteeing an optimal binding between the signal and the metadata. To enforce this requirement, it is necessary to interleave the metadata between two (or more) signal coded segments, in such a manner that if the metadata is removed or the *CTU* is truncated before the metadata, the reconstructed signal will not have clinical validity. This admits various coding alternatives — e.g. replacing refinement bits in selected coded signal segment(s) with metadata, replacing only certain refinement bits or both significant and refinement bits — whose performance (foreseen as a higher security level at the cost of higher complexity and less coding efficiency) would need to be evaluated and compared with the current approach.

## 4.5 Keytagging biomedical image-based tests

The second signal-based security technique developed in this Thesis, called keytagging, is presented, analyzed and evaluated throughout Sections 4.5-4.8. The procedure proposed for associating keytags  $\{KT\}$ , to bind the content of some tags  $\{T\}$  to an image  $I_{or}$ , is formally described in Algorithm 3 and illustrated by means of an example in Figure 4.6; while the procedure for retrieving  $\{T\}$  from  $I_{or}$ , or from some modified version  $\tilde{I}_{or}$ , is defined in Algorithm 4.  $\{KeytagType\}$  is an important input parameter of these algorithms, which establishes the expected robustness of the tags when  $I_{or}$  undergoes common image modifications in the biomedical context and, according to it, their security applications (analyzed in Section 4.7). Stable tags are expected to be retrieved with low distortion even when  $\tilde{I}_{or}$  has undergone aggressive image modifications which may have caused the loss of its clinical value, semistable tags are intended to remain undistorted only if  $\tilde{I}_{or}$  has undergone mild modifications and preserves the clinical value of  $I_{or}$ , and volatile tags are intended to be retrieved highly distorted even if the modifications of  $\tilde{I}_{or}$  are minor. Both Algorithm 3 and 4 rely on a preprocessing of the image, a selection of appropriate image features, a compact coding/decoding of the keytags and cryptographic protection of/access to the keytags. These processes are depicted in detail throughout Sections 4.5.1-4.5.4, which follow the notation described in Table 4.7. Finally, Section 4.5.5 describes how keytagging can be integrated within the JPEG2000 compressor.

### 4.5.1 Preprocessing

The first step of Algorithms 3-4 (line 2) is the segmentation of the region of interest (*ROI*) of the image, so that the tags can be associated to the most important parts of the image. The intention is to prevent the tags from being distorted or removed due to modifications affecting the *RONI*, such as biomedical image compression by areas [173], blackening private data for anonymization or the insertion of visible watermarks. If all the tag are associated outside the *RONI*, these modifications would be incapable of distorting or removing them. In some biomedical image modalities, an algorithm has been designed to obtain the *ROI* automatically, as is the case in [381] with the atherosclerotic plaque ultrasound. In addition to this, several biomedical image acquisition devices currently deliver the image *ROI* separated from the blocks of associated data that compose the *RONI* (see Figure 2.4). As explained in Section 2.1.4, in the DICOM standard [79] a calibration configuration was introduced for ultrasound images in which regions are defined with the same calibration. But since not all acquisition devices have this built-in capability, the *ROI* may be roughly segmented by means of some simple method, with the only conditions that the same method shall be used in both Algorithms 3-4 and

Table 4.7: Operators and notation of the keytagging algorithm

Notation	Meaning
$output(s) \leftarrow f(input(s))$	Assignment of value to one or several outputs from a function or operator $f()$ with one or several inputs.
$[ ], [ ], \oplus$	Operators of concatenation, rounding to the nearest greater integer and binary XOR.
$\{X\}$	Set of elements of type $X$ , each element $i$ represented as $X\{i\}$ .
$\#X$	Number of elements that compose the set $X$ .
$V(i : j : k)$	Vector derived from a vector $V$ , corresponding to a subset of its elements, $[V(i), V(i + j), V(i + 2 \cdot j), \dots, V(k)]$ .
$M(:)$	Vector derived from a matrix $M$ , corresponding to the concatenation of its rows, $[M(1, :), M(2, :), \dots, M(end, :)]$ .
$I_{or}$	Original image to be used for keytagging.
$\tilde{I}_{or}$	Modified version of $I_{or}$ (e.g. compressed, filtered, clipped, rotated).
$ROI(I), RONI(I)$	Regions of interest and non-interest of an image $I$ .
$MBR$	Minimum bounding rectangle.
$R(I), G(I), B(I)$	Levels of $R, G$ and $B$ colors in RGB format of an image $I$ .
$I_g$	Grayscale image derived from an image $I$ .
CDF 9/7 or 5/3	Cohen-Daubechies-Feauveau 9/7-tap or 5/3 (also known as LeGall) filters.
$Coeff, h, w \leftarrow WT(I, \underline{f}, j)$	Function that returns $Coeff$ , the $j$ -th wavelet decomposition calculated with filters $\underline{f}$ of an image $I$ ; $h$ and $w$ , the height and width of the wavelet decomposition levels from 1 to $j$ .
$MWL(I)$	Maximum wavelet decomposition level of an image $I$ .
$LL, LH, LH, HH$	Coefficients of a wavelet subband obtained with horizontal and vertical low-pass filtering ( $LL$ ), horizontal high-pass filtering and vertical low-pass filtering ( $LH$ ), horizontal low-pass and vertical high-pass filtering ( $LH$ ), and horizontal and vertical high-pass filtering ( $HH$ ).
$aWL(I)$	Wavelet level allowed for an image $I$ to associate certain tag(s).
$C$	Subset of coefficients from $aWL$ .
$F$	Features from $C$ used for the coding of one or several $T$ .
$abs(X)$	Absolute value(s) of $X$ .
$LSB(X)$	Least significant bit(s) of $X$ .
$T$	Tag, binary data string to be associated to an $I_{or}$ by means of a $KT$ .
$\tilde{T}$	Tag retrieved from a modified image, $\tilde{I}_{or}$ .
$s.out \leftarrow LFSR(s, t)$	Linear feedback shift register with initial state $s$ and taps $t$ .
$GolombSeq$	A binary sequence that meets Golomb's randomness postulates.
$(X)^*$	A scrambled binary sequence derived from $X$ by means of a reversible transformation.
$BM$	Bi-level map that encodes a tag as positions of certain coefficients of $aWL$ .
$KT$	Keytag, which permits the retrieval of a $T$ from an image.
$Sk$	Secret key used for symmetric encryption-decryption.
$PrU$	Private key to be used by user $U$ for asymmetric decryption of data or for its signature.
$PbU$	Public key of user $U$ , used by any user for asymmetric encryption of data intended for $U$ , or to verify any signature issued by $U$ .
$DS(D, \underline{Alg}, PrU)$	Digital signature of $D$ using the algorithm $\underline{Alg}$ and the private key of the signatory $U$ .
$checkDS(D, \underline{Alg}, PbU)$	Verification of the $DS$ of $D$ by using the algorithm $\underline{Alg}$ public key of the signatory $U$ .
$encrypt(Plaintext, \underline{Alg}, K)$	Encryption of $Plaintext$ using the algorithm $\underline{Alg}$ and the key $K$ .
$decrypt(Ciphertext, \underline{Alg}, K)$	Decryption of $Ciphertext$ using the algorithm $\underline{Alg}$ and the key $K$ .

that it shall leave out at least part of the black background and peripheral text of the image (if any). It is recommended performing the automatic delineation of the minimum bounding rectangle (*MBR*) that encloses the biomedical image content (*ROI*). As a final step for the preprocessing, color *ROIs* are transformed into grayscale by calculation of their luma components according to the standard ITU-R Recommendation BT.601-7 [382] (Algorithms 3-4: line 3). This ensures compliance with both color and grayscale *ROIs*, and that further modifications of the color map does not affect the tag(s).

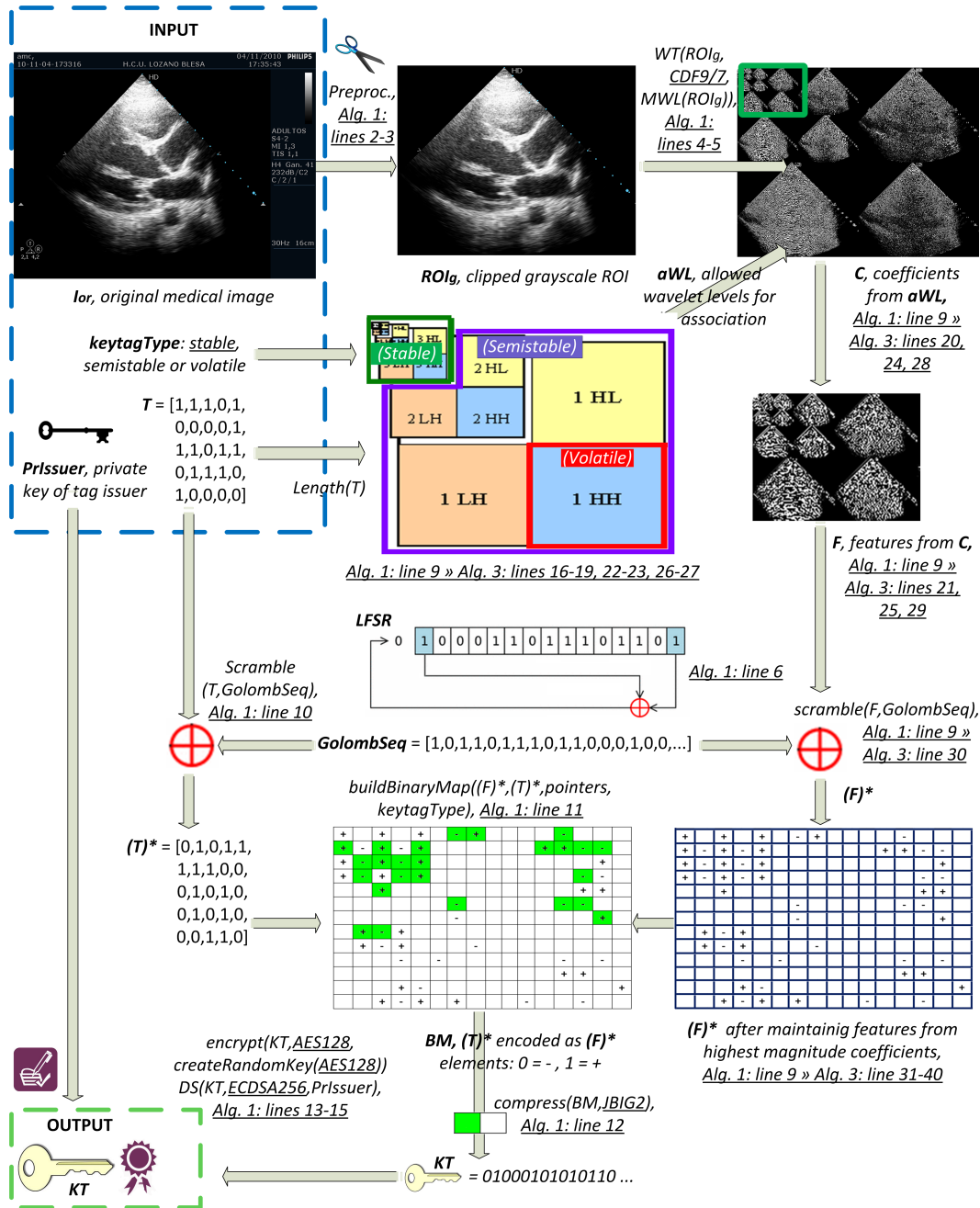


Figure 4.6: Main steps for the association of a stable keytag according to Algorithm 3.



### 4.5.2 Selection of suitable image features

The 2-D Discrete Wavelet Transform (see Section 2.2.1, Algorithms 3-4: line 5) decomposes the image into several scales, located in ordered regions of the transformed image, which host coefficients concentrating certain frequencies. This enables efficient compression and also facilitates keytag association because the transform separates stable, semistable and volatile parts of the image. The main advantage of using wavelets over other transforms is its variable resolution: the higher frequencies, which correspond to details (volatile features of the image), are represented with higher spatial resolution than the lower frequencies. To obtain  $WT(ROI_g, \underline{f}, j)$ ,  $ROI_g$  is initially filtered by rows and columns with two filters, decimated by two and arranged in four subimages:  $LL, LH, HL, HH$ . The process is iteratively repeated, taking the last  $LL$  as input, until reaching the desired  $j$ -th decomposition level. As a result, the lowest frequencies (most important parts, stable features) of the image are represented with only a few high-magnitude coefficients, located in the upper-left corner of  $WT(ROI_g, \underline{f}, j)$  —note this in the 5th-level decomposition in Figure 2.6: upper left corner. The choice of the wavelet family, which sets the filters  $\underline{f}$ , is relevant for compression but it was empirically found that it does not have a big impact on the robustness-capacity tradeoff. The only exception to the latter rule was observed when  $\underline{f}$  are set to those used by a compressor, which improves the robustness to this compressor for a given capacity. Thus, the choice is using the filters implemented by the widespread JPEG2000 compressor (see Section 4.5.5), CDF 9/7 for lossy compression and CDF 5/3 for lossless compression, which also saves a number of operations when keytagging is combined with compression (see Section 4.6.5). If the information about the compressor is not available,  $\underline{f}$  is set to CDF 9/7 since further compression would be more likely performed with lossy JPEG2000.

In keytagging, the choice of wavelet level,  $j$ , is very relevant. High  $j$  values permit obtaining very stable image features from the lowest frequencies. Tags retrieved from keytags associated to these features endure with little or no distortion high image compression rates and aggressive low-pass image filtering, e.g. averaging masks, Gaussian and median filters. Therefore, the choice is setting the highest possible value (Algorithms 3-4: line 4),  $MWL$ , given by the maximum number of recursive steps of decimation by 2. Furthermore, it has been observed that each time a new decomposition level is calculated, the sum of the energy of the coefficients in the four resulting subbands exceeds the energy of the coefficients in the mother subband. Thus, calculating the maximum decomposition level maximizes the number of high magnitude coefficients available for keytagging. As is shown in Table 4.8, the highest decomposition levels concentrate more energy,  $\frac{\sum_{i,j \in \text{subband}} C(i,j)^2}{\#C(i,j) \in \text{subband}}$ , from the lowest frequencies. Nonetheless, they have fewer coefficients, which results in less capacity.

Table 4.8: Average energy and maximum number of coefficients in the wavelet subbands of the images from the keytagging test set

Subband	Level 1		Level 2		Level 3		Level 4		Level 5		Level 6		Level 7		Level 8		Level 9	
	<i>En.</i>	<i>#C</i>	<i>En.</i>	<i>#C</i>	<i>En.</i>	<i>#C</i>	<i>En.</i>	<i>#C</i>	<i>En.</i>	<i>#C</i>	<i>En.</i>	<i>#C</i>	<i>En.</i>	<i>#C</i>	<i>En.</i>	<i>#C</i>	<i>En.</i>	<i>#C</i>
Approximation (LL)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	30.43	1
Horizontal detail (HL)	1.08	65,536	1.86	16,384	2.19	4,096	2.80	1,024	3.66	256	5.09	64	6.66	16	9.21	4	10.79	1
Vertical detail (LH)	1.21	65,536	1.96	16,384	2.34	4,096	3.01	1,024	3.62	256	4.67	64	6.43	16	7.59	4	13.23	1
Diagonal detail (HH)	0.42	65,536	1.03	16,384	1.32	4,096	1.59	1,024	2.05	256	2.69	64	3.75	16	4.50	4	4.55	1
Overall	2.71	196,608	4.86	49,152	5.85	12,288	7.40	3,072	9.33	768	12.45	192	16.84	48	21.29	12	58.99	4

Abbreviations:

*En.* is the energy of average energy of the coefficients in the subband,

*#C* is the number of coefficients in the subband.

To balance capacity and a suitable degree of robustness to typical image modifications in the biomedical context (see Section 4.6.1), it was determined through exhaustive testing that the optimal subset of wavelet coefficients  $C$  for the association of keytags comes from allowed wavelet levels,  $aWL \geq MWL - 6$  for stable keytags (Algorithm 5: lines 17, 20),  $aWL \leq MWL - 7$  for semistable (Algorithm 5: lines 23-24), and the  $HH$  subband of  $WL = 1$  for volatile keytags (Algorithm 5: lines 27-28). This multiplexing of keytags in the wavelet domain is represented in Figure 4.6: center. In addition to this, the final  $aWL$  for stable keytags is adjusted to the length of the tag. It was empirically found that setting  $aWL$  to the maximum wavelet level that contains a number of coefficients  $\geq 10 \cdot \text{length}(T)$  (Algorithm 5: lines 18-19) improves the endurance of tags to local operations such as median filtering, while maintaining the endurance to compression and common image processing. This occurs thanks to the restriction of preserving only those features coming from the lowest frequencies of the image, the most robust to low-pass filtering. Finally, the features  $F$  that will be used for keytag coding are extracted. These are the sign bit of the coefficients in  $C$  (the most robust to image changes, Algorithm 5: lines 21, 25) if the tag is stable/semistable and the  $LSB$  if the tag is volatile (Algorithm 5: line 29).

### 4.5.3 Coding and decoding of keytags

The coding and decoding of keytags produces the same effect as the embedding and retrieval of zero-watermarks — the association and reading of certain contents to/from the image without distorting it —, but following a different procedure conceived to achieve a better robustness-capacity tradeoff with simple operations and guaranteeing high security and specificity. A keytag basically encodes an input tag  $T$ , a binary string, as the positions of selected binary features  $F$  from the subset  $C$ . The extraction of  $C$  from  $ROI_g$  depends on the intended tag type (stable, semistable or volatile), as explained in Section 4.5.2. The coding proposed below is intended to bound the keytag with the image in a compact and fast manner. To ensure this bounding, each feature  $F$  can encode only one  $T$  bit. Otherwise, it would be known that each time that a certain feature is repeated, it encodes the same bit value, so a percentage of  $T$  bits could be derived from the keytag without the image. In addition to this, the algorithm encodes unidirectionally since changes of direction would indicate that two consecutive  $T$  bits have opposite values.

To minimize the size of the keytags,  $T$  and  $F$  are transformed into  $(T)^*$  and  $(F)^*$  by means of a scrambling process (Algorithm 3: lines 9-10). The intention of this scrambling is that the mean bit value of  $(T)^*$  and  $(F)^*$  is approximately 0.5, and that any long series of 0s or 1s is broken. To scramble the bits of  $T$  and  $F$  in a reversible manner (see Algorithm 5: line 42), they are XOR-ed with a sequence meeting Golomb's randomness postulates [383], so that the operation can be reversed by a second XOR with the same sequence.

Golomb's postulates establish that in this type of random sequences 1) the number of 1s and 0s is approximately the same; 2) half of the bits in the sequence belong to a series of length 1 (e.g. ...010..., ...101...), a quarter of the bits in the sequence belong to a series of length 2 (e.g. ...0110..., ...1001...), an eighth of the bits in the sequence belong to a series of length 3 (e.g. ...01110..., ...10001...) and so on; and 3) that the out-of-phase correlation  $AC(k)$  has the same value with different values of  $k$ . The procedure to obtain a Golomb sequence consists of running a non-zero input in a linear feedback shift register [344] (see Algorithm 5: lines 42-46) with taps described by an irreducible polynomial of the finite field  $F_2$  [384]. The polynomial  $x^{17} + x^3 + 1$  (see Algorithm 3: line 6) was chosen since it obtains a high periodicity of  $2^{17} - 1$ , much larger than the size of any  $T$  to be used in the evaluation (see Section 4.6), and truncate the resulting Golomb sequence to the length of  $T/F$ .

As a result of scrambling, there is a probability of 0.5 of encoding a  $(T_i)^*$  bit with the first available feature in  $(F)^*$  (when  $(T_i)^* = (F_j)^*$ ), a probability of  $(1 - 0.5) \cdot 0.5 = 0.5^2$  of encoding it with the second available feature (if  $(T_i)^* \neq (F_j)^*$ ,  $(T_i)^* = (F_{j+1})^*$ ), a probability of  $(1 - 0.5)^2 \cdot 0.5 = 0.5^3$  of encoding it with the third available feature (if  $(T_i)^* \neq (F_j)^*$ ,  $(T_i)^* \neq (F_{j+1})^*$ ,  $(T_i)^* = (F_{j+2})^*$ ) and so on. According to this, the sum of the series  $\sum_{k=1}^{\infty} (0.5)^k \cdot k$  gives the average number of features from  $(F)^*$  required to encode a  $(T)^*$  bit, 2. To guarantee high robustness, the function *buildBinaryMap* (Algorithm 3: line 11) keeps only those features of  $F$  coming from the  $N$  highest-magnitude coefficients in  $abs(C)$  for the coding (see Algorithm 5: lines 31-40).  $N$  is the minimum number of features from  $(F)^*$  required for the coding of any  $(T)^*$  of a certain length. It has already been demonstrated that the average number of features required is  $2 \cdot length(T)$ , so setting  $N = (2 + 6\sigma(length(T))) \cdot length(T)$  ensures that the number of tags which can not be completely coded is  $< 1$  for every  $5 \cdot 10^8$ . To set reliable values for the standard deviation,  $\sigma(length(T))$ ,  $10^6$  random  $(F)^*$  and  $(T)^*$  were created for each length corresponding to the powers of 2 ranging from 64 to 8192 bits, and the coding was carried out. To generate realistic random binary sequences  $T$  and  $F$ , individual pseudo-random float sequences  $\{X\}$  with uniform distribution probability  $Pr(X) \in [0, 1]$  were created, and transformed into binary sequences with random bias by doing  $Y = ((-1)^{X\{1\} < 0.5}) \cdot 0.5 \cdot X\{2\} + X > 0.5$ . The results from the coding test showed that the mean value of  $N$  was exactly  $2 \cdot (length(T))$  and that the  $\sigma$  for those tag lengths was  $[0.1853, 0.1218, 0.0865, 0.0629, 0.0423, 0.0292, 0.0214, 0.0150]$ . If a given  $length(T)$  is among two of these studied values (e.g. 2048 and 4096), the  $\sigma$  of the lower of these two values is used. Next, *buildBinaryMap* creates a bi-level map  $BM$  of the same size as  $C$  and initializes all its elements to be white (see Algorithm 3: line 24). This function encodes in  $BM$  the  $(T)^*$  bits as features  $(F_j)^*$ : the first element moving forward along  $(F)^*$  from the last encoding element  $j - 1$  whose feature value matches the  $(T_i)^*$  bit value

to be encoded is marked as a black pixel in the same position in  $BM$  (see Algorithm 3: 25-38 and Figure 4.6: bottom). This process is repeated until all  $(T)^*$  bits have been coded. Finally, for a compact arithmetic coding of  $BM$ , the standard JBIG2 [385] is applied in lossless mode (Algorithm 3: line 12). It uses a context-dependent algorithm called the QM coder. The result is the keytag  $KT$ , which will be used to reverse this process and retrieve  $(T)^*$ , by overlapping  $(F)^*$  and  $BM$ , and obtain  $T$  (Algorithm 4: line 15).

#### 4.5.4 Cryptographic protection of keytags

Since the keytagging algorithms are intended to become public, they shall include cryptographic protection for the keytags. In the first place, the tag issuer shall digitally sign his/her keytags with his/her private key for signature ( $PrIssuer$ , see Algorithm 3: line 13), so that any user can verify their origin and integrity with its paired public key ( $PbIssuer$ , see Algorithm 4: line 10). In addition to this, confidential keytags shall be encrypted with random keys ( $Sk\{i\}$ , see Algorithm 3: lines 14-15), which will be grouped and encrypted with the public key of each intended user ( $PbUser\{i\}$ , see Algorithm 3: lines 16-21). In this way, only authorized users can retrieve their symmetric keys with their private keys ( $PrUser\{i\}$ , see Algorithm 4: lines 7) and decrypt their authorized keytags (Algorithm 4: line 9). According to the recommendations of the (IHE) SDO profile (Section 2.6.3), these are the choice for the following:

- Digital signature of a keytag  $KT$ : The standardized Elliptic Curve Digital Signature Algorithm 256 [366], which performs signature-verification in 3.92 – 6.56 *Mcycles*.  $PbIssuer-PrIssuer$  shall be renewed every 1-3 years. As part of the checking of a digital signature, it is required to verify that the digital certificate of the signatory has not expired or been revoked, by means of Check Revocation Lists or by using the Online Certificate Status Protocol [386].
- Symmetric encryption of a keytag  $KT$ : Twofish [356], whose encryption/decryption speed is 29.4 cycles/byte. Its key size is set to 128 bits and its block size is also 128 bits, so padding bits will be added if the data to be encrypted is not a multiple of this block size. A symmetric key shall be created to encrypt each keytag.
- Asymmetric encryption of authorized users' access keys  $SkU$ : RSA2048 [360], which performs encryption-decryption in 0.29 – 11.22 *Mcycles* (per block). The block size of RSA2048 is 2048 bits, so there will be overhead if the data to be encrypted is not a multiple of this block size, and its performance for encryption-decryption is 0.29 – 11.22 *Mcycles* per block. Asymmetric encryption keys,  $PbUsers-PrUsers$ , shall be renewed every 1-2 years

**Algorithm 3** Keytag association

---

```

1: procedure KEYTAGGING( $I_{or}$ ,  $f$ ,  $\{T\}$ ,  $\{keytagType\}$ ,  $PrIssuer$ ,  $\{authorizedTags\}$ ,  $\{PbUser\}$ )
2:    $ROI(I_{or}) \leftarrow segmentation(I_{or}, \underline{MBR})$   $\triangleright$  To segment the  $ROI$ 
3:    $ROI_g \leftarrow 0.299 \cdot R(ROI(I_{or})) + 0.587 \cdot G(ROI(I_{or})) + 0.114 \cdot B(ROI(I_{or}))$   $\triangleright$   $ROI$  to grayscale
4:    $MWL(ROI_g) \leftarrow \lceil \log_2(\min(\#rows(ROI_g), \#columns(ROI_g))) \rceil$   $\triangleright$  Max. wavelet decomp. level
5:    $Coeff, h, w \leftarrow WT(ROI_g, f, MWL(ROI_g))$   $\triangleright$  Wavelet transformation of  $ROI_g$ 
6:    $GolombSeq \leftarrow LFSR([1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0], [17, 3])$   $\triangleright$  See Algorithm 5
7:    $pointers \leftarrow [1, 1, 1]$ 
8:   for  $i$  in 1 to  $\#T$  do  $\triangleright$  This loop associates one keytag in each iteration
9:      $(F)^* \leftarrow extractFeatures(Coeff, h, w, 1, keytagType\{i\}, length(T\{i\}), MWL(ROI_g), GolombSeq)$ 
10:     $(T\{i\})^* \leftarrow scramble(T\{i\}, GolombSeq)$   $\triangleright$  See Algorithm 5
11:     $BM, pointers \leftarrow buildBinaryMap((F)^*, (T\{i\})^*, pointers, keytagType\{i\})$ 
12:     $KT\{i\} \leftarrow compress(BM, \underline{JBIG2})$ 
13:     $KT\{i\} \leftarrow [KT\{i\}, DS(KT\{i\}, \underline{ECDSA256}, PrIssuer)]$   $\triangleright$  Adding a signature to each keytag
14:     $Sk\{i\} \leftarrow createRandomKey(\underline{Twofish128})$ 
15:     $KT\{i\} \leftarrow encrypt(KT\{i\}, \underline{Twofish128}, Sk\{i\})$   $\triangleright$  Symmetric encryption of each keytag
16:  for  $i$  in 1 to  $\#PbUsers$  do  $\triangleright$  This loop prepares the cryptographic material
17:     $SkU \leftarrow [ ]$   $\triangleright$  to allow users to retrieve their authorized keytags
18:    for  $j$  in 1 to  $\#T$  do
19:      if  $(authorizedTags\{i, j\})$  then  $\triangleright$   $authorizedTags$  sets which users
20:         $SkU \leftarrow [SkU, Sk\{j\}]$   $\triangleright$  have access to each keytag
21:     $KeysUser\{i\} \leftarrow encrypt(SkU, \underline{RSA2048}, PbUser\{i\})$   $\triangleright$  Only an authorized user can decrypt
     $\triangleright$  his/her entry with his/her  $PrUser$ 
22:  return  $\{KT\}, \{KeysUser\}$ 

23: procedure BUILDBINARYMAP( $(F)^*$ ,  $(T\{i\})^*$ ,  $pointers$ ,  $keytagType$ )  $\triangleright$  To build the binary map
     $\triangleright$  that encodes  $(T\{i\})^*$  as elements in  $(F)^*$ 
24:    $BM \leftarrow zeros((F)^*)$   $\triangleright$  Initialized as a matrix of zeros with the same size as  $(F)^*$ 
25:   if  $keytagType = Stable$  then
26:      $p \leftarrow 1$ 
27:   else if  $keytagType = Semistable$  then
28:      $p \leftarrow 2$ 
29:   else  $\triangleright$   $keytagType$  is Volatile
30:      $p \leftarrow 3$ 
31:    $index \leftarrow pointers(p)$   $\triangleright$  To continue encoding from the first available position
32:   for  $v$  in 1 to  $length((T\{i\})^*)$  do
33:      $r, s \leftarrow obtainIndices((F)^*, index)$   $\triangleright$  See Algorithm 5
34:     while  $(T\{i\})^*(v) \neq (F)^*(r, s)$  do  $\triangleright$  To move forward along  $(F)^*$  from the last
35:        $index \leftarrow index + 1$   $\triangleright$  encoding element until their values match
36:        $r, s \leftarrow obtainIndices((F)^*, index)$ 
37:        $BM(r, s) \leftarrow 1$   $\triangleright$  To record the position where the element  $v$  in  $(T\{i\})^*$ 
38:        $index \leftarrow index + 1$   $\triangleright$  matches the first available element in  $(F)^*$ 
39:    $indices \leftarrow pointers$ 
40:    $indices(p) \leftarrow index$   $\triangleright$  To update the pointer used
41:  return  $BM, indices$ 

```

---

**Algorithm 4** Tag retrieval

---

```

1: procedure TAGRETRIEVAL( $I_{or}$ ,  $f$ ,  $\{KT\}$ ,  $\{keytagType\}$ ,  $PbIssuer$ ,  $KeysUser$ ,  $PrUser$ )
2:    $ROI(I_{or}) \leftarrow segmentation(I_{or}, MBR)$   $\triangleright$  To segment the  $ROI$ 
3:    $ROI_g \leftarrow 0.299 \cdot R(ROI(I_{or})) + 0.587 \cdot G(ROI(I_{or})) + 0.114 \cdot B(ROI(I_{or}))$   $\triangleright$   $ROI$  to grayscale
4:    $MWL(ROI_g) \leftarrow \lceil \log_2(\min(\#rows(ROI_g), \#columns(ROI_g))) \rceil$   $\triangleright$  Max. wavelet decomp. level
5:    $Coeff, h, w \leftarrow WT(ROI_g, f, MWL(ROI_g))$   $\triangleright$  Wavelet transformation of  $ROI_g$ 
6:    $GolombSeq \leftarrow LFSR([1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0], [17, 3])$   $\triangleright$  See Algorithm 5
7:    $\{Sk\} \leftarrow decrypt(KeysUser, RSA2048, PrUser)$   $\triangleright$  To obtain the keys of the user's keytags
8:   for  $i$  in 1 to  $\#KT$  do  $\triangleright$  This loop retrieves a tag in each iteration
9:      $KT\{i\} \leftarrow decrypt(KT\{i\}, Twofish128, Sk\{i\})$   $\triangleright$  To decrypt the keytag
10:    if  $checkDS(KT\{i\}, ECDSA256, PbIssuer)$  then  $\triangleright$  To verify its digital signature
11:       $KT\{i\} \leftarrow removeDS(KT\{i\})$   $\triangleright$  To remove the signature after verification
12:       $BM \leftarrow uncompress(KT\{i\}, JBIG2)$   $\triangleright$  To obtain the binary map that encodes a tag
13:       $lengthT \leftarrow sum(BM)$   $\triangleright$  The length of the tag is the number of 1s in  $BM$ 
14:       $(F)^* \leftarrow extractFeatures(Coeff, h, w, 0, keytagType\{i\}, lengthT, MWL(ROI_g), GolombSeq)$ 
15:       $T\{i\} \leftarrow extractTag((F)^*, BM, GolombSeq)$ 
16:    else  $\triangleright$  The tag is not retrieved if the
17:       $Warning\ caused\ by\ invalid\ signature$   $\triangleright$  signature of its keytag is invalid
18:    return  $\{T\}$ 

19: procedure EXTRACTTAG( $(F)^*$ ,  $BM$ ,  $GolombSeq$ )  $\triangleright$  To extract a tag from  $(F)^*$  by means of  $BM$ 
20:    $(T)^* \leftarrow []$ 
21:   for  $r$  in 1 to  $\#rows(BM)$  do
22:     for  $s$  in 1 to  $\#columns(BM)$  do
23:       if  $BM(r, s)$  then  $\triangleright$  To move along  $BM$  and find the 1s, which spot
24:          $(T)^* \leftarrow [(T)^*, (F)^*(r, s)]$   $\triangleright$  the positions in  $(F)^*$  that encode the bits of  $(T)^*$ 
25:    $T \leftarrow scramble((T)^*, GolombSeq)$   $\triangleright$  To retrieve the original tag,  $T$ 
26:   return  $T$ 

```

---

**Algorithm 5** Auxiliary procedures used in keytag association and tag retrieval (I)

---

```

1: procedure LFSR( $s, t$ )  $\triangleright$  To calculate the output of running a  $LFSR$  with initial state  $s$  and taps  $t$ 
2:    $n \leftarrow length(s)$ 
3:    $m \leftarrow length(t)$ 
4:    $c(1, :) \leftarrow s$   $\triangleright$   $C$  stores in its rows all the states of the  $LFSR$ 
5:   for  $k$  in 1 to  $2^n - 2$  do
6:      $b(1) \leftarrow s(t(1)) \oplus s(t(2))$   $\triangleright$   $b$  is used to calculate the
7:     if  $m > 2$  then  $\triangleright$  feedback for the next state
8:       for  $i$  in 1 to  $m - 2$  do
9:          $b(i + 1) \leftarrow s(t(i + 2)) \oplus b(i)$ 
10:     $s(2 : n) \leftarrow s(1 : n - 1)$   $\triangleright$  Shifting the bits of the state one position
11:     $s(1) \leftarrow b(m - 1)$   $\triangleright$  The first element in the state is the feedback
12:     $c(k + 1, :) \leftarrow s$   $\triangleright$  from the previous
13:    $s\_outS \leftarrow c(:, n)$   $\triangleright$  The output is the concatenation of the outputs of each state
14:   return  $s\_out$ 

```

---

**Algorithm 5** Auxiliary procedures used in keytag association and tag retrieval (II)

---

```

15: procedure EXTRACTFEATURES(Coef, h, w, filter, keytagType, lengthT, MWL, GolombSeq)
16:   if (keytagType = Stable) then
17:     aWL  $\leftarrow$  MWL - 6 ▷ Selecting coefficients from top levels, such their number of
18:     while  $h(aWL + 1) \cdot w(aWL + 1) \geq 10 \cdot \text{length}T$  do ▷ coefficients exceeds  $10 \cdot \text{length}T$ 
19:       aWL  $\leftarrow$  aWL + 1 ▷ The maximum number of coefficients to be
20:       C  $\leftarrow$  Coef(1 : h(aWL), 1 : w(aWL)) ▷ selected are those from levels  $\geq MWL - 6$ 
21:       F  $\leftarrow$  (C  $\geq$  0) ▷ and the features of interest are their signs
22:   else if (keytagType = Semistable) then
23:     aWL  $\leftarrow$  MWL - 7 ▷ Selecting coefficients from levels  $\leq MWL - 7$ 
24:     C(1 : h(aWL + 1), 1 : w(aWL + 1))  $\leftarrow$  0 ▷ by setting coefficients from levels  $\geq MWL - 6$  to 0,
25:     F  $\leftarrow$  (C  $\geq$  0) ▷ the features of interest are their signs
26:   else ▷ keytagType is Volatile
27:     aWL  $\leftarrow$  1 ▷ Selecting coefficients from
28:     C  $\leftarrow$  Coef(h(aWL + 1) + 1 : end, w(aWL + 1) + 1 : end) ▷ the HH subband of level 1,
29:     F  $\leftarrow$  LSB(C) ▷ the features of interest are their LSBs
30:     (F)*  $\leftarrow$  scramble(F, GolombSeq)
31:   if filter then ▷ Removing the features from the  $2 + 6 \cdot \sigma(\text{length}T)$  lowest magnitude coefficients
32:      $\sigma_s = [0.1853, 0.1218, 0.0865, 0.0629, 0.0423, 0.0292, 0.0214, 0.0150]$ 
33:     lengths = [64, 128, 256, 512, 1024, 2048, 4096, 8192]
34:     for i in 1 to length( $\sigma_s$ ) do ▷ This loop sets the value of  $\sigma$ 
35:       if  $\text{length}T \leq \text{lengths}(i)$  then ▷ according to the value of lengthT
36:          $\sigma \leftarrow \sigma_s(i)$ 
37:         sorted_values, sorted_indices  $\leftarrow$  sort(abs(C(:)), descending) ▷ Obtaining the indices of
38:         indicesToDelete  $\leftarrow$  sorted_indices( $\lceil (2 + 6 \cdot \sigma) \cdot \text{length}T \rceil$  : end) ▷ the lowest magnitude
39:         rows_IndicesToDelete, cols_IndicesToDelete  $\leftarrow$  obtainIndices(indicesToDelete, C) ▷ coefs,
40:         (F)*(rows_IndicesToDelete, cols_IndicesToDelete)  $\leftarrow$  2 ▷ which are removed by setting them
41:   return (F)* ▷ to 2, a value not existing in T (composed of 0s and 1s)
42: procedure SCRAMBLE(M, GolombSeq) ▷ To scramble/descramble a binary vector
43:   (M)*  $\leftarrow$  M ▷ or matrix M by adding GolombSeq
44:   for i in 1 to #rows(M) do
45:     (M)*(i, :)  $\leftarrow$  M(i, :)  $\oplus$  GolombSeq( $1 + (i - 1) \cdot \#columns(M) : i \cdot \#columns(M)$ )
46:   return (M)*
47: procedure OBTAININDICES(M, pointers) ▷ To translate unidimensional pointers into
48:   r  $\leftarrow$   $\lceil \text{pointers} / \#columns(M) \rceil$  ▷ bidimensional indices for a matrix M
49:   s  $\leftarrow$   $1 + \text{module}(\text{pointers} - 1, \#columns(M))$ 
50:   return r, s ▷ r are de indices for rows, s are the indices for columns
51: procedure ZEROS(M) ▷ To initialize a vector/matrix of zeros
52:   zerosM  $\leftarrow$  M ▷ of the same size as M
53:   zerosM(1 : end, 1 : end)  $\leftarrow$  0
54:   return zerosM
55: procedure SUM(M) ▷ To sum all the elements in a matrix/vector M
56:   S  $\leftarrow$  0
57:   for i in 1 to #rows(M) do
58:     for j in 1 to #columns(M) do
59:       S  $\leftarrow$  S + M(i, j)
60:   return S

```

---



### 4.5.5 Support for JPEG2000 compression

Both the JPEG2000 compression standard, depicted in Section 2.2.3, and the keytagging process share the use of wavelets (Section 2.2.1), with the same filters, for a representation of the image adjusted to the properties of the human vision system. As a result, JPEG2000 compression causes no or very little distortion to the retrieved stable and semistable tags, as is demonstrated in Section 4.6.4. In addition to this, if the keytags association is integrated in the compression process, most of the runtime cost of the former is covered by the latter (see Section 4.6.5). In the case of volatile tags, the compression would destroy them, as this process is a modification of the original image. Otherwise, if it is desired that this initial compression is not detected, the volatile keytags shall be associated after the whole JPEG2000 encoding is completed and the first encoded wavelet decomposition level — where volatile keytags are associated — is available. Finally, it is worth noting that the JPEG2000 formats JP2 and JPX allow the embedding of metadata, which can be used to conveniently store the keytags.

The processes of the JPEG2000 encoder and decoder are illustrated in Figure 2.9. To ensure full compliance of compression with keytagging, the initial color transformation must be the irreversible ICT and the further tiling of the image must be set to its size. The last steps of the compression (tier 1 and 2 encoding) are independent from the keytagging. These are performing context modeling and bit-plane arithmetic coding, arranging the coded data in layers corresponding to quality levels and performing post-compression rate allocation.

## 4.6 Experimental evaluation of keytagging

The features of this algorithm that need to be experimentally evaluated are its robustness-capacity tradeoff when the image undergoes different image modifications, its specificity when the original image is replaced, its compatibility with JPEG2000 compression, its average runtime cost for different parameter configurations and its scalability when the image size is increased. Complementarily, Section 4.7 analyzes the security foundations of the keytagging method.

### 4.6.1 Evaluation setup

The image test set is composed of 64 images, sized  $512 \times 512 px^2$ , corresponding to different medical modalities (see Figure 4.7) and parts of the body:

- 18 computed tomography (CT) images, gathered from [387]: 6 chest (Artifix), 6 dental area (Incisix) and 6 pelvis (Pelvix) images.
- 18 magnetic resonance images (MRI), gathered from [387]: 6 brain (Brainix), 6 knee (Knix) and 6 thoracic and lumbar area (MRIX) images.
- 12 positron emission tomography (PET)-CT images from a whole body scan, gathered from [387] (PETCETIX).
- 16 ultrasound images (US): 4 mode B echocardiograms provided by Lozano Blesa Hospital in Zaragoza, 4 mode M, 4 Doppler color, 4 pulsed and continuous wave Doppler.

The image test set is processed with typical modifications in the biomedical context, which are indexed for reference in Figure 4.8 and Tables 4.9-4.14:

- 1-10. Compression: JPEG with quality factors 75%, 50%, 25%, 15% and 5% (Figure 4.8: 5), JPEG2000 with compression ratios 4:1, 8:1, 16:1, 32:1 and 64:1 (Figure 4.8: 10).
- 11-18. Common image processing:  $\beta$  correction  $-0.3$ ,  $-0.5$  (Figure 4.8: 12),  $+0.4$  and  $+0.7$  (Figure 4.8: 14), contrast stretching 2% and 10% (Figure 4.8: 16), color inversion (Figure 4.8: 17) and local histogram equalization (Figure 4.8: 18).
- 19-27. Local operations: edge sharpening (Figure 4.8: 19), median filtering  $5 \times 5$  and  $7 \times 7$  (Figure 4.8: 21), averaging mask  $5 \times 5$  and  $7 \times 7$  (Figure 4.8: 23), Gaussian filtering  $7 \times 7$  and  $11 \times 11$ , and motion blur with 7 and 9 pixels displacement (Figure 4.8: 27).
- 28-33. Geometric transformations: clipping the *ROI*, rotating  $90^\circ$ ,  $180^\circ$  and  $270^\circ$ , horizontal and vertical flipping (Figure 4.8: 33).
- 34. Insertion of visible annotations (Figure 4.8: 34).
- 35. Blackening private data parts for anonymization.

and attempting to distort the tag or part of it, by means of a watermark-based attack:

- 36-40. Modification of  $l = 64$  (Figure 4.8: 34),  $l = 128$ ,  $l = 256$ ,  $l = 512$ ,  $l = 1024$  and  $l = 2048$  sign bits from the highest-level wavelet coefficients of the image.

The robustness of keytagging to those modifications is evaluated by measuring the distortion of the retrieved tags  $\tilde{T}$  with respect to the original  $T$  associated to  $I_{or}$ , by means of the Normalized Hamming Distance [388]:

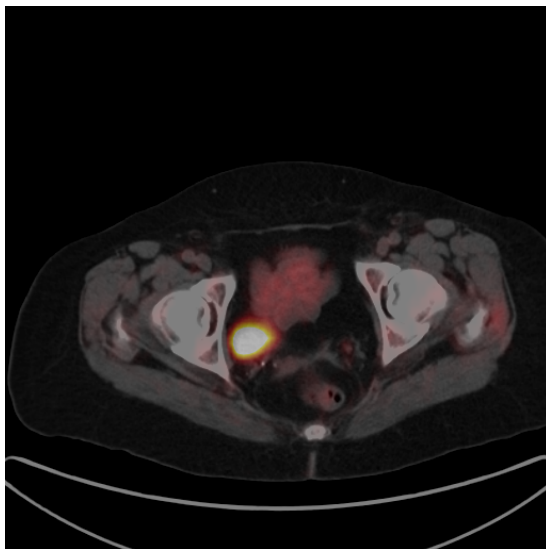
$$NHD = \frac{\tilde{T} \oplus T}{\text{length}(T)}, \quad (4.5)$$



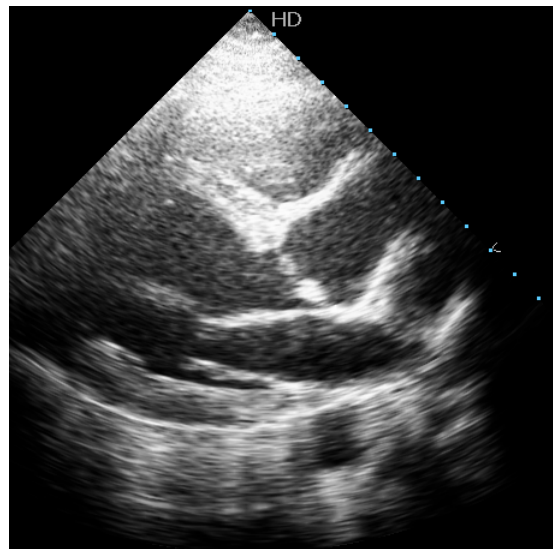
(a) Computed tomography



(b) Magnetic resonance



(c) Positron emission tomography



(d) Ultrasound

Figure 4.7: Sample images from the keytagging test set, belonging to different acquisition modalities.

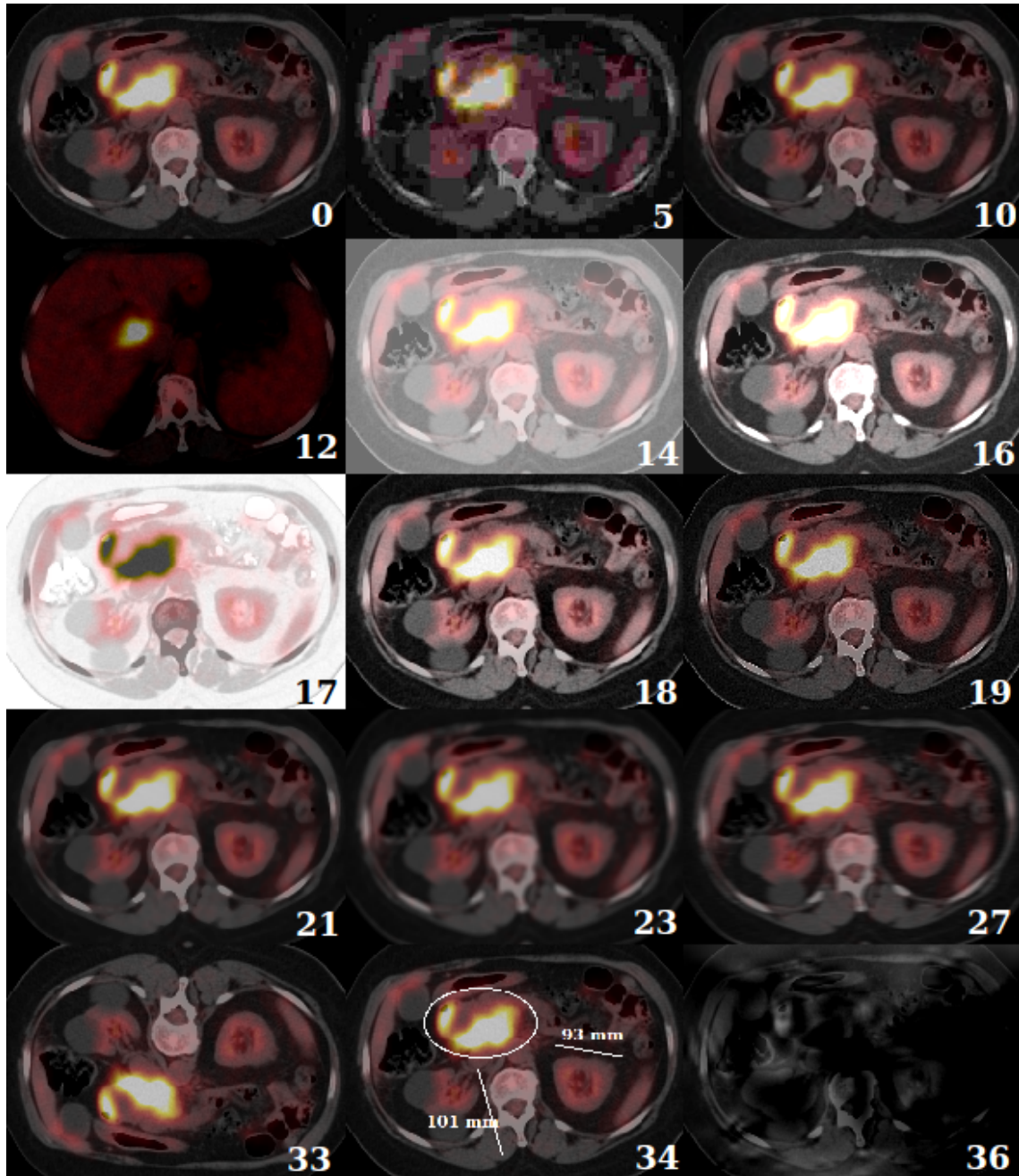


Figure 4.8: *ROI* of a  $512 \times 512 \text{ px}^2$  PET-CT image, original (0) and resulting from the application of JPEG QF=5% and JPEG2000 CR 64:1 compression (5,10),  $\beta$  correction  $-0.5$  and  $+0.7$  (12,14), 10% contrast stretching (16), color inversion (17), local histogram equalization (18), edge sharpening (19), median filter  $7 \times 7$  (21), image averaging  $7 \times 7$  (23), motion blur 9 (27), vertical flipping (33), insertion of annotations (34) and watermark-based attack with  $l=128$  (36).

where  $T$  and  $\tilde{T}$  are binary vectors and  $\oplus$  is the XOR logical operator. Those  $\tilde{T}$  that endure the image modifications end up very similar to  $T$  and obtain  $NHD \approx 0$ , while those  $\tilde{T}$  which are very dissimilar to  $T$  obtain  $NHD \approx 0.5$ , e.g. when retrieved from very degraded versions of  $I_{or}$ . The Normalized Hamming Distance is very useful to determine how much redundancy needs to be added to overcome the distortion of  $\tilde{T}$  by means of some redundant coding.

*Simulation setup 1:* The image modifications described above are applied to the test set. A fixed-length random tag  $T$  is associated to each image, by means of keytags  $KT$ , retrieving  $\tilde{T}$  from the corresponding modified image  $\tilde{I}_{or}$ . The resulting  $NHD$  is calculated, and the process of keytag association-tag retrieval is repeated for different tag lengths and for the three types of keytags: stable, semistable and volatile. The results are depicted in Tables 4.9-4.12, which also shows how much distortion is caused to  $ROI_g$  (the area of  $I_{or}$  used for the association of keytags) by each modification (which results in a  $\tilde{ROI}_g$ ), measured with two different indices, the classic Peak Signal-to-Noise Ratio and the mean Structural SIMilarity index:

$$PSNR(I, \tilde{I}) = 20 \cdot \log_{10} \left( \frac{\max(I(:))}{\sqrt{\frac{1}{\#rows(I) \cdot \#cols(I)} \cdot \sum_{i=1}^{\#rows(I)} \sum_{j=1}^{\#cols(I)} \|I(i, j) - \tilde{I}(i, j)\|^2}} \right), \quad (4.6)$$

$$MSSIM(I, \tilde{I}) = \frac{1}{M} \sum_{j=1}^M \frac{(2 \cdot \mu_{I_j} \mu_{\tilde{I}_j} + (0.01 \cdot L)^2) \cdot (2 \cdot \sum_{i=1}^N w_i \cdot (I_i - \mu_I)(\tilde{I}_i - \mu_{\tilde{I}}) + (0.03 \cdot L)^2)}{(\mu_{I_j}^2 + \mu_{\tilde{I}_j}^2 + (0.01 \cdot L)^2) \cdot (\sum_{i=1}^N w_i \cdot ((I_i - \mu_I)^2 + (\tilde{I}_i - \mu_{\tilde{I}})^2) + (0.03 \cdot L)^2)}, \quad (4.7)$$

where  $L$  is the dynamic range of the pixel values (255 for 8-bit grayscale images),  $w_i$  correspond to an  $11 \times 11$  circular-symmetric Gaussian weighting function with standard deviation 1.5 samples (normalized so that  $\sum_{i=1}^N w_i = 1$ ),  $\mu_I = \sum_{i=1}^N w_i \cdot I_i$ ,  $M$  is the number of local windows in the image and  $N$  the number of pixels in the local window. Further details about this index may be consulted in [389] and the implementation of the *MSSIM* algorithm used in this work is available online at [390].

The *PSNR* is a simple mathematical measure that directly compares the value of the pixels from the two images. Although it is very popular, the correlation between this measure and the visual perception of quality is not tight enough in many cases. The *MSSIM* assumes that the human vision system is highly adapted for extracting structural information from images. Thus, it basically compares local patterns of pixel intensities that have been normalized for luminance and contrast.

*Simulation setup 2:* This follows the process of setup 1 but considers each image as a modified version of the rest. This setup is intended to evaluate the degree of distortion of tags retrieved from images that are different from the original ones. Since some images of the test set come from the same patient and acquisition session, some pairs of  $ROI_g$  are quite similar: five have  $PSNR > 20$  dB and  $MSSIM > 0.67$ , and may obtain low  $NHD$  values.

Table 4.9: Average distortion of variable-length stable, semistable and volatile tags when the keytagging image test set (unshaded cells) and its interpolated counterpart (lightly shaded cells when calculating  $aWL$  according to Algorithm 3, shaded cells when maintaining the  $aWL$  of the original test set) undergo common modifications in the biomedical context (see Sections 4.6.1 and 4.6.6)

#. Operation	Length(T)	Image size — $px^2$ —	Image quality — $PSNR(dB)$ , $MSSIM$ —	Distortion of stable tags — $NHD$ (%)—					Distortion of semistable tags — $NHD$ (%)—							Distortion of volatile tags — $NHD$ (%)—				
				128/BCH	256/BCH	512/BCH	1024/BCH	2048	128/BCH	256/BCH	512/BCH	1024/BCH	2048/BCH	4096/BCH	8192/BCH	16384/BCH	64	128	256	
Compression																				
1.	JPEG QF=75%	512 × 512	37.7, 0.98	0	0	0	0	0	0	0	0	0	0.2/0	1.2/0.3	4.2/10.6	11.8/19.8	48.4	48.4	49.4	
	JPEG QF=30%	1024 × 1024	38.9, 0.98	0	0	0	0	0	0	0	0	0	0.4/0	2.4/4.5	6.5/13.8	50.8	50	49.8		
	JPEG QF=30%	1024 × 1024	38.9, 0.98	0	0	0	0	0	0	0	0	0.3/0	1/0	2.7/7.9	8.2/14.9	15.9/23.5	50.8	50	49.8	
2.	JPEG QF=50%	512 × 512	35.2, 0.97	0	0	0	0	0	0	0	0	0.3/0	1.2/0	3.9/7.7	8.7/16.6	18.5/26.1	48.4	49.2	49.8	
	JPEG QF=20%	1024 × 1024	37.0, 0.97	0	0	0	0	0	0	0	0	0.2/0	0.2/0	1.2/0.4	4.5/10.9	11.1/18.8	49.2	50.2	50.1	
	JPEG QF=20%	1024 × 1024	37.0, 0.97	0	0	0	0	0	0	0	0	0.2/0	1/0	2.5/4.4	6.3/13.1	13.6/22	21.3/29.6	49.2	50.2	50.1
3.	JPEG QF=25%	512 × 512	33.2, 0.95	0	0	0	0	0.2	0	0	0.6/0	1.4/0	4/7.8	8.8/17.2	17.2/26.3	26.3/33.5	50	49.6	50.8	
	JPEG QF=15%	1024 × 1024	35.3, 0.92	0	0	0	0	0.2	0	0	0	0.1/0	0.6/0	2.5/7.9	8.5/14.9	14.9/22.3	50	49.2	49.9	
	JPEG QF=15%	1024 × 1024	35.3, 0.92	0	0	0	0	0	0	0	0.4/0	1.4/0	4.2/9.1	10.1/17.2	18.5/26.2	25.8/32.6	50	49.2	49.9	
4.	JPEG QF=15%	512 × 512	31.4, 0.92	0	0	0	0	1.9	0	0.8/0	1.4/0	4.7/7.4	9.7/15.3	17/25	26.6/33.8	34/38.6	49.2	50.8	49.6	
	JPEG QF=10%	1024 × 1024	33.2, 0.92	0	0	0	0	1	0	0	0	0.5/0	2.2/4.4	6.7/13.7	14.2/23.4	23.9/31.5	50.8	49.8	49.8	
	JPEG QF=10%	1024 × 1024	33.2, 0.92	0	0	0	0	0.3	0	0.4/0	1.4/0	3.9/8.2	8.7/15.2	15.9/23.7	23.8/31.3	32.2/37.5	50.8	49.8	49.8	
5.	JPEG QF=5%	512 × 512	26.7, 0.80	0	0	0.7/0	4.5/5.9	13.6	3.5/10.8	7.2/10.2	12.6/16.6	18.8/23.9	27/32.6	34.3/39.2	40.1/43.9	44.5/45.8	46.9	50	49.8	
	JPEG QF=5%	1024 × 1024	28.9, 0.74	0	0	0	0/2.6	6.3	0	0.4/0	1.4/0	4.3/10.4	10.5/17.4	18.6/26.4	26.9/34	35/39.4	50.8	50.8	49.7	
	JPEG QF=5%	1024 × 1024	28.9, 0.74	0	0	0	0.9/0	3.8	3.1/9.1	4.5/10	8/15.6	14/20.9	20.6/27.6	27.6/33.3	34.1/39.3	40.2/43.5	50.8	50.8	49.7	
6.	JPEG2000 CR 4:1	512 × 512	50.5, 1.0	0	0	0	0	0	0	0	0	0	0	0	0	0	51.6	50	50	
	JPEG2000 CR 16:1	1024 × 1024	50.2, 1.0	0	0	0	0	0	0	0	0	0	0	0	0	0	50	50	50	
	JPEG2000 CR 16:1	1024 × 1024	50.2, 1.0	0	0	0	0	0	0	0	0	0	0	0	0	0.3/0	50	50	50	
7.	JPEG2000 CR 8:1	512 × 512	47.6, 0.99	0	0	0	0	0	0	0	0	0	0	0	0	1.7/7.9	50	49.2	50.2	
	JPEG2000 CR 32:1	1024 × 1024	47.3, 1.0	0	0	0	0	0	0	0	0	0	0	0	0	0.7/0.4	50	49.2	50.2	
	JPEG2000 CR 32:1	1024 × 1024	47.3, 1.0	0	0	0	0	0	0	0	0	0	0	0	0.3/0	2.7/9.7	50	49.2	50.2	
8.	JPEG2000 CR 16:1	512 × 512	42.7, 0.99	0	0	0	0	0	0	0	0	0	0	0.2/0	1.7/7.2	8.7/16.1	51.6	49.2	50.4	
	JPEG2000 CR 64:1	1024 × 1024	42.0, 0.99	0	0	0	0	0	0	0	0	0	0	0.1/0	1.6/4.3	6.4/13.7	50	49	50.4	
	JPEG2000 CR 64:1	1024 × 1024	42.0, 0.99	0	0	0	0	0	0	0	0	0	0.2/0	1.6/1.3	5.2/12	12.2/20	50	49	50.4	
9.	JPEG2000 CR 32:1	512 × 512	37.9, 0.96	0	0	0	0	0.2	0	0	0	0	0.9/1.2	5.1/11.9	12.3/21.8	21.3/29.7	49.2	48.4	48.8	
	JPEG2000 CR 128:1	1024 × 1024	37.8, 0.96	0	0	0	0	0.2	0	0	0	0.1/0	0.9/0.4	4.6/11.9	11.4/21.4	21.3/29.8	50	49.8	50.2	
	JPEG2000 CR 128:1	1024 × 1024	37.8, 0.96	0	0	0	0	0	0	0	0.7/0	2.5/8.1	7/14.7	12.5/22.4	20.1/30.4	28.1/36.4	50	49.8	50.2	
10.	JPEG2000 CR 64:1	512 × 512	33.6, 0.92	0	0	0	0.2/0	3.3	0	0	0.4/0	2.8/7	7.8/16.5	16.4/25.9	27.5/34.1	35.2/39.6	51.6	50	50	
	JPEG2000 CR 256:1	1024 × 1024	33.7, 0.91	0	0	0	0.1/0	3.4	0	0	0.3/0	2.4/5.8	7.8/15	16.5/25.3	26.4/33.7	34.4/39.2	50	49.6	49.7	
	JPEG2000 CR 256:1	1024 × 1024	33.7, 0.91	0	0	0	0.2/0	2.3	2.3/7	4.5/7.2	7.3/11	13.1/18.5	19.7/27.6	27/35.5	33.6/40.4	39.8/43.8	50	49.6	49.7	



Table 4.10: Average distortion of variable-length stable, semistable and volatile tags when the keytagging image test set (unshaded cells) and its interpolated counterpart (lightly shaded cells when calculating  $aWL$  according to Algorithm 3, shaded cells when maintaining the  $aWL$  of the original test set) undergo common image processing in the biomedical context (see Sections 4.6.1 and 4.6.6)

#. Operation	$Length(T)$	Image size	Image quality	Distortion of stable tags					Distortion of semistable tags							Distortion of volatile tags			
		$-px^2-$	$-PSNR(dB),$ $MSSIM-$	$-NHD (%) -$					$-NHD (%) -$							$-NHD (%) -$			
		-	-	128/BCH	256/BCH	512/BCH	1024/BCH	2048	128/BCH	256/BCH	512/BCH	1024/BCH	2048/BCH	4096/BCH	8192/BCH	16384/BCH	64	128	256
Common image processing																			
11. $\beta$ correction $-0.3$	$512 \times 512$	512 × 512	20.7, 0.85	0	0	0	0	0.3	0	0	0	0	0	0	0.2/0	0.7/0	50	49.6	49.8
$\beta$ correction $-0.3$	$1024 \times 1024$	1024 × 1024	21.1, 0.80	0	0	0	0	0.3	0	0	0	0	0	0	0.2/0	0.6/0	48.8	49.6	48.6
$\beta$ correction $-0.3$	$1024 \times 1024$	1024 × 1024	21.1, 0.80	0	0	0	0	0	0	0	0	0	0	0.2/0	0.4/0	0.8/0	48.8	49.6	48.6
12. $\beta$ correction $-0.5$	$512 \times 512$	512 × 512	16.1, 0.60	0	0.4/0	0.2/0	0.8/0	2	0	0	0.1/0	0.2/0	0.5/0	1.1/0	2.1/0.7	4.6/8.8	50	50	49.6
$\beta$ correction $-0.5$	$1024 \times 1024$	1024 × 1024	16.3, 0.50	0	0.2/0	0.2/0	0.7/0	2.1	0	0	0.1/0	0.3/0	0.7/0	1.3/0	2.9/0.6	5/5.3	50	50.8	49.8
$\beta$ correction $-0.5$	$1024 \times 1024$	1024 × 1024	16.3, 0.50	0	0.4/0	0.2/0	0.7/0	1	0	0.8	1.1/0	1.3/0	1.8/0	3/0.3	4.3/5.7	7.1/10.4	50	50.8	49.8
13. $\beta$ correction $+0.4$	$512 \times 512$	512 × 512	17.1, 0.74	0	0	0	0	0.1	0	0	0	0	0.1/0	0.2/0	0.2/0	0.3/0	50	49.2	49
$\beta$ correction $+0.4$	$1024 \times 1024$	1024 × 1024	17.1, 0.71	0	0	0	0	0.1	0	0	0	0	0	0.2/0	0.3/0	0.4/0	47.7	48	48.7
$\beta$ correction $+0.4$	$1024 \times 1024$	1024 × 1024	17.1, 0.71	0	0	0	0	0	0	0	0	0	0.2/0	0.3/0	0.4/0	0.5/0	47.7	48	48.7
14. $\beta$ correction $+0.7$	$512 \times 512$	512 × 512	10.7, 0.49	0	0	0.1/0	0.5/0	1	0	0	0.2/0	0.6/0	0.8/0	1/0	1.4/0	1.6/0	51.6	49.6	50.4
$\beta$ correction $+0.7$	$1024 \times 1024$	1024 × 1024	10.7, 0.45	0	0	0.2/0	0.5/0	1.1	0	0	0.2/0	0.5/0	1/0	1.2/0	1.7/0	2.2/0	49.2	50.4	50.1
$\beta$ correction $+0.7$	$1024 \times 1024$	1024 × 1024	10.7, 0.45	0	0	0.2/0	0.5/0	0.5	0	0.8/0	1/0	1.4/0	1.7/0	1.9/0	2.3/0	2.8/0	49.2	50.4	50.1
15. Contrast stretching 2%	$512 \times 512$	512 × 512	18.1, 0.87	0	0	0	0.1/0	0.2	0	0	0	0.2/0	0.3/0	0.6/0	0.9/0	1/0	50	49.2	49.2
Contrast stretching 2%	$1024 \times 1024$	1024 × 1024	18.1, 0.72	0	0	0	0.1/0	0.2	0	0	0.2/0	0.2/0	0.7/0	1/0	1.3/0	1.5/0	49.6	49.4	49
Contrast stretching 2%	$1024 \times 1024$	1024 × 1024	18.1, 0.72	0	0	0	0.1/0	0.2	1.6/0	0.4/0	0.5/0	0.8/0	1.7/0	1.9/0	1.9/0	1.9/0	49.6	49.4	49
16. Contrast stretching 10%	$512 \times 512$	512 × 512	16.6, 0.83	0	0	0	0.3/0	0.5	0	0	0.1/0	0.3/0	1.5/0	1.7/0	1.8/0	1.9/0	47.7	50	50
Contrast stretching 10%	$1024 \times 1024$	1024 × 1024	16.2, 0.66	0	0	0.2/0	0.2/0	0.7	0	0	0.3/0	1.1/0	1.5/0	2.2/0	2.7/0	3/0	50	50	49.8
Contrast stretching 10%	$1024 \times 1024$	1024 × 1024	16.2, 0.66	0	0	0.2/0	0.5/0	0.5	1.6/0	1.4/0	1.5/0	3.5/0	2.9/0	3.4/0	3.5/0	3.7/0	50	50	49.8
17. Invert colors	Any size	Any size	2.7, -0.10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18. Local hist. equal.	$512 \times 512$	512 × 512	21.3, 0.86	0	0	0	0.1/0	0.3	0	0	0	0	0.1/0	0.3/0	0.5/0	0.7/0	50	50	50
Local hist. equal.	$1024 \times 1024$	1024 × 1024	21.2, 0.81	0	0	0	0.1/0	0.4	0	0	0	0.1/0	0.1/0	0.4/0	0.8/0	1.1/0	49.6	50.2	49.4
Local hist. equal.	$1024 \times 1024$	1024 × 1024	21.2, 0.81	0	0	0	0.1/0	0.1	0	0	0.2/0	0.2/0	0.6/0	1/0	1.5/0	1.7/0	49.6	50.2	49.4

Table 4.11: Average distortion of variable-length stable, semistable and volatile tags when the keytagging image test set (unshaded cells) and its interpolated counterpart (lightly shaded cells when calculating  $aWL$  according to Algorithm 3, shaded cells when maintaining the  $aWL$  of the original test set) undergo local operations (see Section 4.6.1 and 4.6.6)

#. Operation	Image size — $px^2$ —	Image quality — $PSNR(dB)$ , $MSSIM$ —	Distortion of stable tags — $NHD$ (%)—					Distortion of semistable tags — $NHD$ (%)—								Distortion of volatile tags — $NHD$ (%)—		
			128/BCH	256/BCH	512/BCH	1024/BCH	2048	128/BCH	256/BCH	512/BCH	1024/BCH	2048/BCH	4096/BCH	8192/BCH	16384/BCH	64	128	256
Local operations																		
19. Edge sharpening	512 × 512	24.4, 0.89	0	0	0	0.1/0	0.5	0	0	0	0	0.2/0	0.4/0	0.6/0	1.2/0	48.4	48.8	48.8
Edge sharpening	1024 × 1024	25.4, 0.89	0	0	0	0.1/0	0.5	0	0.6/0	0.5/0	0.8/0	0.8/0	1.1/0	1.7/0	2.4/0.1	49.2	49.4	49.7
Edge sharpening	1024 × 1024	25.4, 0.89	0	0	0	0.1/0	0.3	1.6/0	2.3/0	2.8/0	2.6/0	2.7/0	2.8/0	3.5/0.6	4.6/2.7	49.2	49.4	49.7
20. Median filter 5 × 5	512 × 512	27.8, 0.92	0	0	0	0.2/0	1	5.5	5.7/6.8	9.1/11	13.1/16.3	20.4/22	27.3/28.5	31.8/33.4	35.8/37.7	50	49.2	50
Median filter 11 × 11	1024 × 1024	27.8, 0.92	0	0	0	0.4/0	1.6	4.3/6.6	5.9/7.8	10.6/13.6	15.6/17.7	23.3/25.3	29.9/31.6	35.7/36.3	39.1/39.9	48.4	50.4	49.8
Median filter 11 × 11	1024 × 1024	27.8, 0.92	0	0	0	0.4/1	5.7	41/43.8	40.4/42.7	40.5/43.9	41.2/44.8	42/47.3	44.7/48.5	46.6/49.2	47.2/47.9	48.4	50.4	49.8
21. Median filter 7 × 7	512 × 512	25.5, 0.87	0	0	0.8/0	1.9/0	4.8	23.4/23.2	25/24.5	21.6/28.3	27/32.5	32/37.2	36.3/40.5	39.4/42.4	41.5/44.3	50.8	50	50
Median filter 14 × 14	1024 × 1024	25.4, 0.88	0	0	1/0	2.1/0	4.8	22.3/22.8	21.3/23.8	23.1/27.8	25.7/32.2	32.6/36.6	37.2/40.4	40.3/43.6	43.7/45.2	50	50	49.8
Median filter 14 × 14	1024 × 1024	25.4, 0.88	0	0	1/0	2.3/9.1	13.4	46.1/45.2	46.1/48.2	45.9/47.6	45.6/47	47.2/47.9	47.1/48	47.8/47.4	47.7/49.2	50	50	49.8
22. Image averaging 5 × 5	512 × 512	26.2, 0.91	0	0	0	0.2/0	1	16.8/17.4	29.1/22.3	32.8/28.1	36.7/36.6	40.7/37.9	45.5/44.4	49.2/45.9	50/46.9	49.2	49.6	50.4
Image averaging 11 × 11	1024 × 1024	26.3, 0.90	0	0	0.2/0	0.5/0	1.8	12.1/18.9	18.6/19.7	25.1/27.2	32/35.7	40.6/41.5	47.9/46.9	51.7/49.3	51.7/49.9	50.8	50.4	49.6
Image averaging 11 × 11	1024 × 1024	26.3, 0.90	0	0	0.1/0	0.6/6.1	11.5	77.3/77.5	74.8/77.9	72/73.9	69/70.1	64.7/65	63/62.9	61.2/58.8	56.6/57.4	50.8	50.4	49.6
23. Image averaging 7 × 7	512 × 512	23.8, 0.85	0	0	1.3/0	2.6/0.3	5.5	53.9/49.6	49.4/51.9	50.9/53.5	50.3/54.9	54.7/55.7	54.8/55.1	54.1/54.4	54/53.1	48.4	48.8	50.2
Image averaging 13 × 13	1024 × 1024	25.1, 0.87	0	0	0.6/0	1.7/0	4.1	35.9/35.7	35.4/36.5	39.3/41.7	44.6/49.5	50.5/54.1	52/54.9	55.5/55.2	54.4/53.4	50.4	50.6	50.6
Image averaging 13 × 13	1024 × 1024	25.1, 0.87	0	0	0.8/0	1.9/12.5	19.7	81.3/76.4	80.5/77.1	77.6/74.4	73.2/70.2	67.3/67.7	63.1/65.7	60.9/61.2	58.1/54.9	50.4	50.6	50.6
24. Gaussian filtering 7 × 7	512 × 512	25.7, 0.90	0	0	0.2/0	0.5/0	1.7	3.1/3.3	4.5/5.5	7.3/10.9	12.4/17.6	20.5/22	25.5/29.3	31.4/33.4	36.3/38.1	50	50	49.6
Gaussian filtering 14 × 14	1024 × 1024	26.2, 0.90	0	0	0	0.3/0	1.3	0	0.8/0	2.3/1	4.9/6.1	8.9/10.2	12.2/16.8	17/21.1	23.8/26.4	50.8	50.4	50.6
Gaussian filtering 14 × 14	1024 × 1024	26.2, 0.90	0	0	0	0.4/0	2.9	3.5/4.3	3.9/6.9	7.6/11.1	12.4/15.8	16.8/22.1	20.8/26.1	26.6/32	32.5/35.5	50.8	50.4	50.6
25. Gaussian filtering 11 × 11	512 × 512	24.4, 0.89	0	0	0.4/0	1.1/0	2.9	4.7/6.1	6.3/6.8	9.6/12	14.3/20.7	23.8/26	29.2/30.7	33.4/35.5	38.1/39.2	51.6	50.4	50.2
Gaussian filtering 17 × 17	1024 × 1024	25.1, 0.87	0	0	0	0.1/0	0.9	0.8/0	2/0	4/3.6	6.7/6.9	10.4/11.7	14.3/17.7	19.3/22.8	25/27.7	50.8	50	49.4
Gaussian filtering 17 × 17	1024 × 1024	25.1, 0.87	0	0	0	0.2/0	2.9	5.5/7.9	7.8/9.5	10.2/13.5	14.3/17.9	19.2/24.7	23.5/28.3	27.6/33.2	32.9/36.8	50.8	50	49.4
26. Motion blur 7	512 × 512	27.7, 0.92	0	0	0.4/0	0.8/0	1.7	24.6/19.5	20.3/20.3	21.4/21.1	22.2/22.9	23.7/24.3	27.6/29	30.2/31.2	32.9/32.8	51.6	50.8	50
Motion blur 15	1024 × 1024	27.3, 0.92	0	0	0.4/0	1.2/0	2.7	25.8/25.2	23/24.6	23.1/22.1	23.1/22.1	23/24.3	24.5/26.2	27.3/29	30.1/30.3	49.2	49.6	49.4
Motion blur 15	1024 × 1024	27.3, 0.92	0	0	0.6/0	1.5/0.6	11.4	25.8/24.6	24.8/21.8	21.3/20.8	22/23.2	24.2/24.6	25.5/26.9	28.8/28.3	28.9/29	49.2	49.6	49.4
27. Motion blur 9	512 × 512	26.0, 0.88	0	0	2.1/0	3.6/0.2	6.3	33.2/32.2	31.6/30.5	27.1/28.4	29.5/28.6	29.6/29.9	32.5/33.6	35/36.1	36.3/35.7	51.6	50.8	50.4
Motion blur 17	1024 × 1024	26.7, 0.89	0	0	1.2/0	2.5/0	4.8	30.9/28.3	27.9/27	27.1/26.5	26.1/25.9	25.1/26.6	26.5/29	29.7/30.2	31.8/32.5	51.2	50	50.3
Motion blur 17	1024 × 1024	26.7, 0.89	0	0	1.4/0	2.9/1.5	15.7	18.8/18	17.8/18.9	20.3/20.4	21.2/22.6	23.1/25.7	25.4/27.7	28.1/29.7	30.5/31.1	51.2	50	50.3



Table 4.12: Average distortion of variable-length stable, semistable and volatile tags when the keytagging image test set (unshaded cells) and its interpolated counterpart (lightly shaded cells when calculating  $aWL$  according to Algorithm 3, shaded cells when maintaining the  $aWL$  of the original test set) undergo geometrical transformations, insertion of annotations and watermark-based attacks (see Section 4.6.1 and 4.6.6)

Length( $T$ ) # Operation	Image size — $px^2$ —	Image quality — $PSNR(dB)$ , — $MSSIM$ —	Distortion of stable tags — $NHD$ (%)—					Distortion of semistable tags — $NHD$ (%)—						Distortion of volatile tags — $NHD$ (%)—					
	-	-	128/BCH	256/BCH	512/BCH	1024/BCH	2048	128/BCH	256/BCH	512/BCH	1024/BCH	2048/BCH	4096/BCH	8192/BCH	16384/BCH	64	128	256	
Geometrical transformations																			
28. Clipping the $ROI$	Any size	Inf, 1.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
29. Rotating $90^\circ$	Any size	12.2, 0.26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
30. Rotating $180^\circ$	Any size	12.6, 0.29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
31. Rotating $270^\circ$	Any size	12.2, 0.24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
32. Horizontal flipping	Any size	14.8, 0.41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
33. Vertical flipping	Any size	12.9, 0.31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Inserting annotations																			
34. Inserting annotations	$512 \times 512$	28.7, 0.94	0	0	0	0	0.2	0	0	0	0	0	0	0	0.1/0	0.2/0	0.5	0.7	0.9
Inserting annotations	$1024 \times 1024$	28.4, 0.94	0	0	0	0	0.2	0	0	0	0	0	0	0.1/0	0.2/0	0.7	0.9	1.0	
Inserting annotations	$1024 \times 1024$	28.4, 0.94	0	0	0	0.1/0	0.3	0	0	0	0	0	0	0.1/0	0.2/0	0.7	0.9	1.0	
Darken private data																			
35. Darken private data	Any size	Inf, 1.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Watermark-based attack																			
36. $l = 128$	$512 \times 512$	13.0, 0.29	51.5/24.1	24.3/24.2	24.2/18.7	19.0/19.2	19.7	10.2/8.8	9.0/11.2	13.6/14.4	16.2/20.7	20.4/19.8	20.7/20.4	20.9/18.6	20.2/20.5	48.4	47.7	48.5	
$l = 128$	$1024 \times 1024$	12.2, 0.27	48.2/25.3	23.3/23.7	24.1/17.6	19.4/19.0	20.3	12.1/10.4	9.9/13.1	13.2/15.6	16.7/19.3	19.9/20.2	21.1/20.5	21.3/21.5	21.5/20.9	53.4	54.2	53.8	
$l = 128$	$1024 \times 1024$	12.2, 0.27	50.5/23.6	23.3/23.1	22.2/19.7	20.0/18.2	19.7	14.3/14.5	14.9/15.6	16.7/17.9	18.3/19.8	20.4/20	20.7/20.1	20.9/21.3	20.5/19.7	53.4	54.2	53.8	
37. $l = 256$	$512 \times 512$	12.7, 0.28	40.8/36.1	54.7/35.8	36.4/25.4	25.3/24.0	24.4	8.2/8.8	9.2	10.8/11	14.8/17.8	18.8/19.2	19.6/19.3	20.4/20.1	21.4/20.7	47.7	46.9	47.4	
$l = 256$	$1024 \times 1024$	12, 0.26	40.6/36.4	52.4/34.8	38.4/27.4	26.3/22.0	23.9	8.9/9.2	9.6/10.3	11/12.4	14.5/15.5	18.5/19.1	19.3/19.4	19.9/19.2	20.2/21.6	49.7	49.9	50.3	
$l = 256$	$1024 \times 1024$	12, 0.26	42.8/38.0	53.9/36.8	37.5/26.4	25.7/23.2	23.8	8.2/8.4	9.2/9.5	10.8/13.3	14.8/16.6	18.8/19.2	19.6/20.1	20.4/20	20.9/21.1	49.7	49.9	50.3	
38. $l = 512$	$512 \times 512$	12.3, 0.22	51.2/56.3	51.3/55.4	55.6/27.2	27.0/26.9	27.3	10.2/10.4	10.7/11.1	12.7/13	15.4/16.9	17.6/18.9	19.8/20.3	20.8/20.5	21.4/20.9	47.7	47.7	47.8	
$l = 512$	$1024 \times 1024$	11.9, 0.23	49.3/54.3	51.5/54.4	53.6/26.1	25.0/24.2	22.3	9.7/10.1	10.4/11.3	12.1/13.1	14.8/16.7	17.1/17.9	18/19.8	20.2/20.3	20.1/20.6	51.3	51.5	51.1	
$l = 512$	$1024 \times 1024$	11.9, 0.23	51.2/56.3	51.3/55.4	55.6/27.2	27.0/26.9	27.4	9.1/9.2	9.9/10.8	11.8/12.5	14.9/15.2	16.6/18.8	18.9/19.5	20.3/20.6	20.5/19.8	51.3	51.5	51.1	
39. $l = 1024$	$512 \times 512$	12.5, 0.26	43.9/40.8	53.6/41.6	41.5/56.6	57.8/46.3	46.4	11.7/12.1	12.5/13.3	15.4/15.5	16.1/18.6	17.3	19.3/20.3	21.2/21.8	22.6/21.6	50	49.2	50.1	
$l = 1024$	$1024 \times 1024$	12.7, 0.28	45.2/41.3	54.3/42	42.7/55.3	58.3/47.5	46.8	12.2/12.8	13.2/14.9	15.5/15.1	16.2/16.8	17/17.7	18.9/20.3	21/20.9	21.3/21.7	49.8	50.2	50	
$l = 1024$	$1024 \times 1024$	12.7, 0.28	44.5/41	53.9/41.9	42.2/56.9	58.1/46.7	46.6	11.5/12	12.2/13.1	14.9/15.2	15.8/17.1	16.9/18.5	19.2/20.2	21.3/21.1	20.7/20.3	49.8	50.2	50	
40. $l = 2048$	$512 \times 512$	12.3, 0.23	52.1/56.4	53.1/56.6	56.6/57.7	57.5/58.0	58.6	11.3/11.9	12.5/12.4	13.6/16.2	16.7/17.6	18.5/19.8	20.3/21.5	21.9/21	22.3/21.6	48.4	49.2	49.3	
$l = 2048$	$1024 \times 1024$	12.3, 0.24	53.3/55.9	54.2/55.2	56/54.4	54.9/54.4	55.6	11.7/11.9	12.8/13.3	14.1/15.9	16.8/18.2	18.3/18.4	20.2/20.8	21.5/22.1	22.1/19.8	50.4	50.2	49.8	
$l = 2048$	$1024 \times 1024$	12.3, 0.24	51.7/54.4	52.7/55.5	54.1/55.2	57.1/55.9	56.8	11.9/12.7	13.1/13.9	14.2/16.6	17.3/18	18.8/19.7	20.4/21.7	22.1/21	21.7/22.2	50.4	50.2	49.8	

### 4.6.2 Robustness-capacity

In the case of stable and semistable tags, there is a tradeoff between their lengths and their robustness to image modifications. Naturally, this occurs because the keytag association algorithm sorts and selects image features according to their degree of robustness, in descending order. Nonetheless, not all the modifications have the same impact on the image. Figure 4.8 illustrates the effect of several modifications from Section 4.6.1 on a biomedical image, and Tables 4.9-4.12: column 2 (unshaded cells) shows the average *PSNR* and *MSSIM* of the image test set after each modification. JPEG2000 compression is one of the most typical modifications. It maintains the image clinical value with compression factors around 16:1, obtaining  $PSNR \simeq 42 \text{ dB}$  and  $MSSIM \simeq 0.99$ . Higher compression ratios may cause unacceptable distortion, so they are not recommended. Common image processing techniques can help to find a better representation of the image.  $\beta$  correction changes the brightness and can be reversed; contrast stretching, local histogram equalization and color inversion help to enhance the details of the image, and the latter can be totally reversed. In the case of local operations, edge sharpening helps to enhance certain details, so it only modifies volatile parts of the image. The rest of the local operations modify both the semistable and volatile parts of the image, high and some middle frequencies, leaving only the stable parts intact. There are also several image modifications that neither affect the image quality nor distort its associated tags. These are clipping the *ROI*, since there are no keytags associated outside this region; geometrical changes, which are detected and reversed by means of a resynchronization step depicted in Section 4.7.2; inserting annotations, usually in the borders of the *ROI* or outside; and darkening private data, which is most often located outside the *ROI*. Finally, it was observed that modifying the sign of the most significant coefficients in the highest decomposition level is the most effective manner to willfully destroy stable tags, but at the cost of completely destroying the image as well, since the *PSNR* becomes  $\leq 13$ .

The results in Tables 4.9-4.12 (unshaded cells cells, left side of slashes), demonstrate that the overall robustness of stable tags to any tested image modification is high up to capacities of 512-1024 bits, with an average *NHD*  $< 1\%$ , decreasing for aggressive image compression and filtering at 2048 bits. It is worth mentioning that the local operations (except edge sharpening) are the most challenging modifications, since they affect many subbands. In fact, the motion blur modification yields an average  $NHD = 3.6\%$  in stable tags of 1024 bits. Since the number of coefficients available from level 3 (*aWL* for  $512 \times 512 \text{ px}^2$  images) to the top is 16,384, and only one feature can be extracted from each coefficient, associating tags longer than 2048 bits will make the overall robustness decrease sharply. BCH(511,259,30) coding [391] was successfully tested with stable tags to improve their robustness. Each tag is divided into blocks of 259 bits and encoded as

511-bit redundant blocks. Although it is then possible to correct up to 30 bits per block, the length of the associated keytag is almost double that of the keytag associated to the tag without BCH coding, which reduces its overall robustness. As can be seen in Tables 4.9-4.12 (unshaded cells, right side of slashes), the balance is positive and the  $NHD$  is reduced to 0 or almost 0 in most cases. Nonetheless, BCH can not be applied to all images for capacities of  $\geq 2048$  bits, which turn into  $\geq 4096$  bits after this coding, since some clipped  $ROIs$  do not have enough coefficients for the keytag association. Therefore, BCH coding-decoding will be applied to all stable tags with length  $\leq 1204$  bits, the coding as a previous step to Algorithm 3 and the decoding as a final step after Algorithm 4.

Semistable tags show good robustness to mild image compression and common image processing, e.g.  $NHD = 0.2\%$  with  $L = 4096$  for JPEG2000 compression 16:1,  $NHD = 0\%$  with  $L = 8192$  for 8 : 1. As was also expected, their robustness to modifications that remove details (e.g. image averaging  $7 \times 7$ ) is very low, while for edge sharpening, which enhances them, it is very high ( $NHD = 0.6\%$  for  $L = 8192$ ). It is also observed that BCH coding is pertinent for capacities up to 4096 bits, since it reduces the  $NHD$  of permissible modifications, which do not affect the clinical value of the image (JPEG2000 CR 16:1, common image processing and edges sharpening). Therefore, semistable tags with length  $\leq 4096$  bits will implement BCH coding. The  $NHD$  of permissible modifications is  $\leq 2.1\%$  for capacities of 8192 bits (to be implemented without BCH coding), which is tolerable. Nonetheless, it is not recommended exceeding this capacity since the distortion of permissible modifications increases a lot, e.g.  $NHD = 8.7\%$  for JPEG2000 CR 16:1 with tag length of 16384 bits. Finally, volatile tags present very low robustness, with  $NHD \approx 50\%$ , to any irreversible modification affecting the image  $ROI$  even when the tag length is very short.

### 4.6.3 Specificity

Specificity is a relevant feature of keytagging, since it measures how much information can be retrieved with a keytag when the image it is associated to is replaced with another image (not derived from the former). The distortion of the tags retrieved from non-original images shall be considerably high for two reasons: to avoid that someone can read the tag content without the original image (thus, affecting its privacy) and to avoid that someone can establish a relation between certain keytag and another image not associated to it (thus, affecting its security). The results of the specificity evaluation, using simulation setup 2 (see Section 4.6.1), are represented in Table 4.13. It can be seen that the average values of distortion for any keytag type and length are close to the ideal  $NHD$ , 50%, which guarantees perfect destruction of the tag content. Nevertheless, it is also observed that the shorter the keytag, the highest the likelihood of retrieving some tag with lower

distortion. In particular, the minimum  $NHD$  measured when retrieving the tag content with a very similar image was 12.5% and 15.6% for 128-bit stable and semistable keytags. Although these values far exceed those obtained when evaluating robustness (retrieving the tags from images derived from the original),  $NHD = 0\%$  for 128-bit stable keytags and semistable keytags, they shall be taken into account when designing certain keytag-based security measures (see Sections 4.7.3 and 4.7.5).

#### 4.6.4 Effect of JPEG2000 compression

As explained in Section 4.5.5, the keytagging algorithm has similarities with the JPEG2000 compressor. For this reason, the robustness of stable and semistable tags to JPEG2000 compression is high, as the results in Table 4.9 demonstrate. Nonetheless, to claim high compatibility with this compressor, the robustness to the image modifications tested in the table must also be evaluated in compressed versions of the original images. Since biomedical images are expected to be compressed with ratios around 16, it was tested with ratios of 8, 16 and 32. The new results, which are compared with those from the uncompressed images, are depicted in Table 4.14. Positive values imply that the results of the compressed test set are worse, since the  $NHD$  increases, while negative values indicate better results for the opposite reason. Thus, it is observed that the effect of keytagging compressed images instead of the original ones is null on the distortion of stable tags if their length is  $\leq 512$  bits. For 1024 bits, only two filters suffer a slight change, and for 2048 bits the  $NHD$  increases by an average of 0.2%, which is not significant. Semistable tags maintain very similar robustness to common processing, with the exception of  $\beta$  correction  $-0.5$  for a high capacity (8192 bits), which becomes significantly worse. Regarding local operations, there is an important change in the results of semistable tags, but their overall robustness to these operations is still low or very low, as intended. Volatile keytags maintain minimum robustness to any modification, with  $NHD \simeq 50\%$ . Geometrical modifications and darkening private data remain with  $NHD = 0$  for stable and semistable tags, and inserting annotations on the compressed images produces no or very slight change. Thus, it can be concluded that keytagging JPEG2000 compressed images instead of the original images obtains very similar results, which permits implementing the same applications with the same operating parameters (see Section 4.7).

Table 4.13: Distortion of variable-length stable, semistable and volatile tags when retrieved from an image different from the one they were associated to (see Sections 4.6.1 and 4.6.3)

		Distortion of stable tags — <i>NHD</i> (%)—					Distortion of semistable tags — <i>NHD</i> (%)—								Distortion of volatile tags — <i>NHD</i> (%)—			
		128	256	512	1024	2048	128	256	512	1024	2048	4096	8192	16384	64	128	256	
Measure	<i>Length</i> ( <i>T</i> )																	
Mean	— without BCH coding	48.8	49.2	49.7	49.8	49.9	49.6	49.9	50	50.1	50	50	50	50	50	50	49.9	50
	— with BCH coding	48.8	49.3	49.7	49.8	-	49.6	50	50	50.1	50	50	50	50	50	-	-	-
Standard deviation	— without BCH coding	4.5	3.7	2.6	1.9	1.3	4	2.8	2	1.3	1	0.6	0.5	0.4	5	3.5	2.5	
	— with BCH coding	5	3.6	2.6	1.9	-	3.9	2.8	2	1.3	1	0.6	0.5	0.4	-	-	-	
Minimum	— without BCH coding	13.3	18.8	24.2	30.6	36.7	15.6	23.6	37.9	40.7	44.7	46.1	47	47.4	31.2	38.3	40.4	
	— with BCH coding	12.5	19.1	25.2	30.6	-	15.9	23.6	37.8	42.1	44	46.3	47.1	47.4	-	-	-	



### 4.6.5 Average runtime cost

Most of the processes comprising Algorithm 3-4 are of linear complexity, as can be inferred from their description throughout Sections 4.5.1-4.5.4. Table 4.15 shows the runtime cost of these processes when executed in a MATLAB<sup>®</sup> R2014a implementation running on an Intel Core i5 Quad Core at 2.9 GHz with OS X Yosemite. The slowest process is the tag BCH coding, taking 158 – 187 *ms*, which can be performed offline and is recommended for stable tags with length  $\leq 1024$  bits and for semistable tags with length  $\leq 4096$  bits, and the decoding, which needs to be performed online but takes only 15 – 24 *ms*. The segmentation and the color reduction of the image have a negligible cost, while the wavelet transformation is the second slowest process. Most of its runtime cost is concentrated on calculating the first 3-4 decomposition levels and is highly dependent on the size of the original image. When the size of the image is increased by two in both rows and columns, the runtime cost increases approximately by four. The coding of a keytag has linear complexity and low runtime costs, e.g. 0.1 *ms* for 128-bit tags and 7.1 *ms* for 8192-bit tags; and its decoding has a very low fixed cost of 0.3 *ms*. Regarding cryptographic processes, the digital signature of a keytag and its verification have a low fixed cost, 2.6 and 7.2 *ms*. The cost of encrypting a keytag depends linearly on the length of the tag and its runtime cost is very low, 0.2 *ms* for a 8192-bit tag. The costs of encrypting and decrypting a package of up to 16 access keys to keytags intended for a user are 0.45 and 5.3 *ms*.

According to the data in Table 4.15, the overall delays for associating several keytags (in this example 4 128-bit stable, 3 2048-bit semistable and 1 256-bit volatile) to an  $512 \times 512 px^2$  image (operations 1a-3a) and retrieving the corresponding tags (operations 1r, 4r-6r) are  $< 55 ms$  and  $< 115 ms$  respectively. If keytagging is integrated within the JPEG2000 compressor, these overall delays drop to  $\leq 30, 90 ms$  for any image size, since this compressor performs the wavelet transformation. Finally, when some tags are private, it is necessary to encrypt and decrypt (operations 4a and 3r) the keytags and the corresponding access keys (operations 5a and 2r) of each user. These operations add an extra delay of  $< 0.5 \cdot \#users ms$  in the keytag association and 5.5 *ms* in the tag retrieval procedure.

Table 4.15: Average runtime cost (in *ms*, unshaded cells) of the processes for keytag association and tag retrieval depending on different parameter values (shaded cells)

Operation:	Parameter(s)	Value 1	Value 2	Value 3	Value 4	Value 5	Value 6	Value 7	Value 8	Value 9	Value 10	Value 11
Keytag association process												
0a. BCH coding of a tag	$length(T)$	128	256	512	1024	2048	4096	-	-	-	-	-
		157.9	162.0	188.1	185.3	185.7	187.2					
1a. Segmentation, color reduction and wavelet transformation of $I_{or}$ ,	$WL$	1	2	3	4	5	6	7	8	9	10	11
	Image size											
Algorithm 3: lines 2-5	$512 \times 512 px^2$	19.9	21.4	23.9	25.3	25.4	25.4	25.6	25.6	25.7		
	$1024 \times 1024 px^2$	87.6	95.9	105.0	110.4	110.4	110.6	110.8	110.9	110.8	111.1	
	$2048 \times 2048 px^2$	359.7	421.7	455.2	479.0	479.3	478.1	478.4	478.5	478.4	478.7	478.7
2a. Coding of a keytag, Algorithm 3: lines 6-7, 9-12	$length(T)$	64	128	256	512	1024	2048	4096	8192	-	-	-
		0.1	0.1	0.2	0.5	0.9	1.9	3.6	7.1			
3a. Signature of a keytag, Algorithm 3: line 13							2.6					
4a. Encryption of a keytag, Algorithm 3: lines 14-15	$length(T)$	64	128	256	512	1024	2048	4096	8192	-	-	-
		0.1	0.1	0.1	0.1	0.1	0.1	0.2	0.2			
5a. Encryption of a user's access keys, Algorithm 3: lines 17-21							0.45					
Tag retrieval process												
1r. Segmentation, color reduction and wavelet transformation of $I_{or}$ ,	$WL$	1	2	3	4	5	6	7	8	9	10	11
	Image size											
Algorithm 4: lines 2-5	$512 \times 512 px^2$	19.9	21.4	23.9	25.3	25.4	25.4	25.6	25.6	25.7		
	$1024 \times 1024 px^2$	87.6	95.9	105.0	110.4	110.3	110.6	110.8	110.9	110.8	111.1	
	$2048 \times 2048 px^2$	359.7	421.7	455.2	479.0	479.3	478.1	478.4	478.5	478.4	478.7	478.7
2r. Decryption of a user's access keys, Algorithm 4: line 7							5.3					
3r. Decryption of a keytag, Algorithm 4: line 9	$length(T)$	64	128	256	512	1024	2048	4096	8192	-	-	-
		0.1	0.1	0.1	0.1	0.1	0.1	0.2	0.2			
4r. Verification of keytag signature, Algorithm 4: line 10							7.2					
5r. Decoding of a keytag, Algorithm 4, lines 6, 11-15							0.3					
6r. BCH decoding of a tag	$length(T)$	128	256	512	1024	2048	4096	-	-	-	-	-
		15.3	15.8	15.9	16.7	19	23.8					



### 4.6.6 Scalability

The scalability of any technique for protecting biomedical images is an important feature since the tendency is to increase their resolution for better image processing and visualization. The shaded cells in Tables 4.9-4.12 depict the robustness-capacity trade-off in a second image test set. This corresponds to the original data set introduced in Section 4.6.1 after bicubic interpolation by a factor of two in both rows and columns, which has been processed with the same modifications as the former but tuning the parameters so that the image distortion caused is closely similar in *PSNR* and *MSSIM*. Otherwise, if the parameter values for the image modifications are maintained and the images are enlarged, the distortion caused is usually lower (especially when the image undergoes compression and local operations) and the robustness-capacity tradeoff would improve only because the image is less degraded.

Two different parameter configurations have been tested, using the *aWL* in Algorithm 5: *extractFeatures* (the lightly shaded cells in Tables 4.9-4.12) and reusing the same *aWL* as for the original test set, comprised by  $512 \times 512 px^2$  images (the shaded cells in Tables 4.9-4.12). When associating stable keytags and performing image compression and common image modifications, it can be seen that both options obtain results similar to those for  $512 \times 512 px^2$  images up to tag lengths of 1024 bits. The second option gives better results, but these are still not good enough to allow capacities higher than 1024 bits. When associating stable keytags and performing local image operations, the first option obtains much better results than the second, since the tag is associated to lower frequencies of the image which better endure these types of image modifications. These results are very similar to those obtained with  $512 \times 512 px^2$  images. Regarding semistable keytags, the first option also obtains results that are closer to those obtained with  $512 \times 512 px^2$  images. The configuration for volatile keytags has been maintained by selecting coefficients from the *HH* subband in the first decomposition level, to guarantee very low robustness. Regarding the rest of the image modifications, the results are equal or very similar for both options. As a general conclusion, the parameters proposed in Algorithms 3-4 guarantee the scalability of keytagging with respect to the robustness-capacity trade-off, which is maintained for different image sizes.

Regarding the runtime cost of keytagging, increasing the size of the image increases the cost of performing its wavelet transformation (operations 1a and 4r in Table 4.15) by an  $n^2$  factor. For instance, calculating the *MWL* of a  $512 \times 512 px^2$  image takes 25.7 *ms*, while for a  $1024 \times 1024 px^2$  image it takes 111.1 *ms* and for a  $2048 \times 2048 px^2$  image it takes 478.7 *ms*. As a result, the overall delays for associating keytags and retrieving tags presented in Section 4.6.5 ( $\simeq 55, 115 ms$ ) increase to  $\simeq 140, 200 ms$  for  $1024 \times 1024 px^2$

images and to  $\simeq 510, 570 ms$  for  $2048 \times 2048 px^2$ . Therefore, it is recommended combining keytagging with JPEG2000 compression in order to guarantee the scalability of keytagging, since it reduces these delays to  $\simeq 30, 90 ms$  for any image size.

## 4.7 Protection of biomedical images by means of keytagging

The integration of keytagging to strengthen the protection of images transmitted within m-Health architectures is analyzed in Section 4.7.1. In addition to this, the operating parameters of keytagging are adjusted in order to implement the security measures proposed in Section 1.3.2. The use of specific keytags for image resynchronization, authentication and traceability, copyright protection, private captioning, integrity control and location of tampered areas is summarized in Table 4.16, and described in detail throughout Sections 4.7.2-4.7.7. Furthermore, the security of the keytagging method, including all the security measures that it can implement, is comprehensively assessed in Section 4.7.8. Finally, the potential limitations of keytagging are analyzed in Section 4.7.9.

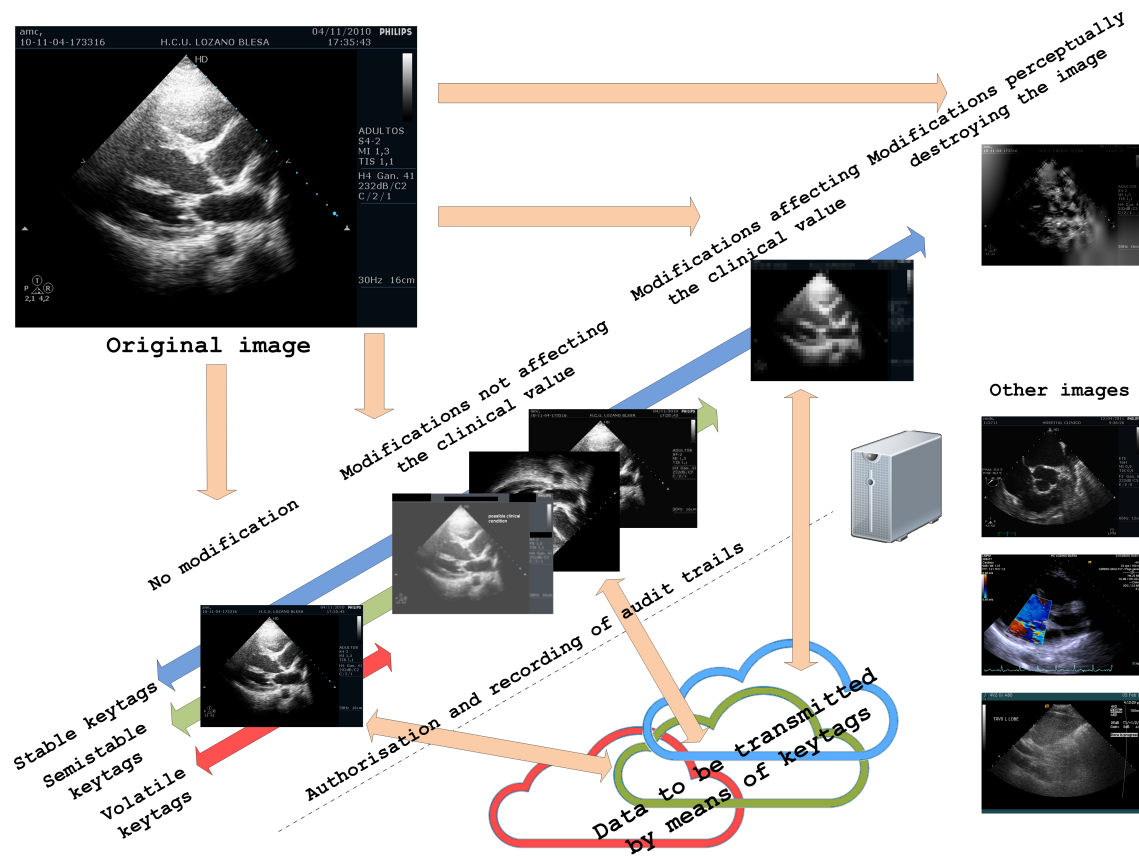


Figure 4.9: Integration of keytagging in m-Health architectures.

### 4.7.1 Integration of keytagging in m-Health architectures

The keytagging method is aimed for supplementing the security in the transmission of images within cooperative m-Health architectures, which at a technical level are typically supported by standards like DICOM (see Section 2.6.4). As portrayed in Figure 4.9, the integration of keytagging for the sharing of information among different users in these architectures poses three constraints:

- Although the keytagging algorithm guarantees that keytags are protected and verified (by means of cryptography, Section 4.5.4), the integration of keytagging in m-Health architectures requires the implementation of a reliable authorization mechanism to control which specific entities (e.g. the device that acquired the image the keytag is associated to, a physician in charge of supervising the image, the holder of the image copyright, etc.) are entitled to add, remove or consult keytags of an image.
- The m-Health architecture shall also implement a mechanism to record which keytags are added, removed or consulted, in order to guarantee the auditability of these events and the accountability of the entities involved.
- The capacity of the different types of keytags to transmit information among different users is conditioned by the perceptual and clinical distortion that their instances of the image —associated to the keytags— may undergo. This property is used for the implementation of the keytag-based security measures described throughout Sections 4.7.2-4.7.7.

### 4.7.2 Image resynchronization

The biomedical image may be subject to geometrical transformations, which in this context may be 90/180/270° rotation, vertical or horizontal flipping. Recovering the original image position is essential to retrieve its tags correctly, since otherwise they would be desynchronized. To accomplish this task, a reference synchronization tag is associated to the image. This is a 128-bit public stable tag, which is retrieved six times, from the received position and from each of the geometrical transformations (by rotating/mirroring each subband in *Coef* just after line 5 in Algorithm 4). The retrieved tag most similar to the original reference corresponds to the transformation that recovers the original image position. If it is observed that a retrieved tag is more dissimilar than the most similar tag, e.g. 127 wrong bits in the former and 80 correct bits in the latter, this means that the original position corresponds to the former, whose colors have been inverted. In that case, the values of *Coef* need to be inverted (just after line 5 in Algorithm 4).

Table 4.16: Recommended parameters to implement various keytag-based security measures (see Section 4.7)

Security measure	Keytag type	$aWL$ , allowed wavelet level(s)	Tag content	Tag length (bits)	Tag BCH coding	$Th$ , tag detection threshold (bits)	Keytag encryption	Issuer of DS keytag
Image resynchronization	Stable	$\geq MWL(ROI_g) - 6$	Reference	128	Yes	Most similar/ dissimilar tag	No	Image acquisition device or image issuer
Authentication and traceability	Stable	$\geq MWL(ROI_g) - 6$	Reference	128	Yes	126	No	Image acquisition device or image issuer, and each entity that processes the image
Pursuing illegal image copies	Stable	$\geq MWL(ROI_g) - 6$	ID of image copyright holder	128	Yes	126	No	Holder of image copyright
Image purchase	Stable	$\geq MWL(ROI_g) - 6$	ID of image buyer	128	Yes	126	Yes	Holder of image copyright
Private captioning with RBAC	Semistable	$\leq MWL(ROI_g) - 7$	Text/codes	$\geq 256$ $\leq 8192$	No	-	Yes (RBAC)	User authorized to update test data
Integrity control	Volatile	1 ( $HH$ subband)	Reference	64	No	-	No	Image acquisition device or image issuer
Location of tampered areas	Volatile	1 ( $HH$ subband)	Reference	$\geq 512$	No	-	No	Image acquisition device or image issuer

### 4.7.3 Image authentication and traceability

Authentication refers to the capacity to determine if an image is either derived from another, including perfect copies in this category, or if it is unrelated. To implement image authentication, a reference public stable tag is associated to the original image. It is then retrieved from the image to be authenticated. Only if the reference and retrieved tags are very similar or equal is the image positively authenticated. The authentication ability of keytagging is adjusted by means of two operating parameters: the length of the reference tag and the detection threshold,  $Th$ . Assuming that decoding each tag bit has a probability of success of  $\simeq 0.5$  when it is done from a wrong image, the probability of false positives  $P_{fp}$  in authentication can be approximated by means of the following binomial distribution:

$$P_{fp} = \sum_{i=Th}^{n=length(T)} (0.5)^n \cdot \frac{n!}{i!(n-i)!} \quad (4.8)$$

The image is positively authenticated only if the number of correctly decoded tag bits exceeds the threshold,  $\sum_{i=1}^{length(T)} (\tilde{T}_i = T_i) \geq Th$ . On the one hand, the probability of false positives  $P_{fp}$  in image authentication is expected to be similar to that required in applications of biometric recognition,  $\leq 10^{-6}$ . Thus, avoiding images that were not keytagged for authentication from obtaining false positives requires setting a high  $Th$ . On the other hand, too high values of  $Th$  (low permitted  $NHD$ ) will increase the probability of false negatives (non-authenticated images that were actually associated with the authentication tag). As can be seen in Tables 4.9-4.12, the robustness of stable tags with BCH coding is total ( $NHD = 0\%$ ) for tag lengths up to 512 bits, which ensures no false negatives. However, a shorter tag is enough to ensure that the likelihood of false positives,  $P_{fp}$ , is very low. Using  $length(T) = 128$  and  $Th = 126$  ( $NHD = 1.6\%$ ) makes  $P_{fp} = 2.5 \cdot 10^{-35}$ . The minimum  $NHD$  in simulation setup 2 (see Section 4.6.1) was obtained when associating-retrieving a reference 128-bit tag using the two most similar images in the test set ( $PSNR = 23dB$ ), two close slices from a PET-CT. That  $NHD$  value, the closest to causing a false positive, was 17.2%, still far greater than  $Th$  ( $= 1.6\%$ ). To sum up, these operating parameters ensure the perfect authentication of the whole test set.

Traceability policies intend to facilitate the tracking of entities that process or simply forward the biomedical image test. This can be easily accomplished if each entity validates the digital signature(s) of the authentication keytag, authenticates the image and adds its own digital signature to the authentication keytag if the previous verifications are positive. Otherwise, the image is reported as replaced or heavily tampered with and requested from the last entity that validated it.

#### 4.7.4 Copyright protection

Copyright protection may be implemented by means of a specific double authentication mechanism (see Section 4.7.3), involving the image copyright holder and each image buyer, in the following manner:

- The copyright holder is identified by means of a public ID (e.g. Rubio@eHealthZ14), which he/she associates to the image by means of a 128-bit stable tag. Besides, this tag has a secondary purpose: enabling the automatic search for illegal copies of the image in internet sites and databases. An internet bot may use the keytag to retrieve tags from the images in targeted sites and compare them with the copyright holder ID. If some image is positively authenticated, it is an illegal copy.
- Each buyer is identified by means of an ID, which the copyright holder associates to the image with a 128-bit private stable tag. In this manner, any buyer can prove that he/she holds a legal copy, even if he/she has made substantial modifications to it.

#### 4.7.5 Private captioning with RBAC

The association of private information with the image, only retrievable by authorized users if the image preserves its clinical value, may be easily carried out by means of semistable private tags. Nonetheless, the results in Tables 4.9-4.12 suggest that the overall size of these captions should not exceed 8192 bits. Therefore, it is recommended compressing them as much as possible, e.g. by replacing text with codes. Nevertheless, it is also recommended that the overall tag length is not too short, to guarantee a good specificity. As pointed out in Table 4.13, a minimum length of 256-bit ensures that the minimum distortion ( $NHD$ ) of tags retrieved from very similar images (but not derived from the original) is high,  $> 23\%$ . Therefore, short tags shall add padding bits until their length is  $\geq 256$  bits.

Cryptographic-based RBAC may be applied to improve private captioning (see Algorithms 3: lines 14-21 and Algorithm 2: lines 7-9). For each tag, its associated keytag is symmetrically encrypted with a specific symmetric key,  $Sk$ , and all the symmetric keys corresponding to tags intended for a user are encrypted with his/her public key,  $PbUser\{i\}$ . Thus, each user decrypts his/her symmetric keys  $\{Sk\}$  with his/her private key,  $PrUser\{i\}$ , and then decrypts his/her keytags with these symmetric keys. All this can be easily managed by encapsulating the keytags with CMS. There are two reasons to implement RBAC in this manner, instead of by associating a different keytag for each user. First, because all the users retrieve the same tag content, even when the image is

modified. Otherwise the users may retrieve tag contents with different degrees of distortion. Second, because associating several keytags with the same content would reduce the overall capacity.

#### 4.7.6 Integrity control and location of tampered areas

The detection and location of modifications affecting the image may be efficiently performed by means of public volatile tags. Tables 4.9-4.12 shows that these tags suffer high distortion even when the image modifications are mild, which implies very low robustness. Given these results, the following configurations are proposed:

- For integrity control, it is sufficient to use 64-bit reference tags, since they have an average  $NHD \simeq 50\%$ . Thus, approximately 32 bits are wrongly detected when the image  $ROI$  undergoes non-geometrical modifications (geometrical modifications are reversed by means of resynchronization, see Section 4.7.2). The exception to this,  $NHD$  slightly  $> 0$ , occurs when the image is partially annotated in the  $ROI$ , since only a few pixels in isolated regions change.
- For the location of tampered areas, the position in  $BM$  of wrongly detected tag bits is marked in the corresponding positions of the image. The even distribution of tampered pixels, detected after a common image modification, is shown in Figure 4.10: center. Logically, longer reference tags are able to achieve finer granularity in the delimitation of modified image areas, which is especially important in the case of detecting annotations in the image  $ROI$ . Considering that usually only  $\simeq 2\%$  pixels have been annotated and half (1%) change the value of the features used for coding of these keytags (the  $LSB$  of certain wavelet coefficients), a 512-bit tag is able to locate approximately 5 tampered areas in the  $ROI$ , as shown in Figure 4.10: right.

It is worth noting that implementing location of tampered areas already ensures integrity control, but not conversely.

#### 4.7.7 Simultaneous implementation

This section analyzes whether all the previous security measures can be implemented simultaneously in the images from the test set, by analyzing the results of robustness-capacity in Tables 4.9-4.12 and the keytagging parameters in Table 4.16. According to these results, the security measures based on public stable tags can reach an overall capacity of 512 bits with  $NHD = 0$ , and they only require 384 bits. Regarding semistable tags, their capacity shall be adjusted to  $\leq 8192$  bits in order to maintain an adequate robustness in

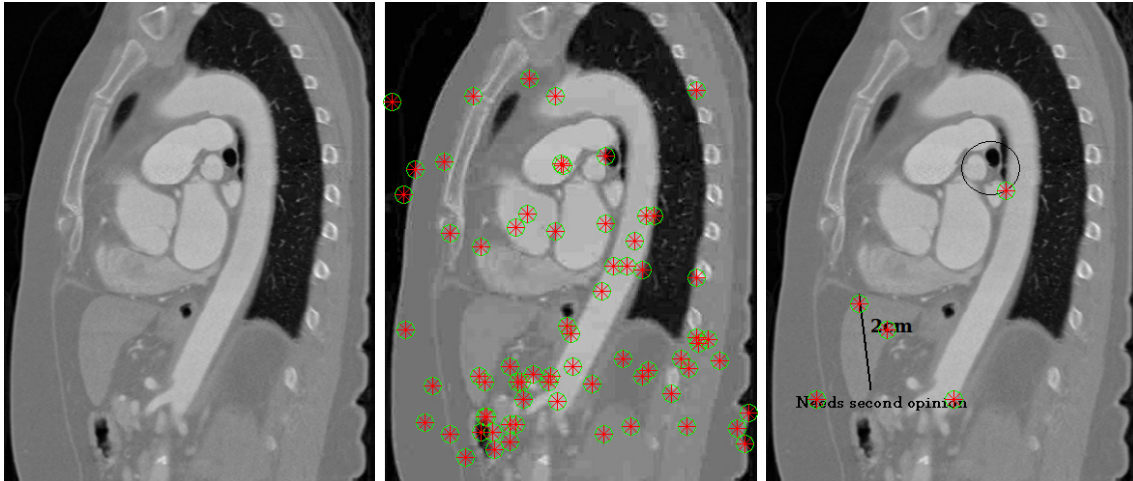


Figure 4.10: Location of tampered areas on the *ROI* of a  $512 \times 512 \text{ px}^2$  original image (left), on its JPEG  $QF = 15\%$  compressed version (center, tag length = 128 bits) and on an annotated version (right, tag length = 512 bits).

private captioning. With respect to volatile tags, there are no capacity restrictions. Thus, all these security measures can be implemented simultaneously. Furthermore, in this case, it is recommended that the tags for image resynchronization, authentication-traceability and location of tampered areas-integrity control associate the same reference. This would require extending the reference used for location of tampered areas, e.g. by repeating several times the shorter reference used to implement the other security measures. In this manner, the reference does not need to be transmitted since comparisons may be established among the tags retrieved. Consequently, the keytagging-based security system would be able to operate in a blind manner.

An overview of the overall keytagging system is introduced below by means of the following use case. A patient's biomedical image is acquired by means of a CT scanner, whose software generates a 128-bit reference and runs the keytagging algorithm to associate it by means of three keytags. Two of these keytags are stable, intended for resynchronization and authentication, and the third is volatile (resulting from the concatenation of the reference 8 times), intended for the location of tampered areas. The keytags are attached with the image file and recorded in the audit trail system of the m-Health architecture to which the CT scan is connected. The access control system of the architecture establishes that this image can be edited by two specialists of the patient and consulted by his general practitioner. Each time that one of them accesses the image, the visualization software runs the keytagging algorithm to validate the keytags associated and read their content. Next, the reference introduced after the acquisition is used to authenticate and resynchronize the image (if necessary), and also to pinpoint tampered areas (if any). The specialists can introduce text regarding the diagnosis of the patient or his/her treatment,



which the visualization software will associate by running the keytagging algorithm to add semistable keytags. These keytags will be attached in the image file and recorded in the audit trail system. The three users can consult the image, perform modifications on it and, using the visualization software, consult the keytags. In spite of possible modifications, the visualization software will still be able to authenticate and resynchronize the image, to display the content of the semistable keytags (if the image has not lost its clinical value) and to pinpoint the modified areas. Finally, the specialists (but not the practitioner) can use the visualization software to order the removal of their own semistable keytags from the image file, being this event recorded in the audit trail system.

#### 4.7.8 Risk assessment

The keytagging method, described in Section 4.5, involves different elements; namely, the keytagging algorithm itself, the keytagged image, the keytag(s) associated to it and the content of the corresponding tag(s). Several considerations can be done about the character, either public or private, of these elements. In the first place, Kerckhoff's principle states that the system shall be secure even if everything about it, except certain keys, is public knowledge. Hence, considering that the enemy will eventually discover the keytagging algorithm [392], it is proposed in Section 4.5.4 to make it public from the beginning. Similarly, medical keytagged images cannot be considered as impossible to obtain under any circumstance. In fact, certain situations may facilitate attackers to obtain an image copy. Some patients may give their informed consent to the use of their biomedical images for certain purposes —e.g. teaching, research— after anonymization, which increases the number of accesses to the image (and the number of potential opportunities for attacker accordingly); and even strictly confidential images may be a reasonably target for attackers if at a certain time they are handled (e.g. filtered, annotated) out of a protected standardized format (e.g. as JPX instead of DICOM files). Regarding keytags and their associated tag contents, they can be either public or private depending on the security measures that they implement (see Table 4.16). The former are available to anyone for consultation, while the latter are considered as the most difficult elements to be obtained (in clear) by an attacker.

With the purpose of weakening the security of the system, an attacker with access to some of its elements may try to perform certain attack(s) to interfere with the security measures described throughout Sections 4.7.2-4.7.6. Therefore, performing a comprehensive risk assessment, comprising all feasible attacks and the existing countermeasures, is essential for the prevention of potential security breaches. The following risk assessment, based on reference publications on watermarking security [393, 394, 395] and tailored to the specifics of keytagging, analyzes attacks depending on the keytag-based measures af-

fect, the actions intended by the attacker and the system elements he/she needs access to. The following attacks may potentially affect the privacy in image purchase and in image captioning (see Sections 4.7.4-4.7.5):

- Unauthorized detection and reading of private keytags. It is impossible to detect keytags if the attacker only knows the image: no information can be extracted from the image alone since keytagging does not modify it in any manner. As regards to reading the whole content of private tag(s) associated to an image, the algorithm requires both the image and the plain keytag(s) associated. With respect to the former, the attacker may try to use another image if he/she does not have the original, but the specificity of keytags guarantees that the content retrieved will be highly distorted, as demonstrated in Section 4.6.3. Regarding the latter, keytag(s) is/are protected with adequate encryption (see Section 4.5.4), which makes obtaining its/their plain version(s) very unlikely. There is also another possible attack, which—generally speaking—requires even more knowledge about the system and only permits reading part of certain tag(s) content. To explain this attack, it is worth reminding that while public keytags shall be associated to different features of the image to avoid eavesdropping, different independent users may associate private keytags to certain repeated image features. Therefore, if an attacker knows one or several plain private keytags with its/their associated tags, he/she would be able to read those tag bits from other keytags associated to the same image features. Nevertheless, this requires the attacker being able to break the encryption of the keytags from different users (to obtain the plain versions) and to know the tag content of at least a private keytag, which is highly unlikely.

And these attacks may potentially affect all the security measures described throughout Sections 4.7.2-4.7.6:

- Writing of forged keytags. The attempt to copy a legitimate keytag in another image will not succeed since the keytagging algorithm guarantees that keytags are dependent on the image. This high specificity guarantees that the tag content read will be highly distorted, as proved in Section 4.6.3. Alternatively, any attacker can decide to associate his/her own keytag(s) to any image, since the keytagging algorithm is intended to become public. Nevertheless, the attacker cannot add the required digital signature of a trusted entity to the keytags, unless he/she has broken or stolen the private key of a trusted entity—which is highly unlikely.
- Malicious removal of legitimate keytags. There are three possibilities: attacking the keytag, the image it is associated to or the association. As regards to keytags, although they may be attacked, its integrity and provenance can be evaluated any

time by means of its digital signature, which is a mandatory element (see Table 4.16). As explained before, to forge the digital signature of the signatory entity, so that the attack cannot be detected, the attacker needs to break/steal his/her private key. Regarding attacks on the image, their effects on the robustness of the different types of keytags have been evaluated in Section 4.6.2. In fact, the different measures described throughout Section 4.7.2-4.7.6 are designed based on the intended robustness of keytags —e.g. authentication is based on stable keytags, which can be detected even when the image undergoes important modifications; tamper detection is based on volatile keytags, which get highly distorted even if the modification(s) on the image are minor. Therefore, the effect of the modifications of the image have already been taken into account in the design of the security measures. Alternatively, the keytagging algorithm can be exploited to change the value of image features used to encode the keytags. In point of fact, this attack can destroy the tag content when the plain keytag is known (e.g. if it is public), but at the cost of destroying the image as well (see Section 4.6.2). Regarding collusion attacks (popular in watermarking), which combine different keytagged versions of an image to produce another image with distorted keytags, they would be pointless since any keytagged version of an image is exactly like the original. Finally, the attacker may attempt to make the tag reader think that certain keytags are associated to a different image, with the intention of confusing him/her. To detect this attack, it has been proposed associating a reference tag with two independent stable keytags (one for image resynchronization and another for image authentication and traceability, see Section 4.7.7). In this manner, the tag content of these keytags only match when retrieved from the original image (or from an image derived from it, e.g. compressed or filtered).

- Malicious edition of legitimate keytags. This is a combination of the previous types of attack. Therefore, it requires knowing the plain keytag (breaking its encryption if it is private), editing the content of the keytag total or partially (as intended by the attacker), replacing the previous signature with a new valid one (which requires the private key of the original keytag signatory) and, if the keytag is private, re-encrypting the keytag with the same cryptographic key used for its decryption.

The careful design of the keytagging algorithm, its combination with adequate cryptographic elements and the choice of the parameters to enforce the different security measures (mainly the robustness of the keytags) are the foundations of the keytagging method. From this security assessment, it can be concluded that the only manner to weaken the security of this system is by attacking the cryptographic protection of the keytags. Hence, the security of keytagging cannot be considered as lower than the security of cryptography.

On the contrary, the former requires an additional element for the retrieval of the content associated: the image.

#### 4.7.9 Potential limitations

With respect to the algorithm, the main limitation for its integration in m-Health applications is the length of the keytags, which ranges from  $\approx 4 \cdot \text{length}(\text{tag})$  to  $7 \cdot \text{length}(\text{tag})$ , depending on the size of the image and on the type of keytag. In addition, the results of robustness-capacity presented are the average of the image test set; however, it was observed that images with higher energy obtained better results. Thus, defining an index relating the energy of the image with its robustness-capacity for different image modifications would be helpful for fine-tuning the capacity of the keytags and also to decide which image(s) shall be chosen for keytagging in short video modalities composed of a series of images. It is also worth noting that this technique is complemented by cryptography, and thus the validity of the encryption and signature algorithms involved shall be permanently revised.

As regards to the applications of keytagging, the main limitation of this technique is that it can not mark each individual signal in a different manner — what fingerprinting does — since this technique does not modify the images. Nonetheless, this would be of interest to locate the source in leakages of tests. To bypass this issue partially, in cases of leakages keytagging can be used to locate copies of leaked tests and demand and verify the proofs of ownership provided by the parties involved.

## 4.8 Conclusions

The main objective of this Chapter was to define novel, cost-efficient, signal-based methods for the protection of biomedical tests. This objective has been divided into two: the development of an embedding-based coding for biomedical tests and of a technique, called keytagging, for the association of information to biomedical signals (particularized for images). The main conclusions relating to these specific objectives are listed below:

- The proposed coding for 1D biomedical signals meets all the requirements proposed in Section 1.2.2: information associated to the biomedical signal, signal compression, security and privacy, role-based access control and low complexity encoding and short access time. The information of the test is embedded within the coded biomedical signal, resulting in one or several *Coded Test Unit(s)* (*CTUs*). Within a *CTU*, the information is so tightly associated to the signal that the whole *CTU* is used to reconstruct the signal in the time domain. The compression ratio achieved by

the coding is quite high, typically ranging from  $\simeq 3$  in real-time transmission to  $\simeq 5$  in offline operation for ECG and EEG-based tests, despite of the preservation of the clinical value of the signal and of the embedding of additional, protected metadata. From another angle, this coding permits embedding large amounts of additional information within the signal (e.g.  $\simeq 3$  KB in resting ECGs,  $\simeq 200$  KB in stress tests,  $\simeq 30$  MB in ambulatory ECGs,  $\simeq 350$  KB in epilepsy detection tests,  $\simeq 4.7$  MB in polysomnographic studies) without exceeding the size of the original, uncompressed signal alone. In addition, the risk assessment demonstrates that this coding provides appropriate levels of security and privacy, by combining the robustness of encryption — partial for the signal and symmetric-asymmetric for the metadata — and the secrecy contributed by steganography. Furthermore, a role-based access control policy, enabled by means of a efficient syntax, regulates the privacy of the contents stored in *CTU*(s) and permits the simultaneous implementation of various secure m-Health applications (e.g. emergency care/surgery, diagnosis, research, teaching, etc.). Finally, the coding/decoding system uses simple operations, which allows real-time operation (with overall delays of  $\simeq 2 - 3.3$  s), and it can be easily handled by systems and users through an intuitive interface that is provided.

- Keytagging, the method proposed to associate information to biomedical signals (specified for images) has demonstrated that its features makes it a better candidate for this task than previous proposals in the state of the art, based on watermarking (Section 1.3.2), for a number of reasons. First and foremost, its comprehensive risk assessment, which takes into consideration all the elements of the keytagging algorithm and the possible attacks, has demonstrated that the level of security of this technique is appropriate and better than cryptography alone. Furthermore, there is a proposal which details the keytagging parameters that enable the — individual or simultaneous— implementation of a variety of security applications, including private captioning with role-based access control, integrity control and location of tampered areas, authentication, traceability and copyright protection of the image. Second, keytagging does not modify the image since — unlike in non-zero watermarking techniques — keytags are encoded as a function of certain image features and the data to be associated, so the image clinical value is not affected during or after this process. Third, unlike in zero-watermarking techniques, the coding method is optimized towards the selection of the most robust image features — not just very robust image features —, in order to maximize the robustness-capacity tradeoff. The experimental evaluation, carried out with  $512 \times 512$  and  $1024 \times 1024$  pixel images, shows that the robustness of stable tags to modifications that are typical in the biomedical context is perfect ( $NHD = 0$ ) up to 512 bits and still very high (only three modifications produce  $NHD > 0$ ) for 1024 bits. Semistable tags obtain good

robustness to JPEG2000 CR 16:1 image compression and contrast and brightness change ( $NHD = 0\%$  for tag length of 4096 bits), and bad, as intended, to local operations that distort the details of the image (average  $NHD > 15\%$  for tag length  $\geq 512$  bits). Volatile tags achieve very little robustness to any modification of the image, even when associating very short tags ( $NHD > 45\%$  for length  $\geq 64$  bits). Fourth, the operations involved in the algorithm for the selection of image features are simple, and as a result, the runtime costs are low: associating a set of keytags and retrieving the corresponding tags for the simultaneous implementation of the aforementioned security measures takes only  $\simeq 55, 115 ms$  for  $512 \times 512 px^2$  images;  $\simeq 140, 200 ms$  for  $1024 \times 1024 px^2$  images and  $\simeq 510, 570$  for  $2048 \times 2048 px^2$  images. In addition, the scalability of keytagging has been evidenced when this method is combined with JPEG2000 compression, since its robustness-capacity tradeoff is maintained while the keytag association-tag retrieval delays are reduced to only  $\simeq 30, 90 ms$  for any image size.

To sum up, both techniques help to build different parts of a secure and cost-efficient m-Health architecture. In the case of the biomedical test coding, most of its features (high signal compression with clinical quality, real-time operation, embedding within the signal, security with reduced overhead) are not currently supported by well-established signal standards (e.g. DICOM waveform 30, SCP-ECG), which makes it a promising option for the BAN/PAN part of the m-Health architecture, which is highly constrained in costs. With respect to keytagging, it has been explained how this method can be seamlessly integrated within DICOM to facilitate the deployment of efficient cooperation among different authorized users, so that they can update DICOM files with new information and share it without sacrificing any security measure. Therefore, this technique may be integrated in the traditional PACS of the architecture, but also in the PAN/BAN for applications such as tele dermatology.

*“There is no real ending.  
It’s just the place where you stop the story.”*

Frank Herbert

*“Our virtues and our failings are inseparable, like force and  
matter. When they separate, man is no more.”*

Nikola Tesla

# 5

## Conclusions

This last Chapter lays out the conclusions of the Thesis and future work derived. The research objectives presented in Chapter 1 have been discussed throughout the Thesis. The most challenging key factors in the design of a secure and cost-efficient m-Health architecture have been addressed. These include proposing an overall design enabling m-Health services with different security and interoperability requirements, the enhancement of standard protocols for the exchange of biomedical information and the development of novel methods for the protection of biomedical tests. This Chapter is organized as follows. Section 5.1 specifies how the objectives of the Thesis have been achieved chapter by chapter. Section 5.2 enumerates and details the contributions of this work and the results accomplished. Finally, future work is described in Section 5.3.

### **5.1 Research objectives achieved**

Chapter 1 describes the m-Health scenario, the benefits that it can provide to the stakeholders involved in the healthcare system and its main issues, emphasizing those related with security. Section 1.2 describes the core components of the m-Health architecture and Section 1.3 presents an overview of current security trends in m-Health, their challenges and some clues about what can be improved. The objectives of this Thesis are established

in Section 1.4; being the main aim to investigate and develop a secure and cost-efficient architecture enabling an enhanced exchange of biomedical information in m-Health scenarios — focusing on biomedical tests. All the detailed objectives listed in Chapter 1 are addressed throughout the remaining chapters.

- Reviews on the state of the art in general aspects regarding security in m-Health: major biomedical standards, biomedical signal coding methods, transport technologies and legal regulations have been carried out in Chapter 2. This has led to a thorough risk assessment of the m-Health architecture and the raising of the guidelines for strengthening its security.
- The enhancement of the security of major biomedical standard protocols (ISO/IEEE 11073 PHD and SCP-ECG) according to the previous guidelines, which maximize their interoperability and cost-efficiency, has been addressed in Chapter 3.
- The design and evaluation of novel biomedical test protection methods based on their associated signals (embedding and keytagging), which enable advanced security features for strengthening the m-Health architecture with reduced costs, is addressed in Chapter 4.

The detailed conclusions and objectives achieved in each chapter are depicted in Sections 3.6 and 4.8.

## 5.2 Contributions and accomplished results

The bold contribution of this Thesis is the proposal of a strengthened m-Health architecture along with the tools to implement it in an efficient and inexpensive manner. The work involved in reaching this wide objective results in the achievement of the detail objectives established in Section 1.4. They are presented below, subdivided into the main topics of this research. First of all, as regards to the **contributions on the design of a secure and cost-efficient m-Health architecture**:

1. *Preparation of a detailed risk assessment of the m-Health architecture* (Section 2.5). This identifies the entities that may participate in the acquisition, transmission and storage of biomedical information of users (e.g. PHDs, CDs, alert systems, PACS) and the different threats that may cause loss, corruption or theft of this information, endangering the health and the privacy of the users. The attacks associated to these threats, e.g. devices hacking, replay attacks, user impersonation, man-in-the-middle attack, etc., and its likelihood of success depending on different parameters (e.g. length of a certain key, frequency of renewal) are determined.



2. *Analysis of common demands of major legal regulations regarding the m-Health context* (Section 2.4). The health IT directives of regulations such as the HIPAA and the GDPR are summarized in those requirements regarding the addressing of information security (confidentiality, integrity, availability, accountability, auditability, authenticity, non-repudiation and privacy) in order to minimize the risks associated to m-Health architecture and framework.
3. *Proposal of a well-depicted, cost-efficient, global security proposal for the m-Health architecture* (Section 2.6.1). This defines a layered interoperability model for m-Health applications demanding different requirements of security and integration with medical systems. For instance, the processing of simple real-time measurements (e.g. for daily blood pressure visualization) in a concentrator device requires only low security and no further integration, while the reliable interpretation of biomedical measurements and signals acquired at home — with personal health devices — in medical systems (e.g. clinical decision support systems) for clinical disease management requires high security and integration capabilities. This model takes into account the economical dimension and defines real use cases where some costs are saved, e.g. it is not essential to demand a user authenticator (e.g. based on bar codes or RFID tokens) in personal health devices that are not to be shared by different users.
4. *Translation of the previous global security proposal into specific security and integration measures* (Sections 2.6.2, 2.6.3 and 2.6.5). A careful analysis of the most suitable IHE profiles (e.g. ATNA, CT, DEC, ACM, WCM, XDS, etc.) to implement the security and integration measures demanded by each of the layers. Since IHE is not particularly aimed for Personal Area Networks, a new IHE profile needed — named SDO — to be defined to cover reliable communications between personal health devices and concentrator devices. The features of this profile (cryptographic algorithms, crypto periods, key lengths, etc.), their relations with the security layers and with already-existing IHE profiles (e.g. as a supplement of DEC, ACM or WCM) are specified.
5. *Security assessment of the m-Health architecture after its enhancement* (Sections 3.2.1, 3.4.1, 4.4.1 and 4.7.8). This includes comprehensive evaluations of how the new features included in 4) and integrated/materialized in 6, 9, 13 and 16) are effective on the prevention of the threats affecting the m-Health architecture, exposed in 1), depending on the security layer 3) implemented. This evaluations help to picture how security (and costs) grows with each layer.

Second, concerning **standardized protocols**:

6. *Design of a cost-efficient security extension for ISO/IEEE 11073 PHD* (Section 3.1). This relies on the adaptation of the layered proposal in 4) to its models of data information, service and communication — where the bottom layer corresponds precisely to the current version of the standard.
7. *Appraisal and discussion of the implications and impact of the former extension* (Sections 3.2.2, 3.2.3 and 3.2.4). This evaluates the number of attributes added to the data information model and the number of new states and frames added to the Finite States Machine that represents the service and communication models depending on the layer implemented. It also measures the extra delays and overhead produced by the implementation of each layer in representative cases, such as the transmission of a discrete measurement, a continuous signal or a block with the maximum size allowed by the standard. Finally, it calculates the minimum hardware that guarantees real-time transmission of a 3-lead electrocardiogram implementing the top layer of the enhanced version of ISO/IEEE 11073 PHD and reasons about the limitations of this extension.
8. *Analysis of the implications of the ISO/IEEE 11073 PHD extension for IHE* (Section 2.6.5). The seamless IHE-based extension of ISO/IEEE 11073 PHD suggests mild modifications or the extension of certain IHE profiles, such as the addition of new alarms to ACM.
9. *Design of a robust and simple security extension for SCP-ECG* (Section 3.3). This extension coordinates with that in 6) for the secure exchange of ECG data and proposes an enhanced file format, based on the features of the new IHE profile proposed in 4) and adapted to the scope and structure of SCP-ECG.
10. *Implementation of the former extension and evaluation* (Sections 3.4 and 3.5). This analyzes the impact of the extension on the SCP-ECG file format, presents a proof-of-concept that carries out the security enhancement of regular SCP-ECG files and the secure access to their contents, and also measures the overhead of the protected SCP-ECG files (in absolute value and comparing with the size of representative SCP-ECG files) and the delays in the processes of protection and access.
11. *Definition of appropriate means to allow the integration of novel biomedical signal protection methods in DICOM* (Section 2.6.4). Specifically, a method for the protection of biomedical signals that may embed periodic measurements, contextual information and/or security elements and a method for the protection of biomedical images by means of keytagging.

Third, as regards **to techniques for the protection of biomedical tests**:

12. *Reviews on the state of the art about methods that permit embedding large amounts of hidden data on signals* (Sections 1.3.2 and 2.2.4). This includes an overview of the main features of these techniques, examples of contents that may be embedded within signals, a thorough classification of embedding alternatives and an analysis of the main drawbacks of these techniques in the m-Health context.
13. *Design of an optimal coding for biomedical signals, periodic measurements and contextual information that facilitates the development of secure and efficient m-Health services* (Sections 1.2.2 and 4.1). This coding guarantees high signal compression — to preserve its clinical value — while reducing bandwidth and storage requirements; tight and secure embedding of measurements and of any other data of interest within the coded signals; role-based access control on the embedded data to enhance its privacy and also efficient, partial signal encryption.
14. *Development, optimization and evaluation of the former coding* (Section 4.2). The evaluation and parameters adjustment is twofold: from the user viewpoint, which demands preserving the clinical quality of the signal, adequate availability of the data and ease of use of the implementation; and from the technical viewpoint, which requires low bandwidth requirements, low overhead of the security elements and enough embedding capacity to include data produced in m-Health services. Two real scenarios are considered: ECG-based tests and EEG-based tests.
15. *Reviews on the state of the art about Medical Image Watermarking methods* (Sections 1.3.2 and 2.2.4). This includes an overview of the main features and constraints of these techniques, of security measures that may be implemented based on watermarking, a comprehensive classification of watermarking alternatives and watermark types, and a discussion about the main advantages and disadvantages of these techniques in the m-Health context.
16. *Design of a novel technique for the protection of biomedical images in m-Health architectures* (Section 4.5). This technique follows a new research direction derived from non-zero watermarking. Its design guarantees the clinical quality of the biomedical image without the need for assessment, high security against eavesdropping and manipulation, robustness against attacks which are typical in medical imaging and efficiency in the association of information to the image and in its access. Moreover, this novel technique can alleviate the cumbersome process for sharing biomedical information associated to the images with security.
17. *Proposal of optimal parameter configurations to associate information in a robust, semifragile and fragile manner and evaluate the robustness, specificity and scalability*

of this technique (Section 4.6). The image test set includes images from different acquisition modalities, computed tomographies, magnetic resonances, positron emission tomographies and ultrasounds. The robustness and the specificity are measured by means of the *PRD*. Furthermore, two aspects of the scalability of this algorithm are also tested, the complexity of its main routines (how the delays grow) and how the capacity (to host information) may vary when increasing the size of the image to be keytagged.

18. *Proposal of security keytagging-based applications* (Section 4.7). Optimal configurations (type of keytag, length, content, detection thresholds, etc.) to implement detection and location of tampered areas in images, private captioning with role-based access control, image authentication and traceability control, copyright protection and image resynchronization.

The most challenging issues have been addressed, and the results obtained indicate the validity, comprehensiveness and cost-efficiency of the solutions reached.

- The simple model proposed for enhancing the security and interoperability of m-Health architectures consists of three layers directly related with the m-Health domains — health and fitness, independent living and clinical disease management, which in turn are subdivided into two sublayers to address economic constraints — e.g. avoid the use of user authenticators in PHDs that are not shared by several users. The newly proposed IHE Secure Device Observation profile facilitates reliable and secure communications from the PCD to the concentrating gateway in implementations of the DEC, ACM and WCM profiles and also improves interoperability with the extended ISO/IEEE 11073 PHD and SCP-ECG.
- The layered, IHE-based extension of ISO/IEEE 11073 PHD introduces a series of countermeasures that put barriers to the threats (user impersonation, data theft, injection of commands, replay attacks) detected in the risk assessment of the hot spots of the traditional m-Health architecture. Furthermore, this extension can be considered cost-efficient. It adds no attributes to t DIM; four new frames have been added to the service model, and another four have been extended with new sub-frames (most of them common to all layers); and only one new sub-state, ‘Authenticating’, has been added in the communication model. As regards to the hardware requirements of the enhanced X73PHD architecture, a personal health device with a simple 9 MHz processor (assuming a throughput of 1 MIPS/MHz) can implement the top layer and transmit a 3-lead ECG in real-time to a concentrator device with a one-core processor at 1 GHz (also assuming the same throughput). With respect to its surrounding framework, the personal health device and the concentrator device

demand an initial configuration (carried out by the administrator), tokens for identification/authentication of users are needed when they share devices, and several IHE profiles need to be implemented by the concentrator device to enable its integration with healthcare systems (PHRs, EHRs, alert managers and CDSS). In summary, it can be considered that all the defining features of X73PHD have been maintained and enhanced with low or moderate costs.

- The security extension of the SCP-ECG file format has been devised to minimize the threats of unauthorized reading of confidential file contents, generation of (trustworthy) forged files and malicious removal or edition of legitimate files. The new security-enhanced format adds a new section (Section 12) with selected security elements and syntax in order to store the rest of file contents safely and proper access to be granted (or denied) to users for different purposes: interpretation of the test, consultation, clinical research or teaching. The access privileges are scaled by means of role-based profiles supported by cryptographic elements (encryption, digital certificates and signatures). The overhead introduced in the protected SCP-ECG is typically 2 – 13% with respect to the size of a regular file, and there is a 2 – 10% of extra delay to protect a newly generated SCP-ECG file and a  $\leq 5$  % extra delay to access it for interpretation. Regarding the users of the standard, they can maintain their regular SCP-ECG devices and software since an intuitive tool to protect SCP-ECG files and access the protected counterparts is provided. Taking all this into consideration, it can be said that a good level of security and availability is technically feasible with low or moderate costs.
- The proposed generic coding for biomedical signals, periodic measurements and contextual information has been conceived to minimize its most relevant threats: unauthorized detection and reading of confidential contents, generation of (trustworthy) forged coded tests and malicious removal or edition of legitimate coded tests. Furthermore, the access to the coded tests is regulated in such manner that they may be used for different, secure m-Health applications simultaneously, e.g. emergency care/surgery, diagnosis, research or examination, teaching, etc. As regards to performance, this new coding has been tuned and evaluated with resting, stress and ambulatory/Holter ECGs and with EEG-based tests for epilepsy detection and polysomnographic studies. The results obtained demonstrate the objective clinical quality of the coded tests, the ability of the coding-access system to operate in real-time (overall delays of 2 s for ECGs and 3.3 s for EEGs) and the its easy handling by PACS and users. Furthermore, this coding permits the embedding of large amounts of additional information within the signal (e.g.  $\simeq 3$  KB in resting ECGs,  $\simeq 200$  KB in stress tests,  $\simeq 30$  MB in ambulatory ECGs,  $\simeq 360$  KB in epilepsy

detection tests and  $\simeq 4.7$  MB in polysomnographic studies), detecting corruption of the signal or the information and implementing different access levels for a variety of professional roles. The compression ratios achieved by the coding are quite high, ranging from  $\simeq 3$  in real-time transmission to  $\simeq 5$  in offline operation, despite of the embedding of security elements and metadata to enable various secure m-Health applications.

- Keytagging has been assessed as a secure technique against its major threats: unauthorized detection and reading of private keytags — no tag bit associated to an image can be derived from the corresponding keytag(s) alone or by using an unrelated image —, writing of forget keytags and malicious removal or edition of legitimate keytags. On these robust basis, a variety of complementary keytagging-based security applications have been proposed, namely: detection and location of tampered areas in images, private captioning, image authentication and traceability control, copyright protection and image resynchronization. With respect to the cost-efficiency of this technique, the results obtained in terms of robustness-capacity and simplicity are remarkable. Tested with  $512 \times 512$  and  $1024 \times 1024$  pixel images, the robustness of stable tags to modifications that are typical in the medical context is total ( $NHD = 0$ ) up to 512 bits and still very high (only three modifications produce  $NHD > 0$ ) for 1024 bits. Semistable tags obtain good robustness to JPEG2000 CR 16:1 image compression and contrast and brightness change ( $NHD = 0\%$  for tag length of 4096 bits), and bad, as intended, to local operations that distort the details of the image (average  $NHD > 15\%$  for tag length  $\geq 512$  bits). Volatile tags achieve very little robustness to any modification of the image, even when associating very short tags ( $NHD > 45\%$  for length  $\geq 64$  bits). Regarding runtime costs, the simultaneous implementation of all the keytagging-based security applications consumes  $\simeq 55 + 115ms$  for  $512 \times 512px^2$  images;  $\simeq 140 + 200ms$  for  $1024 \times 1024px^2$  images and  $\simeq 510 + 570$  for  $2048 \times 2048px^2$  images. It has also been shown how this method can be combined with JPEG2000 compression, maintaining its robustness while reducing the keytag delays to only  $\simeq 30 + 90ms$  for any image size, which demonstrates the scalability of keytagging.

### 5.3 Future work

Although the objectives established in Section 1.4 have been fulfilled and very good results have been obtained, there is still room for improvement with well-oriented research. It is worth noting that some of these proposals may be considered at a pretty early research stage, while some others rely on evolving researches and standards. Thus, both additional,

exhaustive experimentation based on the configurations proposed in this Thesis and the translation or adaptation of external, novel advancements in related researches can foster relevant breakthroughs. Furthermore, certain security methods proposed may be considered as domain-agnostic tools which have been particularized to the specifics of certain biomedical tests, so they could be extended to other test modalities — existing or arising in the future — and also to other, totally different fields, such as military intelligence and secure distribution of commercial multimedia. The following list points out some interesting investigation directions that may be fruitful. First, as regards to the **security of the global m-Health architecture**:

- The periodic update and extension of the layer-based model to include new IHE profiles is requisite to maintain its validity and increase its reach. For instance, the inclusion of the Mobile access to Health Documents (MHD) and the Internet User Authorization (IUA) profile — although not essential — would result interesting for healthcare systems that prefer the simplified HTTP RESTful technology.
- A technical, detailed description of the proposed Secure Device Observation (SDO) profile would be relevant towards its hypothetical integration in IHE. It is worth noting that this profile is aimed at guaranteeing secure acquisition of biomedical information from users to host systems, involving personal health devices as intermediaries. This Thesis already includes an adaptation of SDO to ISO/IEEE 11073-20601 and SCP-ECG. However, it could also be adapted to other biomedical protocols used in Personal and Body Area Networks (e.g. simple protocols associated to open-source platforms, future m-IoT protocols) to enhance their security.
- The modeling and integration of social networks in the IHE guidelines, given that it has been reported in the literature that these tools have the potential to improve user engagement in m-Health services. Nonetheless, this work would research on which roles they could play, such as sources of biomedical information (like personal health devices), communicators of alerts and/or subscribed biomedical information, dedicated personal/electronic health records, etc. Therefore, they may act as entities but also as channels to carry out communication transactions.
- A serious proposal for the integration of m-IoT and social media in a secure and standard-based framework would probably be a milestone towards the construction of larger m-Health ecosystems. It may promote the manufacturing and selling of inexpensive, tiny, wearable and ready-to-use sensors (e.g. to measure body temperature, pulse rate, sweating); the direct and secure transmission of the acquired biomedical measurements and signals to the social media account(s) of the user — so that he/she is on control of his/her own personal data — by means of mobile

broadband technology (e.g. 3G, 4G); and the development of new smart m-Health services (e.g. running as Facebook apps, familiar to hundreds of millions of people) that analyze, store and/or share the biomedical information (or part of it) according to the user preferences. The use of biomedical standard-based means (at least their syntax) in this framework would allow that this data may also be integrated in traditional healthcare systems — e.g. electronic health record, clinical decision support systems.

- The definition of mechanisms for the integration of advanced, signal-based protection methods (e.g. keytagging) in the IHE guidelines, so that they can supplement existing security profiles — such as ATNA, which are entirely based on cryptography.

Second, concerning **standardized protocols** whose security has been enhanced:

- The evaluation of how the extensions of SCP-ECG and ISO/IEEE 11073 presented in this Thesis fit into the new m-IoT paradigm, to deploy frameworks where the personal health devices are internet-ready and the concentrator devices are cloud services. More specifically, it would be necessary to study which protocol(s) (e.g. CoAP [396], MQTT [397]) would best replace traditional transport (typically performed by means of USB, Bluetooth or Zigbee in traditional ISO/IEEE 11073 frameworks) and if some attributes, models or procedures of these standards would require modifications. Furthermore, given the limited energy availability of internet-ready personal health devices, the implementation of the extended standards in open-source platforms would help to assess their suitability for m-IoT.

Third, with respect to the **techniques for the protection of biomedical tests** which have been developed:

- The 1D embedding algorithm, which has been tested with ECGs and EEGs, could be extended to biomedical signals of higher dimension (e.g. 2D: MRIs, CTs, 3D: echocardiograms), since the coding relies on the widespread, generalizable and public SPIHT algorithm. This extension would only require changing to the adequate SPIHT modality (2D or 3D), adjusting empirically the optimal compression parameters and establishing the distortion threshold that permits maintaining the clinical quality of each new type of signal. Furthermore, it is worth noting that as SPIHT becomes more efficient when increasing the dimension (it achieves higher compression ratios for a similar signal quality), the embedding capacity will grow considerably.
- The embedding-based coding for biomedical tests provides a common access to the signal to all users — regardless even if they ignore the presence of embedded contents — since the whole *Coded Test Unit* is introduced into the SPIHT decoder. Although this is a noteworthy feature, still an attacker can remove bits from the end



of a *Coded Test Unit* (corresponding to embedded contents) and the signal would remain readable and preserving its clinical value — in any case this removal is always detected at the decoder. To strengthen, even more, the binding between the signal and the embedded content, this coding shall be enhanced to guarantee the automatic destruction of the clinical content of the signal when the embedded content (or part of it) is removed. Foundations of compressed sensing may be applied to achieve the embedding of metadata in critical parts of the Coded Test Unit with tolerable distortion.

- The embedding-based coding requires the protection of the content to be embedded into the signal. Robust cryptographic elements — encryption and digital signatures — have been proposed and successfully tested for this task. However, the protection may also be based on keytags, which would reinforce the association between the signal and the content — the keytagging procedure would precede the embedding.
- As regards to the keytagging algorithm, the main advance would be the development of an enhanced keytag coding method in order to reduce the overhead, which is the main drawback of this technique with respect to watermarking and cryptography. The second major improvement would be avoiding the need for BCH coding in stable and semistable tags and raising the capacity of semistable tags. To achieve this, it looks promising to research into the combined use of both most significant and sign bits of high magnitude coefficients as stable features, and also on the use of new transforms that may perform better than wavelets (e.g. wave atoms). In third place, it would be interesting to find predictors of the specific keytagging capacity of each individual image. The results obtained in the Thesis are the average of the proposed image test set. However, it was observed that certain modalities obtained a better robustness-capacity tradeoff — particularly, those high higher energy content.
- The extension of the keytagging algorithm to work with color images. There are certain biomedical modalities where the modifications of the color result in a modification of the diagnosis — e.g. color Doppler mode of echocardiograms, and thus shall be detected. In addition to this, working with the three color components (instead of with only the grayscale version of the image) will certainly improve the robustness-capacity tradeoff.
- The application of the keytagging algorithm to DICOM formats that store short videos as a series of frames. A simple operation of combination of the frames into a virtual image that would be keytagged may be enough to protect all the frames at once against attacks such as the removal, reordering or undue modification of frames. Furthermore, the frames may also be used individually or in small groups

to associate large contents — in a coordinated way, organized and indexed by parts.

- The extension of the keytagging algorithm to work on video, guaranteeing good integration with modern, widespread video codecs (e.g. H.265/HEVC) would be the perfect supplement for the current proposal, focused on images and fully compliant with JPEG2000 — and to some extent with JPEG.
- The study of security needs in other fields — apart from the medical — requiring not distorting the signals involved, such is the case of the military or high quality multimedia (based on lossless codecs), may result in new keytagging applications. This would certainly help to widen the popularity and utility of this technique.
- An interesting novel investigation may also be the reversal of the inputs of keytagging, in order to encode a certain secret message as a combination of public, unaltered images — involving very few side data. The research associated would include developing two critical parts: an engine that efficiently searches for images with features fitting a part of the secret message and the secure protocol to establishes the parameters of the transmission of the message(s) (e.g. number of bits coded by each image, channels where the images are shared).

# Bibliography

- [1] G. Eysenbach, "What is e-health?" *Journal of Medical Internet Research*, vol. 3, no. 2, p. e20, June 2001.
- [2] C. Dedding, R. van Doorn, L. Winkler, and R. Reis, "How will e-health affect patient participation in the clinic? A review of e-health studies and the current evidence for changes in the relationship between medical professionals and patients," *Social Science & Medicine*, vol. 72, no. 1, pp. 49–53, 2011.
- [3] J. P. Marcin, T. S. Nesbitt, S. L. Cole, R. M. Knuttel, D. M. Hilty, P. T. Prescott, and M. M. Daschbach, "Changes in diagnosis, treatment, and clinical improvement among patients receiving telemedicine consultations," *Telemedicine and e-Health*, vol. 11, no. 1, pp. 36–43, 2005.
- [4] D. Ahern, J. M. Phalen, and C. B. Eaton, "The role of eHealth in patient engagement and quality improvement," in *eHealth Solutions for Healthcare Disparities*, M. Gibbons, Ed. Springer New York, 2008, pp. 75–92.
- [5] S. Meystre, "The current state of telemonitoring: a comment on the literature," *Telemedicine Journal & e-Health*, vol. 11, no. 1, pp. 63–69, 2005.
- [6] B. G. Celler and R. S. Sparks, "Home telemonitoring of vital signs-technical challenges and future directions," *IEEE Journal of Biomedical and Health Informatics*, vol. 19, no. 1, pp. 82–91, 2015.
- [7] N. Demartines, U. Otto, D. Mutter, L. Labler, A. von Weymarn, M. Vix, and F. Harder, "An evaluation of telemedicine in surgery: telediagnosis compared with direct diagnosis," *Archives of Surgery*, vol. 135, no. 7, pp. 849–853, 2000.
- [8] S. Xing-Hua, Z. Xiao, G. Xiaoling, and P. Wei, "Design and development of tele-diagnosis system of medical image based on mobile terminal," in *2014 7th International Conference on Intelligent Computation Technology and Automation (ICICTA)*, 2014, pp. 149–153.
- [9] A. E. Tchalla, F. Lachal, N. Cardinaud, I. Saulnier, D. Bhalla, A. Roquejoffre, V. Rialle, P.-M. Preux, and T. Dantoine, "Efficacy of simple home-based technologies combined with a monitoring assistive center in decreasing falls in a frail elderly population (results of the Esoppe study)," *Archives of gerontology and geriatrics*, vol. 55, no. 3, pp. 683–689, 2012.
- [10] L. Anido Rifon, C. Rivas Costa, M. Gomez Carballa, S. Valladares Rodriguez, and M. Fernandez Iglesias, "Improving the quality of life of dependent and disabled people through home automation and tele-assistance," in *8th International Conference on Computer Science & Education (ICCSE)*. IEEE, 2013, pp. 478–483.
- [11] C. P. Schade, F. M. Sullivan, S. De Lusignan, and J. Madeley, "e-Prescribing, efficiency, quality: lessons from the computerization of UK family practice," *Journal of the American Medical Informatics Association*, vol. 13, no. 5, pp. 470–475, 2006.
- [12] R. S. Istepanian, E. Jovanov, and Y. Zhang, "Guest editorial introduction to the special section on m-health: beyond seamless mobility and global wireless health-care connectivity," *IEEE Transactions on Information Technology in Biomedicine*, vol. 8, no. 4, pp. 405–414, 2004.
- [13] R. S. H. Istepanian, S. Laxminarayan, and C. S. Pattichis, Eds., *M-health: Emerging mobile health systems*. Berlin: Springer, 2006.

- [14] M. Isakovic, J. Cijan, U. Sedlar, M. Volk, and J. Beter, "The role of mHealth applications in societal and social challenges of the future," in *12th International Conference on Information Technology-New Generations (ITNG)*. IEEE, 2015, pp. 561–566.
- [15] K. Davis, S. C. Schoenbaum, and A.-M. Audet, "A 2020 vision of patient-centered primary care," *Journal of General Internal Medicine*, vol. 20, no. 10, pp. 953–957, 2005.
- [16] R. M. Epstein, K. Fiscella, C. S. Lesser, and K. C. Stange, "Why the nation needs a policy push on patient-centered health care," *Health Affairs*, vol. 29, no. 8, pp. 1489–1495, 2010.
- [17] T. Martin, "Assessing mhealth: Opportunities and barriers to patient engagement," *Journal of health care for the poor and underserved*, vol. 23, no. 3, pp. 935–941, 2012.
- [18] A. Coulter, "Patient engagement—what works?" *The Journal of ambulatory care management*, vol. 35, no. 2, pp. 80–89, 2012.
- [19] M. Anshari and M. N. Almunawar, "mHealth technology implication: Shifting the role of patients from recipients to partners of care," *mHealth multidisciplinary verticals*, pp. 523–540, 2014.
- [20] S. Zan, S. Agboola, S. A. Moore, K. A. Parks, J. C. Kvedar, and K. Jethwani, "Patient engagement with a mobile web-based telemonitoring system for heart failure self-management: a pilot study," *JMIR mHealth and uHealth*, vol. 3, no. 2, 2015.
- [21] R. S. H. Istepanian and Y.-T. Zhang, "Guest editorial introduction to the special section: 4G Health x2014; the Long-Term Evolution of m-Health," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 1, pp. 1–5, 2012.
- [22] K. Ashton, "That "internet of things" thing," *RFID Journal*, vol. 22, no. 7, pp. 97–114, 2009.
- [23] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
- [24] R. Istepanian, A. Sungoor, A. Faisal, and N. Philip, "Internet of m-health Things "m-IoT"," in *IET Seminar on Assisted Living*, 2011, pp. 1–3.
- [25] R. Istepanian, S. Hu, N. Philip, and A. Sungoor, "The potential of Internet of m-health Things "m-IoT" for non-invasive glucose level sensing," in *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBC*, 2011, pp. 5264–5266.
- [26] D. F. Santos, A. Perkusich, and H. O. Almeida, "Standard-based and distributed health information sharing for mHealth IoT systems," in *16th International Conference on e-Health Networking, Applications and Services (Healthcom)*. IEEE, 2014, pp. 94–98.
- [27] P. R. Sama, Z. J. Eapen, K. P. Weinfurt, B. R. Shah, and K. A. Schulman, "An evaluation of mobile health application tools," *JMIR mHealth and uHealth*, vol. 2, no. 2, 2014.
- [28] V. M. Conraads, C. Deaton, E. Piotrowicz, N. Santaularia, S. Tierney, M. F. Piepoli, B. Pieske, J.-P. Schmid, K. Dickstein, P. P. Ponikowski *et al.*, "Adherence of heart failure patients to exercise: barriers and possible solutions," *European journal of heart failure*, vol. 14, no. 5, pp. 451–458, 2012.
- [29] R. Katz, T. Mesfin, and K. Barr, "Lessons from a community-based mhealth diabetes self-management program: It's not just about the cell phone," *Journal of health communication*, vol. 17, no. sup1, pp. 67–72, 2012.
- [30] M. Dredze, "How social media will change public health," *Intelligent Systems, IEEE*, vol. 27, no. 4, pp. 81–84, 2012.
- [31] J. M. Robillard, T. W. Johnson, C. Hennessey, B. L. Beattie, and J. Illes, "Aging 2.0: health information about dementia on Twitter," *PloS one*, vol. 8, no. 7, p. e69861, 2013.
- [32] J. J. Prochaska, C. Pechmann, R. Kim, and J. M. Leonhardt, "Twitter= quitter? An analysis of Twitter quit smoking social networks," *Tobacco control*, vol. 21, no. 4, pp. 447–449, 2012.

- [33] A. Signorini, A. M. Segre, and P. M. Polgreen, "The use of Twitter to track levels of disease activity and public concern in the US during the influenza A H1N1 pandemic," *PloS one*, vol. 6, no. 5, p. e19467, 2011.
- [34] M. Hingle, D. Yoon, J. Fowler, S. Kobourov, M. L. Schneider, D. Falk, and R. Burd, "Collection and visualization of dietary behavior and reasons for eating using Twitter," *Journal of medical Internet research*, vol. 15, no. 6, 2013.
- [35] P. Baumann, "140 healthcare uses for Twitter," URL: <http://philbaumann.com/140-health-care-uses-for-twitter/>[accessed 2015-11][WebCite Cache], 2009.
- [36] A. M. Kaplan and M. Haenlein, "Users of the world, unite! The challenges and opportunities of Social Media," *Business horizons*, vol. 53, no. 1, pp. 59–68, 2010.
- [37] A. K. Triantafyllidis, V. G. Koutkias, I. Chouvarda, and N. Maglaveras, "A pervasive health system integrating patient monitoring, status logging, and social sharing," *Journal of Biomedical and Health Informatics*, vol. 17, no. 1, pp. 30–37, 2013.
- [38] B. Filkins, "SANS health care cyberthreat report: widespread compromises detected, compliance nightmare on horizon," *Norse*. February, 2014.
- [39] A. Prasad, J. Sorber, T. Stablein, D. Anthony, and D. Kotz, "Exposing privacy concerns in mHealth," in *Proceedings of the USENIX Workshop on Health Security (HealthSec)*, 2011.
- [40] D. Lupton, "M-health and health promotion: The digital cyborg and surveillance society," *Social Theory & Health*, vol. 10, no. 3, pp. 229–244, 2012.
- [41] R. Whittaker, "Issues in mHealth: findings from key informant interviews," *Journal of medical Internet research*, vol. 14, no. 5, 2012.
- [42] "Global study of IT security spending & investments," Sponsored by Dell, independtly conducted by Ponemon Institute LLC, Accessed in November 2015, <http://goo.gl/IbJocT>, 2015.
- [43] "Cost of data breach study: global analysis," Benchmark research sponsored by IBM, independtly conducted by Ponemon Institute LLC, Accessed in November 2015, <http://goo.gl/IbJocT>, 2015.
- [44] J. Myers, T. R. Frieden, K. M. Bherwani, and K. J. Henning, "Ethics in public health research: privacy and public health at risk: public health confidentiality in the digital age," *American Journal of Public Health*, vol. 98, no. 5, p. 793, 2008.
- [45] M. E. Johnson, "Data hemorrhages in the health-care sector," in *Financial Cryptography and Data Security*. Springer, 2009, pp. 71–89.
- [46] M. E. Johnson and N. D. Willey, "Usability failures and healthcare data hemorrhages," *IEEE Security & Privacy*, no. 2, pp. 35–42, 2010.
- [47] E. Ball, D. W. Chadwick, and D. Mundy, "Patient privacy in electronic prescription transfer," *Security & Privacy*, vol. 1, no. 2, pp. 77–80, 2003.
- [48] "The Health Insurance Portability and Accountability Act (P.L.104-191)," 1996, enacted by the U.S. Congress.
- [49] "The Personal Information Protection and Electronic Document Act," 2000, enacted in Canada for protection of health information against commercial use.
- [50] "European Parliament legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," 12 March 2014, accessed in November 2015, <http://goo.gl/8L3WwD>.
- [51] "Ley Orgánica de Protección de Datos de carácter personal (Personal Data Protection Act)," 1999, enacted in Spain.
- [52] "FDA Safety Communication: cybersecurity for medical devices and hospital networks," US Food & Drug Administration (and others), 2013.

- [53] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," in *Eighth International Conference on Availability, Reliability and Security (ARES)*, Sept 2013, pp. 546–555.
- [54] C. Chen, D. Haddad, J. Selsky, J. E. Hoffman, R. L. Kravitz, D. E. Estrin, and I. Sim, "Making sense of mobile health data: an open architecture to improve individual-and population-level health," *Journal of medical Internet research*, vol. 14, no. 4, 2012.
- [55] E. Kyriacou, M. Pattichis, C. Pattichis, A. Panayides, and A. Pitsillides, "m-Health e-emergency systems: current status and future directions [Wireless corner]," *Antennas and Propagation Magazine*, vol. 49, no. 1, pp. 216–231, 2007.
- [56] "Annual meeting of the American Telemedicine Association," Accessed in November 2015, <http://goo.gl/6VNg9E>, 2014.
- [57] T. Suzuki, H. Tanaka, S. Minami, H. Yamada, and T. Miyata, "Wearable wireless vital monitoring technology for smart health care," in *7th International Symposium on Medical Information and Communication Technology (ISMICT)*. IEEE, 2013, pp. 1–4.
- [58] M. Alrige and S. Chatterjee, "Toward a taxonomy of wearable technologies in healthcare," in *New Horizons in Design Science: Broadening the Research Agenda*. Springer, 2015, pp. 496–504.
- [59] Y.-L. Zheng, X.-R. Ding, C. Poon, B. Lo, H. Zhang, X.-L. Zhou, G.-Z. Yang, N. Zhao, and Y.-T. Zhang, "Unobtrusive sensing and wearable devices for health informatics," *IEEE Transactions on Biomedical Engineering*, vol. 61, no. 5, pp. 1538–1554, May 2014.
- [60] A. J. Jara, M. A. Zamora-Izquierdo, and A. F. Skarmeta, "Interconnection framework for mHealth and remote monitoring based on the Internet of Things," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 47–65, September 2013.
- [61] A. M.-H. Kuo, "Opportunities and challenges of cloud computing to improve health care services," *Journal of medical Internet research*, vol. 13, no. 3, 2011.
- [62] N. Sultan, "Making use of cloud computing for healthcare provision: Opportunities and challenges," *International Journal of Information Management*, vol. 34, no. 2, pp. 177–184, 2014.
- [63] "HIMSS Analytics Cloud Survey," Accessed in November 2015, <http://goo.gl/x1bjYg>, 2014.
- [64] D. Lupton, "Quantifying the body: monitoring and measuring health in the age of mhealth technologies," *Critical Public Health*, vol. 23, no. 4, pp. 393–403, 2013.
- [65] G. Sorwar and R. Hasan, "Smart-TV based integrated e-health monitoring system with agent technology," in *26th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, March 2012, pp. 406–411.
- [66] D.-M. Shin, D. Shin, and D. Shin, "Smart watch and monitoring system for dementia patients," in *Grid and Pervasive Computing*. Springer, 2013, pp. 577–584.
- [67] Y. Zhao, T. Heida, E. van Wegen, B. R. Bloem, and R. van Wezel, "E-health support in people with Parkinson's disease with smart glasses: A survey of user requirements and expectations in the Netherlands," *Journal of Parkinson's disease*, 2015.
- [68] B. K. Wiederhold, "Time to port augmented reality health apps to smart glasses?" *Cyberpsychology, Behavior, and Social Networking*, vol. 16, no. 3, pp. 157–158, 2013.
- [69] H. Nakajima, T. Shiga, and Y. Hata, "Systems health care: Coevolutionary integration of smart devices and smart services," in *2012 Annual SRII Global Conference*. IEEE, 2012, pp. 231–236.
- [70] C. E. Chronaki and F. Chiarugi, "Interoperability as a quality label for portable & wearable health monitoring systems," *Studies in health technology and informatics*, vol. 117, pp. 108–116, 2005.
- [71] T. Norgall, "Interoperability-a key infrastructure requirement for personalised health services," *Studies in health technology and informatics*, vol. 117, p. 125, 2005.

- [72] G. De Moor, B. Claerhout, G. van Maele, and D. Dupont, "e-Health standardization in Europe: lessons learned," *Studies in Health Technology and Informatics*, vol. 100, pp. 233–7, 2004.
- [73] G. Klein *et al.*, "Standardization of health informatics-results and challenges," *Methods of Information in Medicine*, vol. 41, no. 4, pp. 261–270, 2002.
- [74] "Health informatics. Personal Health Devices communication (X73-PHD), ISO/IEEE 11073 (First edition: 2006). [11073-00103, Technical report-Overview][11073-10101, Nomenclature][1103-104zz, Device specializations][11073-20601<sup>TM</sup>-2014, Application profile-Optimized Exchange Protocol][11073-20101, Medical Device Encoding Rules (MDER)]," Accessed in November 2015, <http://http://goo.gl/i14L9h>.
- [75] J. D. Trigo, A. Alesanco, I. Martínez, and J. García, "A review on digital ECG formats and the relationships between them," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 3, pp. 432–444, May 2012.
- [76] "Standard Communication Protocol for computer-assisted ElectroCardioGraphy (SCP-ECG), ISO 11073-91064:2009," Accessed in November 2015, <http://goo.gl/Z0000k>, 2009.
- [77] "Health Level 7, ANSI standard," Accessed in November 2015, <http://goo.gl/zjATS2>, 2004.
- [78] "Medical waveform Format Encoding Rules (MFER), [ISO/DIS 22077-1:2015, part 1: encoding rule][ISO/TS 22077-2, part 2: electrocardiography][ISO/TS 22077-3, part 3: long term electrocardiography]," Accessed in November 2015, <http://goo.gl/ehjmFd>, 2007.
- [79] "Digital Imaging and COmmunications in Medicine (DICOM), National Electrical Manufacturers Association (NEMA)," Accessed in November 2015, <http://goo.gl/BtYbVP>.
- [80] "The eXtensible Markup Language (XML) 1.0, W3C Recommendation," 26 November 2008, Accessed in November 2015, <http://goo.gl/dCyNwe>.
- [81] A. P. Alves, H. Silva, A. Lourenço, and A. L. Fred, "BITalino: A biosignal acquisition system based on the Arduino," in *BIODEVICES*, 2013, pp. 261–264.
- [82] F. Abtahi, B. Aslami, I. Boujabir, F. Seoane, and K. Lindcrantz, "An affordable ECG and respiration monitoring system based on Raspberry PI and ADAS1000: first step towards homecare applications," in *16th Nordic-Baltic Conference on Biomedical Engineering*. Springer International Publishing, 2015, vol. 48, pp. 5–8.
- [83] "ISO/EN13606 CEN/TC251," Electronic Healthcare Record (EHR) Communication. Standard Parts 1-5. Accessed in November 2015, <http://www.en13606.org/>, 2004.
- [84] "openEHR, an open domain-driven platform for developing flexible e-health system," Accessed in November 2015, <http://www.openehr.org/>, 2004.
- [85] P. Urbauer, S. Sauermann, M. Frohner, M. Forjan, B. Pohn, and A. Mense, "Applicability of IHE/Continua components for PHR systems: Learning from experiences," *Computers in Biology and Medicine*, no. 0, pp. –, 2013.
- [86] N. Archer, U. Fevrier-Thomas, C. Lokker, K. A. McKibbin, and S. Straus, "Personal health records: a scoping review," *Journal of the American Medical Informatics Association*, vol. 18, no. 4, pp. 515–522, 2011.
- [87] "Apple HealthKit," Accessed in November 2015, <https://www.apple.com/es/ios/whats-new/health/>, 2014.
- [88] "Microsoft HealthVault," Accessed in November 2015, <https://www.healthvault.com/>, 2007.
- [89] "IHE International, Inc., IHE.net Home, Welcome to Integrating the Healthcare Enterprise, 2015," Accessed in November 2015, <http://ihe.net>.
- [90] R. Carroll, R. Cnossen, M. Schnell, and D. Simons, "Continua: An interoperable personal healthcare ecosystem," *Pervasive Computing*, vol. 6, no. 4, pp. 90–94, 2007.
- [91] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 3, pp. 1658–1686, 2014.

- [92] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.
- [93] S. Jalaaliddine, C. Hutchens, R. Strattan, and W. Coberly, "ECG data compression techniques-A unified approach," *IEEE Transactions on Biomedical Engineering*, vol. 37, no. 4, pp. 329–343, April 1990.
- [94] K. R. Rao, P. Yip, and V. Britanak, *Discrete Cosine Transform: Algorithms, advantages, applications*. Orlando, FL, USA: Academic Press, Inc., 2007.
- [95] S. Olmos, M. Millan, J. Garcia, and P. Laguna, "ECG data compression with the Karhunen-Loève transform," in *Computers in Cardiology*, September 1996, pp. 253–256.
- [96] M. Akay and C. Mello, "Wavelets for biomedical signal processing," in *Proceedings of the 19th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, vol. 6, November 1997, pp. 2688–2691.
- [97] A. Said and W. Pearlman, "A new, fast, and efficient image codec based on Set Partitioning In Hierarchical Trees," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 6, no. 3, pp. 243–250, June 1996.
- [98] R. Norcen, M. Podesser, A. Pommer, H.-P. Schmidt, and A. Uhl, "Confidential storage and transmission of medical image data," *Computers in Biology and Medicine*, vol. 33, no. 3, pp. 277–292, 2003.
- [99] M. Van Droogenbroeck, "Partial encryption of images for real-time applications," *Fourth IEEE Benelux Signal Processing, Hilvarenbeek, The Netherlands*, pp. 11–15, 2004.
- [100] A. B. Mahmood and R. D. Dony, "Segmentation based encryption method for medical images," in *2011 International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2011, pp. 596–601.
- [101] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, 1998.
- [102] R. J. Anderson and F. A. Petitcolas, "On the limits of steganography," *Selected Areas in Communications*, vol. 16, no. 4, pp. 474–481, 1998.
- [103] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *Security & Privacy*, vol. 1, no. 3, pp. 32–44, 2003.
- [104] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital watermarking and steganography*. Morgan Kaufmann, 2007.
- [105] H.-J. Guth and B. Pfitzmann, "Error-and collusion-secure fingerprinting for digital data," in *Information Hiding*. Springer, 2000, pp. 134–145.
- [106] Z. Lu, D. Kim, and W. Pearlman, "Wavelet compression of ECG signals by the Set Partitioning In Hierarchical Trees (SPIHT) algorithm," *IEEE Transactions on Biomedical Engineering*, vol. 47, no. 7, pp. 849–856, July 2000.
- [107] G. Higgins, B. McGinley, N. Walsh, M. Glavin, and E. Jones, "Lossy compression of EEG signals using SPIHT," *Electronics Letters*, vol. 47, no. 18, pp. 1017–1018, January 2011.
- [108] S.-H. Yang and W.-J. Liao, "A compressed domain image watermarking scheme with the SPIHT coding," *Journal of Information Science and Engineering*, vol. 26, no. 5, pp. 1755–1770, 2010.
- [109] S. Kozat, M. Vlachos, C. Lucchese, H. Van Herle, and P. Yu, "Embedding and retrieving private metadata in electrocardiograms," *Journal of Medical Systems*, vol. 33, pp. 241–259, 2009.
- [110] K. Zheng and X. Qian, "Reversible data hiding for electrocardiogram signal based on wavelet transforms," in *2008 International Conference on Computational Intelligence and Security, CIS*, vol. 1, December 2008, pp. 295–299.



- [111] X. Kong and R. Feng, "Watermarking medical signals for telemedicine," *IEEE Transactions on Information Technology in Biomedicine*, vol. 5, no. 3, pp. 195–201, September 2001.
- [112] R. Jamasebi, N. L. Johnson, F. Kaffashi, S. Redline, and K. A. Loparo, "A watermarking algorithm for polysomnography data," in *30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, August 2008, pp. 5720–5723.
- [113] M. Engin, O. Çidam, and E. Engin, "Wavelet transformation based watermarking technique for human electrocardiogram (ECG)," *Journal of Medical Systems*, vol. 29(6), pp. 589–594, 2005.
- [114] S. Kaur, O. Farooq, R. Singhal, and B. Ahuja, "Digital watermarking of ECG data for secure wireless communication," in *2010 International Conference on Recent Trends in Information, Telecommunication and Computing (ITC)*, Kochi, Kerala, India, March 2010, pp. 140–144.
- [115] K. Srinivasan and M. Ramasubba Reddy, "Efficient preprocessing technique for real-time lossless EEG compression," *Electronics Letters*, vol. 46, no. 1, pp. 26–27, July 2010.
- [116] W. Puech, "Image encryption and compression for medical image security," in *IPTA'08: 1st International Workshops on Image Processing Theory, Tools and Applications*, 2008.
- [117] F. Sufi and I. Khalil, "Enforcing secured ECG transmission for realtime telemonitoring: A joint encoding, compression, encryption mechanism," *Security and Communication Networks*, vol. 1, no. 5, pp. 389–405, 2008.
- [118] A. A. Kumar and A. Makur, "Lossy compression of encrypted image by compressive sensing technique," in *TENCON 2009-2009 IEEE Region 10 Conference*, 2009.
- [119] T. Xiang, J. Qu, and D. Xiao, "Joint SPIHT compression and selective encryption," *Applied Soft Computing*, vol. 21, pp. 159–170, 2014.
- [120] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," *Optics & Laser Technology*, vol. 62, pp. 152–160, 2014.
- [121] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding for all image formats," in *Electronic Imaging*. International Society for Optics and Photonics, 2002, pp. 572–583.
- [122] H.-Y. Huang, C.-H. Fan, and W.-H. Hsu, "An effective watermark embedding algorithm for high JPEG compression," in *MVA*. Citeseer, 2007, pp. 256–259.
- [123] A. Maor and N. Merhav, "On joint information embedding and lossy compression," *IEEE Transactions on Information Theory*, vol. 51, no. 8, pp. 2998–3008, Aug 2005.
- [124] C. Qin, C.-C. Chang, and Y.-P. Chiu, "A novel joint data-hiding and compression scheme based on SMVQ and image inpainting," *IEEE Transactions on Image Processing*, vol. 23, no. 3, pp. 969–978, March 2014.
- [125] W. Chen, Z. Shahid, T. Stütz, F. Autrusseau, and P. Le Callet, "Robust drift-free bit-rate preserving H. 264 watermarking," *Multimedia systems*, vol. 20, no. 2, pp. 179–193, 2014.
- [126] F. Battisti, M. Cancellaro, M. Carli, G. Boato, and A. Neri, "Watermarking and encryption of color images in the Fibonacci domain," in *Electronic Imaging*. International Society for Optics and Photonics, 2008, pp. 68 121C–68 121C.
- [127] M. Keyvanpour and M. Farnoosh, "A new encryption method for secure embedding in image watermarking," in *3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, vol. 2. IEEE, 2010, pp. V2–403.
- [128] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. De Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," *Signal Processing: Image Communication*, vol. 26, no. 1, pp. 1–12, 2011.

- [129] K.-L. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553–562, 2013.
- [130] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: A review of its benefits and open issues," *Signal Processing Magazine*, vol. 30, no. 2, pp. 87–96, 2013.
- [131] J. S. Bhalla and P. Nagrath, "Nested digital image watermarking technique using Blowfish encryption algorithm," *International Journal of Scientific and Research Publications*, vol. 3, no. 4, 2013.
- [132] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images," *Transactions on Information Technology in Biomedicine*, vol. 16, no. 5, pp. 891–899, 2012.
- [133] —, "An a priori and a posteriori protection by means of data hiding of encrypted images: application to ultrasound images," in *The International Conference on Health Informatics*. Springer, 2014, pp. 220–223.
- [134] "IHE Audit Trail and Node Authentication profile," Accessed in November 2015, <http://goo.gl/E0NMW4>.
- [135] "IHE Consistent Time profile," Accessed in November 2015, <http://goo.gl/rpGkUa>.
- [136] "IHE Document Digital Signature profile," Accessed in November 2015, <http://goo.gl/sWDkiw>.
- [137] "IHE Document Encryption profile," Accessed in November 2015, <http://goo.gl/bFrulk>.
- [138] "IHE Secure Retrieve profile," Accessed in November 2015, <http://goo.gl/OjDqYU>.
- [139] "IHE Access Control White Paper," Accessed in November 2015, <http://goo.gl/B3o6Ot>.
- [140] "IHE Basic Patient Privacy Consents profile," Accessed in November 2015, <http://goo.gl/5F7kUw>.
- [141] "IHE Cross-Enterprise User Assertion profile," Accessed in November 2015, <http://goo.gl/UGmGZC>.
- [142] "IHE Internet User Authorization profile," Accessed in November 2015, <http://goo.gl/e5WHxj>.
- [143] "IHE Enterprise User Authorization profile," Accessed in November 2015, <http://goo.gl/bN8Ncy>.
- [144] "Digital Imaging and COmmunications in Medicine (DICOM) Part 15: Security and System Management Profiles. National Electrical Manufacturers Association (NEMA)," Rosslyn, VA, PS 3.15 2015c. Accessed in November 2015, <http://goo.gl/CIafAu>, 2015.
- [145] "DICOM Standard Status, corrections, differences and supplements," Accessed in November 2015, <http://goo.gl/Y8G0p7>.
- [146] "HL7 Version 3: Role-based Access Control Healthcare Permission Catalog (RBAC)," Accessed in November 2015, <http://goo.gl/Snh642>, 2010.
- [147] "HL7 Version 3: Security and Privacy Ontology," Accessed in November 2015, <http://goo.gl/OI4d1b>, 2014.
- [148] "HL7 Healthcare Privacy and Security Classification System (HCS)," Accessed in November 2015, <http://goo.gl/bB7m8E>, 2014.
- [149] "IHE Personnel White Pages," Accessed in November 2015, <http://goo.gl/rUU6PK>.
- [150] "IHE Healthcare Provider Directory profile," Accessed in November 2015, <http://goo.gl/kkQOD8>.
- [151] R. Housley, Cryptographic Message Syntax (CMS), RFC 5652, IETF Network Working Group. Accessed in November 2015, <http://goo.gl/jczLER>, September 2009.
- [152] R. Latuske, "Bluetooth Health Device Profile and the IEEE 11073 medical device framework," *ARS Software GmbH: Starnberg, Bavaria, Germany*, 2009.
- [153] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.

- [154] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal processing*, vol. 90, no. 3, pp. 727–752, 2010.
- [155] R. Amirtharajan, J. Qin, and J. B. B. Rayappan, "Random image steganography and steganalysis: Present status and future directions," *Information Technology Journal*, vol. 11, no. 5, p. 566, 2012.
- [156] R. an Amirtharajan and J. Rayappan, "Steganography – time to time: A review," *Research Journal of Information Technology*, vol. 5, no. 2, pp. 58–66, 2013.
- [157] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Computer Science Review*, vol. 13, pp. 95–113, 2014.
- [158] X. Zhou, H. Huang, and S.-L. Lou, "Authenticity and integrity of digital mammography images," *IEEE Transactions on Medical Imaging*, vol. 20, no. 8, pp. 784–791, 2001.
- [159] F. Cao, H. Huang, and X. Zhou, "Medical image security in a HIPAA mandated PACS environment," *Computerized Medical Imaging and Graphics*, vol. 27, no. 2, pp. 185–196, 2003.
- [160] R. Acharya, U. Niranjana, S. S. Iyengar, N. Kannathal, and L. C. Min, "Simultaneous storage of patient information with medical images in the frequency domain," *Computer Methods and Programs in Biomedicine*, vol. 76, no. 1, pp. 13–19, 2004.
- [161] H.-C. Huang, F.-C. Chang, and W.-C. Fang, "Reversible data hiding with histogram-based difference expansion for QR code applications," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 2, pp. 779–787, 2011.
- [162] M. Bomewar, T. Baraskar, and V. Mankar, "DICOM image size reduction and data embedding using randomization technique," in *International Conference on Pervasive Computing (ICPC)*. IEEE, 2015, pp. 1–6.
- [163] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, "Relevance of watermarking in medical imaging," in *Proceedings of the IEEE International Conference on Information Technology Applications in Biomedicine*, 2000, pp. 250–255.
- [164] G. Coatrieux, L. Lecornu, B. Sankur, and C. Roux, "A review of image watermarking applications in health-care," in *28th IEEE Annual International Conference on Engineering in Medicine and Biology Society (EMBS)*, 2006, pp. 4691–4694.
- [165] D. S. Taubman, Author, M. W. Marcellin, Editor, and M. Rabbani, Reviewer, "JPEG2000: Image compression fundamentals, standards and practice," *Journal of Electronic Imaging*, vol. 11, no. 2, pp. 286–287, 2002.
- [166] I. J. Cox, M. Miller, and J. Bloom, "Watermarking applications and their properties," in *Proceedings of the International Conference on Information Coding and Computing*, 2000, pp. 6–10.
- [167] H. Nyeem, W. Boles, and C. Boyd, "A review of medical image watermarking requirements for teleradiology," *Journal of digital imaging*, vol. 26, no. 2, pp. 326–343, 2013.
- [168] D. Osborne, D. Abbott, M. Sorell, and D. Rogers, "Multiple embedding using robust watermarks for wireless medical images," in *Proceedings of the 3rd International Conference on Mobile and Ubiquitous Multimedia, MUM*, 2004, pp. 245–250.
- [169] X. Zhou, X. Duan, and D. Wang, "A semifragile watermark scheme for image authentication," in *Proceedings of the 10th International Multimedia Modelling Conference*, January 2004, pp. 374–377.
- [170] W. Gang and R. Ni-ni, "A fragile watermarking scheme for medical image," in *27th Annual International Conference of the Engineering in Medicine and Biology Society*, January 2005, pp. 3406–3409.
- [171] S.-G. Miaou, C.-M. Hsu, Y.-S. Tsai, and H.-M. Chao, "A secure data hiding technique with heterogeneous data-combining capability for electronic patient records," in *Proceedings of the 22nd IEEE Annual International Conference on Engineering in Medicine and Biology Society*, vol. 1, 2000, pp. 280–283.

- [172] A. Wakatani, "Digital watermarking for ROI medical images by using compressed signature image," in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences, HICSS*, 2002, pp. 2043–2048.
- [173] E. Cavero, A. Alesanco, L. Castro, J. Montoya, I. Lacambra, and J. Garcia, "SPIHT-based echocardiogram compression: clinical evaluation and recommendations of use," *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 1, pp. 103–112, 2013.
- [174] "J.M. Barton, Method and apparatus for embedding authentication information within digital data," 1997, U.S. Patent 5 646 997.
- [175] X. X. Leng, J. Xiao, D. Y. Li, and Z. Y. Shen, "Study on the digital image zero-watermarking technology," in *Advanced Materials Research*, vol. 765. Trans Tech Publ, 2013, pp. 1113–1117.
- [176] J. M. Zain and M. Clarke, "Reversible region of non-interest (RONI) watermarking for authentication of DICOM images," *International Journal of Computer Science and Network Security*, vol. 7, pp. 19–28, 2007.
- [177] O. M. Al-Qershi and B. E. Khoo, "Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images," *Journal of Digital Imaging*, vol. 24, no. 1, pp. 114–125, 2011.
- [178] C. K. Tan, J. C. Ng, X. Xu, C.-L. Poh, Y. L. Guan, and K. Sheah, "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability," *Journal of Digital Imaging*, pp. 528–540, 2011.
- [179] F. Rahimi, H. Rabbani *et al.*, "A dual adaptive watermarking scheme in contourlet domain for DICOM images," *Biomedical engineering online*, vol. 10, no. 1, p. 53, 2011.
- [180] "IHE Rosetta Terminology Mapping profile," Accessed in November 2015, <http://goo.gl/eapfbd>.
- [181] G. Schadow, The Unified Code for Units of Measure. Accessed in November 2015 <http://goo.gl/cvqf5N>, 2013.
- [182] D. Mills, U. Delaware, and J. Martin, Network Time Protocol version 4: Protocol and algorithms specification. IETF RFC 5905. Accessed in November 2015 <https://goo.gl/Sm51uY>, 2010.
- [183] "IHE Device Enterprise Communication profile," Accessed in November 2015, <http://goo.gl/AWpmGC>.
- [184] "IHE Alarm Communication Management profile," Accessed in November 2015, <http://goo.gl/mmtv61>.
- [185] "IHE Waveform Content Module profile," Accessed in November 2015, <http://goo.gl/QkYAy3>.
- [186] R. Gerhards, The Syslog Protocol. IETF RFC 5424. Accessed in November 2015 <https://goo.gl/16risu>, 2009.
- [187] "IHE Cross-Enterprise Document Sharing profile," Accessed in November 2015, <http://goo.gl/O6BUIo>.
- [188] K. Breining and F. Najmi, Enabling Business using eXtensible Markup Language. ISO 15000-1-5. Accessed in November 2015 <https://goo.gl/5QqkGd>, 2012.
- [189] S. Emery, Kerberos Version 5. General Security Service Application Program Interface (GSS-API) Channel Binding Hash Agility. IETF RFC 6542. Accessed in November 2015 <https://goo.gl/9hn2h9>, 2012.
- [190] "IHE Patient Identifier Cross-Referencing profile," Accessed in November 2015, <http://goo.gl/fJttTT>.
- [191] "IHE Medical Equipment Management: Medical Device Cyber Security – Best Practice Guide," Accessed in November 2015, <http://goo.gl/zzXnj7>.
- [192] I. Martínez, J. Escayola, M. Martínez-Espronedca, P. Muñoz, J. D. Trigo, A. Muñoz, S. Led, L. Serrano, and J. García, "Seamless integration of ISO/IEEE11073 personal health devices and ISO/EN13606 electronic health records into an end-to-end interoperable solution," *Telemedicine and e-Health*, vol. 16, no. 10, pp. 993–1004, 2010.
- [193] J.-H. Lim, C. Park, and S.-J. Park, "Home healthcare settop-box for senior chronic care using ISO/IEEE 11073 PHD standard," in *2010 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 2010, pp. 216–219.

- [194] J. D. Trigo, I. Martínez, A. Alesanco, A. Kollmann, J. Escayola, D. Hayn, G. Schreier, and J. García, “An integrated healthcare information system for end-to-end standardized exchange and homogeneous management of digital ECG formats,” *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 4, pp. 518–529, 2012.
- [195] J. Trigo, F. Chiarugi, A. Alesanco, M. Martínez-Espronedada, L. Serrano, C. Chronaki, J. Escayola, I. Martínez, and J. García, “Interoperability in digital electrocardiography: harmonization of ISO/IEEE x73-PHD and SCP-ECG,” *IEEE Transactions on Information Technology in Biomedicine*, vol. 14(6), pp. 1303–1317, 2010.
- [196] C. Zywietz, V. Mertins, D. Assanelli, and C. Malossi, “Digital ECG transmission from ambulance cars with application of the European Standard Communications Protocol SCP-ECG,” in *Computers in Cardiology*, 1994, pp. 341–344.
- [197] J. Trigo, F. Chiarugi, A. Alesanco, M. Martínez-Espronedada, C. Chronaki, J. Escayola, I. Martínez, and J. García, “Standard-compliant real-time transmission of ECGs: harmonization of ISO/IEEE 11073-PHD and SCP-ECG,” in *Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBC*, Minneapolis, September 2009, pp. 4635–4638.
- [198] C. Chronaki, F. Chiarugi, P. Lees, M. Bruun-Rasmussen, F. Conforti, R. Ruiz, and C. Zywietz, “Open ECG: a European project to promote the SCP-ECG standard, a further step towards interoperability in electrocardiography,” in *Computers in Cardiology*, September 2002, pp. 285–288, accessed in November 2015, <http://www.openecg.net>.
- [199] V. Sakkalis, F. Chiarugi, S. Kostomanolakis, C. Chronaki, M. Tsiknakis, and S. Orphanoudakis, “A gateway between the SCP-ECG and the DICOM supplement 30 waveform standard,” in *Computers in Cardiology*, September 2003, pp. 25–28.
- [200] A. Schloegl, F. Chiarugi, E. Cervesato, E. Apostolopoulos, and C. Chronaki, “Two-way converter between the HL7 aECG and SCP-ECG data formats using BioSig,” in *Computers in Cardiology*, 2007, pp. 253–256.
- [201] G. Moody, R. Mark, and A. Goldberger, “Evaluation of the ‘TRIM’ ECG data compressor,” in *Computers in Cardiology*, September 1988, pp. 167–170.
- [202] G. Moody, “The physionet/computers in cardiology challenge 2008: T-wave alternans,” in *Computers in Cardiology*, September 2008, pp. 505–508.
- [203] “Digital Imaging and COmmunications in Medicine (DICOM) Part 3: Information Object Definitions. National Electrical Manufacturers Association (NEMA),” PS 3.3. Accessed in November 2015, <http://goo.gl/0YNNLv>, 2015.
- [204] H. Wyle, “Run length encoder,” 1962, uS Patent 3,061,672.
- [205] W. B. Pennebaker and J. L. Mitchell, *JPEG: Still image data compression standard*. Springer Science & Business Media, 1993.
- [206] ITU-T H.264. Advanced video coding for generic audiovisual services. Accessed in November 2015 <https://goo.gl/ZsZl2r>, 2014.
- [207] T. Dierks and E. Rescorla, The Transport Layer Security (TLS) protocol version 1.2. IETF RFC 5246. Accessed in November 2015 <http://goo.gl/4Mn9F1>, 2008.
- [208] C. Cahill and J. Hughes, OASIS Security Services TC: Assertions and protocols for the OASIS security assertion markup language (SAML) v2.0. Accessed in November 2015 <http://goo.gl/SHzAIG>, 2005.
- [209] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, DNS Security Introduction and Requirements. IETF RFC 4033. Accessed in November 2015 <https://goo.gl/qr3YNK>, 2005.
- [210] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, Dynamic Host Configuration Protocol for IPv6 (DHCPv6). IETF RFC 3315. Accessed in November 2015 <https://goo.gl/DIER36>, 2003.
- [211] D. Mills, Simple Network Time Protocol version 4 for IPv4, IPv6 and OSI. IETF RFC 4330. Accessed in November 2015 <https://goo.gl/4j6Xzp>, 2006.

- [212] G. J. Mandellos, M. N. Koukias, I. S. Styliadis, and D. K. Lymberopoulos, "e-SCP-ECG+ protocol: an expansion on SCP-ECG protocol for health telemonitoring—Pilot implementation," *International Journal of Telemedicine and Applications*, vol. 2010, pp. 1–17, 2010.
- [213] M. Gerdesa, D. Trinugrohoa, and R. Fenslia, "Aspects of standardisation for point-of-care solutions and remote home monitoring services," in *Scandinavian Conference on Health Informatics*, 2013, p. 19.
- [214] C. Costa and J. L. Oliveira, "Telecardiology through ubiquitous Internet services," *International Journal of Medical Informatics*, vol. 81, no. 9, pp. 612–621, 2012.
- [215] S. Yuan, D. Wei, and W. Xu, *Broadening the exchange of electrocardiogram data from intra-hospital to inter-hospital*. INTECH Open Access Publisher, 2012.
- [216] "eXtensible Access Control Markup Language (XACML) Version 3.0," Accessed in November 2015, <http://goo.gl/2fIERL>, 2013.
- [217] J.-c. Hsieh and M.-W. Hsu, "A cloud computing based 12-lead ECG telemedicine service," *BMC medical informatics and decision making*, vol. 12, no. 1, p. 77, 2012.
- [218] D. S. Seo, S. S. Kim, Y. H. Lee, and J. M. Kim, "Implementation of personal health device communication protocol applying ISO/IEEE 11073-20601," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.
- [219] M. Jung, J. G. Park, J. H. Kim, and J. Cho, "Interoperability between medical devices using Near Field Communication," in *IEEE International Conference on Information Science and Applications (ICISA)*, 2013, pp. 1–4.
- [220] A. F. Martins, D. F. Santos, A. Perkusich, and H. O. Almeida, "UPnP and IEEE 11073: Integrating personal health devices in home networks," in *11th IEEE Consumer Communications and Networking Conference (CCNC)*, 2014, pp. 1–6.
- [221] L. Caranguian, S. Pancho-Festin, and L. Sison, "Device interoperability and authentication for telemedical appliance based on the ISO/IEEE 11073 personal health device (PHD) standards," in *2012 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, August 2012, pp. 1270–1273.
- [222] A. Egner, A. Soceanu, and F. Moldoveanu, "Managing secure authentication for standard mobile medical networks," in *2012 IEEE Symposium on Computers and Communications (ISCC)*, 2012, pp. 390–393.
- [223] S. S. Kim, Y. H. Lee, J. M. Kim, D. S. Seo, G. H. Kim, and Y. S. Shin, "Privacy protection for personal health device communication and healthcare building applications," *Journal of Applied Mathematics*, vol. 2014, 2014.
- [224] A. Kliem, M. Hovestadt, and O. Kao, "Security and communication architecture for networked medical devices in mobility-aware eHealth environments," in *2012 IEEE First International Conference on Mobile Services (MS)*, 2012, pp. 112–114.
- [225] H. G. Barrón-González, M. Martínez-Espronedada, J. D. Trigo, S. Led, and L. Serrano, "Lessons learned from the implementation of remote control for the interoperability standard ISO/IEEE11073-20601 in a standard weighing scale," *Computer Methods and Programs in Biomedicine*, 2015.
- [226] H. Huang, "Teleradiology today," *Telehealth, Business Briefing: Next Generation HealthCare*, pp. 1–7, 1997.
- [227] X. Zhou, S. A. Lou, and H. Huang, "Authenticity and integrity of digital mammographic images," in *Medical Imaging'99*. International Society for Optics and Photonics, 1999, pp. 138–144.
- [228] X. Zhou, H. Huang, and S. A. Lou, "Secure method for sectional image archiving and transmission," in *Medical Imaging*. International Society for Optics and Photonics, 2000, pp. 390–399.
- [229] "openID - The Internet Identity Layer," Accessed in November 2015, <http://openid.net/>, 2015.
- [230] "DICOM Part 18 Version 2015c - Web Services," Accessed in November 2015, <http://goo.gl/ZrkABT>, 2015.

- [231] W. Ma, K. Sartipi, H. Sharghi, D. Koff, and P. Bak, "OpenID connect as a security service in Cloud-based diagnostic imaging systems," in *SPIE Medical Imaging*. International Society for Optics and Photonics, 2015, pp. 94 180J–94 180J.
- [232] Y.-Y. Chang, H.-B. Zhong, and M.-L. Wang, "Implementation of mobile DICOM image retrieval application with QR-code authentication," in *IEEE International Symposium on Computer, Consumer and Control (IS3C)*, 2014, pp. 372–375.
- [233] ElevenPaths, Latch. Accessed in November 2015 <http://goo.gl/ibG201>, November 2013.
- [234] D. Abouakil, J. Heurix, and T. Neubauer, "Data models for the pseudonymization of DICOM data," in *44th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2011, pp. 1–11.
- [235] M. Dzwonkowski, M. Papaj, and R. Rykaczewski, "A new quaternion-based encryption method for DICOM images," *IEEE Transactions on Image Processing*, vol. 24, no. 11, pp. 4614–4622, 2015.
- [236] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in *Advances in Cryptology-CRYPTO 2007*. Springer, 2007, pp. 535–552.
- [237] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography and Data Security*. Springer, 2010, pp. 136–149.
- [238] Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers," in *IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 917–922.
- [239] P. Thiagarajan and G. Aghila, "Reversible dynamic secure steganography for medical image using graph coloring," *Health Policy and Technology*, vol. 2, no. 3, pp. 151–161, 2013.
- [240] H. Al-Dmour and A. Al-Ani, "Quality optimized medical image steganography based on edge detection and hamming code," in *12th IEEE International Symposium on Biomedical Imaging (ISBI)*. IEEE, 2015, pp. 1486–1489.
- [241] L. O. Kobayashi and S. S. Furuie, "Proposal for DICOM multiframe medical image integrity and authenticity," *Journal of digital imaging*, vol. 22, no. 1, pp. 71–83, 2009.
- [242] W. Dou, C. L. Poh, and Y. L. Guan, "An improved tamper detection and localization scheme for volumetric DICOM images," *Journal of digital imaging*, vol. 25, no. 6, pp. 751–763, 2012.
- [243] M. M. Abd-Eldayem, "A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine," *Egyptian Informatics Journal*, vol. 14, no. 1, pp. 1–13, 2013.
- [244] A. Lavanya and V. Natarajan, "Enhancing security of DICOM images during storage and transmission in distributed environment," *Sadhana*, vol. 36, no. 4, pp. 515–523, 2011.
- [245] S. Das and M. K. Kundu, "Effective management of medical information through ROI-lossless fragile image watermarking technique," *Computer methods and programs in biomedicine*, vol. 111, no. 3, pp. 662–675, 2013.
- [246] A. N. Akansu and M. J. Medley, Eds., *Wavelet, subband, and block transforms in communications and multimedia*. Norwell, MA, USA: Kluwer Academic Publishers, 1999.
- [247] S. Mallat, *A wavelet tour of signal processing*. Academic press, 1999.
- [248] B.-J. Kim, Z. Xiong, and W. Pearlman, "Low bit-rate scalable video coding with 3-D Set Partitioning In Hierarchical Trees (3-D SPIHT)," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 10, no. 8, pp. 1374–1387, December 2000.
- [249] G. Ziegler, H. Lensch, M. Magnor, and H.-P. Seidel, "Multi-video compression in texture space using 4D SPIHT," in *6th IEEE Workshop on Multimedia Signal Processing*, September 2004, pp. 39–42.
- [250] M. Wegmueller, D. Perels, T. Blaser, S. Senn, P. Stadelmann, N. Felber, and W. Fichtner, "Silicon implementation of the SPIHT algorithm for compression of ECG records," in *49th IEEE International Midwest Symposium on Circuits and Systems, MWSCAS*, vol. 2, August 2006, pp. 381–385.

- [251] T. H. Oh and R. Besar, "Medical image compression using JPEG-2000 and JPEG: A comparison study," *Journal of Mechanics in Medicine and Biology*, vol. 2, no. 03, pp. 313–328, 2002.
- [252] C. Christopoulos, J. Askelof, and M. Larsson, "Efficient methods for encoding regions of interest in the upcoming JPEG2000 still image coding standard," *IEEE Signal Processing Letters*, vol. 7, no. 9, pp. 247–249, Sept 2000.
- [253] A. Cohen, I. Daubechies, and J. Feauveau, "Biorthogonal bases of compactly supported wavelets," *Communications on Pure and Applied Mathematics*, vol. 45, pp. 485–560, 1992.
- [254] G. Swain and S. K. Lenka, "Steganography using two sided, three sided, and four sided side match methods," *CSI transactions on ICT*, vol. 1, no. 2, pp. 127–133, 2013.
- [255] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.
- [256] Y. Li, C.-T. Li, and C.-H. Wei, "Protection of mammograms using blind steganography and watermarking," in *Third International Symposium on Information Assurance and Security*. IEEE, 2007, pp. 496–500.
- [257] P. K. Dilip and V. B. Raskar, "Hiding patient confidential information in ECG signal using DWT technique," *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 4, no. 2, pp. 533–538, 2015.
- [258] Z. Qian and X. Zhang, "Lossless data hiding in JPEG bitstream," *Journal of Systems and Software*, vol. 85, no. 2, pp. 309–313, 2012.
- [259] L. S. Nair and L. M. Joshy, "An improved image steganography method with SPIHT and arithmetic coding," in *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*. Springer, 2015, pp. 97–104.
- [260] L.-C. Huang, L.-Y. Tseng, and M.-S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images," *Journal of Systems and Software*, vol. 86, no. 3, pp. 716–727, 2013.
- [261] L. Marvel, J. Boncelet, C.G., and C. Retter, "Spread spectrum image steganography," *IEEE Transactions on Image Processing*, vol. 8, no. 8, pp. 1075–1083, August 1999.
- [262] M. Mahajan and N. Kaur, "Adaptive steganography: a survey of recent statistical aware steganography techniques," *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 4, no. 10, p. 76, 2012.
- [263] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal processing*, vol. 66, no. 3, pp. 385–403, 1998.
- [264] A. Tefas and I. Pitas, "Robust spatial image watermarking using progressive detection," in *International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, vol. 3. IEEE, 2001, pp. 1973–1976.
- [265] K. Pal, G. Ghosh, M. Bhattacharya *et al.*, "A comparative study between LSB and modified bit replacement (MBR) watermarking technique in spatial domain for biomedical image security," *International Journal of Computer Applications Technology and Research*, vol. 1, no. 1, pp. 30–39, 2012.
- [266] H.-M. Chao, C.-M. Hsu, and S.-G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Transactions on Information Technology in Biomedicine*, vol. 6, no. 1, pp. 46–53, 2002.
- [267] A. Giakoumaki, S. Pavlopoulos, and D. Koutouris, "A medical image watermarking scheme based on wavelet transform," in *Proceedings of the 25th IEEE Annual International Conference on Engineering in Medicine and Biology Society*, vol. 1, 2003, pp. 856–859.
- [268] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Secure and efficient health data management through multiple watermarking on medical images," *Medical and Biological Engineering and Computing*, vol. 44, no. 8, pp. 619–631, 2006.



- [269] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-domain system for robust image watermarking," *Signal processing*, vol. 66, no. 3, pp. 357–372, 1998.
- [270] I. Kallel, M. Kallel, and M. Bouhleb, "A secure fragile watermarking algorithm for medical image authentication in the DCT domain," in *Information and Communication Technologies, 2nd ICTTA*, vol. 1, 2006, pp. 2024–2029.
- [271] X. G. Xia, C. Bonchelet, and G. Arce, "Wavelet transform based watermark for digital images," *Optics Express*, vol. 3, no. 12, pp. 497–511, December 1998.
- [272] N. Kaewamnerd and K. Rao, "Wavelet based image adaptive watermarking scheme," *Electronics Letters*, vol. 36, no. 4, pp. 312–313, February 2000.
- [273] P. Fakhari, E. Vahedi, and C. Lucas, "Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach," *Digital Signal Processing*, vol. 21, no. 3, pp. 433–446, 2011.
- [274] H. Tao, J. M. Zain, M. M. Ahmed, A. N. Abdalla, and W. Jing, "A wavelet-based particle swarm optimization algorithm for digital image watermarking," *Integrated Computer-Aided Engineering*, vol. 19, no. 1, pp. 81–91, 2012.
- [275] N. Kashyap and G. Sinha, "Image watermarking using 3-level discrete wavelet transform (DWT)," *International Journal of Modern Education and Computer Science (IJMECS)*, vol. 4, no. 3, p. 50, 2012.
- [276] Y.-H. Chen and H.-C. Huang, "A progressive image watermarking scheme for JPEG2000," in *Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*. IEEE, 2012, pp. 230–233.
- [277] S. A. Mostafa, N. El-sheimy, A. Tolba, F. Abdelkader, and H. M. Elhindy, "Wavelet packets-based blind watermarking for medical image management," *The open biomedical engineering journal*, vol. 4, p. 93, 2010.
- [278] H. Y. Leung and L. M. Cheng, "Robust watermarking scheme using wave atoms," *EURASIP Journal on Advances in Signal Processing*, vol. 2011, p. 3, 2011.
- [279] D. Zheng, Y. Liu, J. Zhao, and A. E. Saddik, "A survey of RST invariant image watermarking algorithms," *ACM Computing Surveys (CSUR)*, vol. 39, no. 2, p. 5, 2007.
- [280] J. J. O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal processing*, vol. 66, no. 3, pp. 303–317, 1998.
- [281] C.-Y. Lin, M. Wu, J. Bloom, I. J. Cox, M. L. Miller, Y. M. Lui *et al.*, "Rotation, scale, and translation resilient watermarking for images," *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 767–782, 2001.
- [282] K. Hyung-Shin, Y. Baek, L. Heung-Kyu, and S. Young-Ho, "Robust image watermark using radon transform and bispectrum invariants," in *Information Hiding*. Springer, 2003, pp. 145–159.
- [283] H. Zhu, M. Liu, and Y. Li, "The RST invariant digital image watermarking using Radon transforms and complex moments," *Digital Signal Processing*, vol. 20, no. 6, pp. 1612–1628, 2010.
- [284] M. Deng, Q. Zeng, and X. Zhou, "A robust watermarking against shearing based on improved S-Radon transformation," *Journal of computers*, vol. 7, no. 10, pp. 2549–2556, 2012.
- [285] H. S. Kim and H.-K. Lee, "Invariant image watermark using Zernike moments," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 766–775, 2003.
- [286] J. Guang Sun and W. He, "RST invariant watermarking scheme based on SIFT feature and pseudo-Zernike moment," *International Symposium on Computational Intelligence and Design*, vol. 2, pp. 10–13, 2009.
- [287] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *Multimedia, IEEE Transactions on*, vol. 4, no. 1, pp. 121–128, 2002.
- [288] C.-C. Chang, P. Tsai, and C.-C. Lin, "SVD-based digital image watermarking scheme," *Pattern Recognition Letters*, vol. 26, no. 10, pp. 1577–1586, 2005.

- [289] P. K. Gupta and S. K. Shrivastava, "Improved RST-attacks resilient image watermarking based on joint SVD-DCT," in *International Conference on Computer and Communication Technology (ICCCCT)*. IEEE, 2010, pp. 46–51.
- [290] E. Ganic and A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies," in *Proceedings of the 2004 Workshop on Multimedia and Security*. ACM, 2004, pp. 166–174.
- [291] P. Saxena, S. Garg, and A. Srivastava, "DWT-SVD semi-blind image watermarking using high frequency band," in *2nd International Conference on Computer Science and Information Technology (ICCSIT)*, 2012, pp. 28–29.
- [292] H. Li, S. Wang, W. Song, and Q. Wen, "A novel watermarking algorithm based on SVD and zernike moments," in *Intelligence and Security Informatics*. Springer, 2005, pp. 448–453.
- [293] K. Navas, M. C. Ajay, M. Lekshmi, T. S. Archana, and M. Sasikumar, "DWT-DCT-SVD based watermarking," in *3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE*. IEEE, 2008, pp. 271–274.
- [294] M. I. Khan, M. Rahman, M. Sarker, I. Hasan *et al.*, "Digital Watermarking for Image AuthenticationBased on Combined DCT, DWT and SVD Transformation," *arXiv preprint arXiv:1307.6328*, 2013.
- [295] H.-C. Huang, F.-C. Chang *et al.*, "Robust image watermarking based on compressed sensing techniques," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 2, pp. 275–285, 2014.
- [296] H. Wu, J. Zhou, X. Gong, Y. Wen, and B. Li, "A new JPEG image watermarking algorithm based on cellular automata," *Journal of Information & Computational Science*, vol. 8, no. 12, pp. 2431–2439, 2011.
- [297] S.-Z. Fu, J.-W. Fan, Y.-C. Chen, and R.-J. Chen, "Multi-bit watermarking in the data stream of JPEG2000 using minimum error embedding technique," in *IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*. IEEE, 2015, pp. 390–391.
- [298] A. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, "Robust watermarking of compressed and encrypted JPEG2000 images," *IEEE Transactions on Multimedia*, vol. 14, no. 3, pp. 703–716, 2012.
- [299] A. Mishra, A. Goel, R. Singh, G. Chetty, and L. Singh, "A novel image watermarking scheme using extreme learning machine," in *International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2012, pp. 1–6.
- [300] M. Ali, C. W. Ahn, and M. Pant, "A robust image watermarking technique using SVD and differential evolution in DCT domain," *Optik-International Journal for Light and Electron Optics*, vol. 125, no. 1, pp. 428–434, 2014.
- [301] A. R. B. Shahid, "An image watermarking approach based on Set Partitioning in Hierarchical Trees (SPIHT) algorithm," in *International Conference on Informatics, Electronics & Vision (ICIEV)*. IEEE, 2012, pp. 487–492.
- [302] C.-S. Woo, J. Du, and B. L. Pham, "Multiple watermark method for privacy control and tamper detection in medical images," in *Proceedings of the APRS Workshop on Digital Image Computing*, 2005, pp. 59–64.
- [303] H.-K. Lee, H.-J. Kim, S.-G. Kwon, and J.-K. Lee, "ROI medical image watermarking using DWT and bit-plane," in *Asia-Pacific Conference on Communications*, 2005, pp. 512–515.
- [304] X. Guo and T. ge Zhuang, "A region-based lossless watermarking scheme for enhancing security of medical data," *Journal of Digital Imaging*, vol. 22, no. 1, pp. 53–64, 2009.
- [305] M. Kundu and S. Das, "Lossless ROI medical image watermarking technique with enhanced security and high payload embedding," in *20th International Conference on Pattern Recognition (ICPR)*, 2010, pp. 1457–1460.
- [306] A. Khan, A. Siddiq, S. Munib, and S. A. Malik, "A recent survey of reversible watermarking techniques," *Information Sciences*, vol. 279, pp. 251–272, 2014.
- [307] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

- [308] C. De Vleeschouwer, J.-F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEEE Transactions on Multimedia*, vol. 5, no. 1, pp. 97–105, 2003.
- [309] H. Trichili, M. Boublel, N. Derbel, and L. Kamoun, "A new medical image watermarking scheme for a better telediagnosis," in *IEEE International Conference on Systems, Man and Cybernetics*, vol. 1, 2002, pp. 556–559.
- [310] G. Coatrieux, M. Lamard, W. Daccache, W. Puentes, and C. Roux, "A low distortion and reversible watermark: application to angiographic images of the retina," in *27th Annual International Conference on Engineering in Medicine and Biology Society, IEEE-EMBS*, 2006, pp. 2224–2227.
- [311] G. Coatrieux, C. Le Guillou, J.-M. Cauvin, and C. Roux, "Reversible watermarking for knowledge digest embedding and reliability control in medical images," *Transaction on Information Technology in Biomedicine*, vol. 13, no. 2, pp. 158–165, January 2009.
- [312] X. Guo and T. ge Zhuang, "Lossless watermarking for verifying the integrity of medical images with tamper localization," *Journal of Digital Imaging*, vol. 22, no. 6, pp. 620–628, 2009.
- [313] W. Quan, S. Tan-feng, and W. Shu-xun, "Concept and application of zero-watermark," *Chinese Journal of Electronics*, vol. 31, no. 2, p. 214, 2003.
- [314] W.-h. Niu and S.-h. Yang, "A non-watermarking algorithm based on the MSB structure key," *Computer Engineering & Science*, vol. 4, pp. 55–58, 2010.
- [315] Q. Wen, "Research on robustness and imperceptibility of multimedia digital watermarking," *Jilin University, Jilin*, 2005.
- [316] X.-y. Zhao and J.-y. Sun, "Novel zero-watermarking based on SIFT feature of digital image," *Appli Res Comput*, vol. 27, no. 4, pp. 1517–1520, 2010.
- [317] C. Dong, H. Zhang, J. Li, and Y.-w. Chen, "Robust zero-watermarking for medical image based on DCT," in *6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*. IEEE, 2011, pp. 900–904.
- [318] C. Dong, J. Li, Y.-w. Chen, and Y. Bai, "Zero watermarking for medical images based on DFT and LFSR," in *IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, vol. 1. IEEE, 2012, pp. 22–26.
- [319] S. Che, B. Ma, Z. Che, and Q. Huang, "A wavelet-based method of zero-watermark," in *International Conference on Wavelet Analysis and Pattern Recognition, ICWAPR*. IEEE, 2009, pp. 293–297.
- [320] J. Li, W. Du, Y. Bai, and Y.-w. Chen, "3D-DCT based zero-watermarking for medical volume data robust to geometrical attacks," in *Wireless Communications and Applications*. Springer, 2012, pp. 433–444.
- [321] Y.-t. Zhai and D.-y. Peng, "A image zero-watermarking scheme for resist geometric attacks," *Information Technology*, vol. 11, pp. 33–35, 2007.
- [322] T.-y. Ye, Z.-f. Ma, X.-x. Niu, and Y.-x. Yang, "A zero-watermark technology with strong robustness," *Journal of Beijing University of Posts and Telecommunications*, vol. 33, no. 3, pp. 126–129, 2010.
- [323] Y.-f. Hu and S.-a. Zhu, "Zero-watermark algorithm based on PCA and chaotic scrambling," *Journal of Zhejiang University*, vol. 42, no. 4, pp. 593–597, 2008.
- [324] J. Li, X. Han, C. Dong, and Y.-w. Chen, "Robust multiple watermarks for medical image based on DWT and DFT," in *6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*. IEEE, 2011, pp. 895–899.
- [325] Y. Zhou and W. Jin, "A novel image zero-watermarking scheme based on DWT-SVD," in *International Conference on Multimedia Technology (ICMT)*. IEEE, 2011, pp. 2873–2876.

- [326] W. Wang, A. Men, and X. Chen, "Robust image watermarking scheme based on phase features in DFT domain and generalized radon transformations," in *2nd International Congress on Image and Signal Processing, CISP'09*. IEEE, 2009, pp. 1–5.
- [327] V. Seenivasagam and R. Velumani, "A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud," *Computational and mathematical methods in medicine*, vol. 2013, 2013.
- [328] L. Jing, Y. Zhang, and G. Chen, "Zero-watermarking for copyright protection of remote sensing image," in *9th International Conference on Signal Processing, ICSP*. IEEE, 2008, pp. 1083–1086.
- [329] L. Jing and S. Li, "Robust zero-watermarking scheme using local invariant keypoints," *MUSP*, vol. 7, pp. 39–44, 2007.
- [330] "Universal Serial Bus Device Class Definition for Personal Healthcare Devices," Accessed in November 2015, <http://goo.gl/msnLtG>, 2007.
- [331] "ZigBee Health Care Profile Specifications," Accessed in November 2015, <http://goo.gl/WmHjG1>, 2010.
- [332] "Bluetooth Health Device Profile," Accessed in November 2015, <http://goo.gl/xoJlr3>, 2012.
- [333] "Bluetooth 4.0: Low Energy," Accessed in November 2015, <http://goo.gl/3z8LoQ>, 2010.
- [334] "Near Field Communication," NFC technical specifications. Accessed in November 2015, <http://goo.gl/P7xstO>, 2010.
- [335] "Discover Wi-Fi Direct," Accessed in November 2015, <http://goo.gl/oQPsSh>, 2010.
- [336] "Wireless USB Technical Documents," Accessed in November 2015, <http://goo.gl/yhLIgy>, 2010.
- [337] A. Aragues, J. Escayola, I. Martínez, P. del Valle, P. Muñoz, J. D. Trigo, and J. García, "Trends and challenges of the emerging technologies toward interoperability and standardization in e-health communications," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 182–188, 2011.
- [338] D. G. Feekes, "Out-of-band authentication," November 2013 2014, uS Patent 20,140,337,957.
- [339] K. Singh and L. Koved, "Practical out-of-band authentication for mobile applications," in *Proceedings of the Industrial Track of the 13th ACM/IFIP/USENIX International Middleware Conference*, ser. Middleware Industry '13. New York, NY, USA: ACM, 2013, pp. 3:1–3:6.
- [340] E. Rescorla, Diffie-Hellman key agreement method. IETF RFC 2631. Accessed in November 2015, <http://goo.gl/Eil3fS>, June 1999.
- [341] E. Barker, D. Johnson, and M. Smid, "Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography," *NIST Special Publication*, pp. 800–56A, 2007.
- [342] J. Daemen and V. Rijmen, FIPS PUB 197: Advanced Encryption Standard (AES). Accessed in November 2015 <http://goo.gl/BjL3m9>, November 2001.
- [343] M. Dworkin, "Recommendation for block cipher modes and operation," NIST Special Publication 800-38A, Accessed in November 2015, <http://goo.gl/KWuh0x>, 2001.
- [344] M. Murase, "Linear feedback shift register," February 1992, US Patent 5,090,035.
- [345] D. Whiting, R. Housley, and N. Ferguson, "Counter with CBC-MAC (CCM)," IETF RFC 3610, Accessed in November 2015, <http://goo.gl/Ea35Xt>, 2003.
- [346] J. L. Massey, G. H. Khachatrian, and M. K. Kuregian, "Nomination of SAFER+ as candidate algorithm for the Advanced Encryption Standard (AES)," *NIST AES Proposal*, 1998.
- [347] "ISO 27799:2008. Health informatics – Information security management in health using ISO/IEC 27002," Accessed in November 2015, <http://goo.gl/jDdZkn>, 2008.
- [348] "ISO 27002:2013. Information technology – Security techniques – Code of practice for information security controls," Accessed in November 2015, <http://goo.gl/u389AS>, 2013.

- [349] “Electronic Code of Federal Regulations. Title 45, Part 164 – Security and privacy,” Accessed in November 2015, <http://goo.gl/zX5mCX>, 2013.
- [350] “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,” Accessed in November 2015, <http://goo.gl/3UYfjV>, 1995.
- [351] A. Roy and S. Karforma, “Risk and remedies of e-governance systems,” *Oriental Journal of Computer Science & Technology (OJCST)*, vol. 4, no. 02, pp. 329–339, 2011.
- [352] F. Kargl, E. Lawrence, M. Fischer, and Y. Y. Lim, “Security, privacy and legal issues in pervasive eHealth monitoring systems,” in *7th International Conference on Mobile Business, ICMB '08*, July 2008, pp. 296–304.
- [353] J. Partala, N. Keraänen, M. Särestöniemi, M. Hämäläinen, J. Iinatti, T. Jämsä, J. Reponen, and T. Seppänen, “Security threats against the transmission chain of a medical health monitoring system,” in *15th IEEE International Conference on e-Health Networking, Applications & Services (Healthcom)*, 2013, pp. 243–248.
- [354] S. Kent and K. Seo, Security Architecture for the Internet Protocol. IETF RFC 4301. Accessed in November 2015 <https://goo.gl/5QcVtH>, 2005.
- [355] Bluekript, NIST Cryptographic key length recommendations. Accessed in November 2015 <http://goo.gl/BCxRWI>, 2013.
- [356] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, *The Twofish encryption algorithm: a 128-bit block cipher*. John Wiley & Sons, Inc., 1999.
- [357] W. Burr, “Selecting the Advanced Encryption Standard,” *IEEE Security and Privacy*, vol. 1(2), pp. 43–52, 2003.
- [358] R. L. Rivest, M. J. Robshaw, and Y. L. Yin, “RC6 as the AES,” in *AES Candidate Conference*, 2000, pp. 337–342.
- [359] R. Anderson, E. Biham, and L. Knudsen, “Serpent: A proposal for the advanced encryption standard,” *NIST AES Proposal*, vol. 174, 1998.
- [360] J. Jonsson and B. Kaliski, PKCS 1: RSA cryptography standard. Accessed in November 2015, <http://goo.gl/13HJ4i>, June 2002.
- [361] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” in *Advances in Cryptology*. Springer, 1985, pp. 10–18.
- [362] H. Gilbert and H. Handschuh, “Security analysis of SHA-256 and sisters,” in *Selected areas in cryptography*. Springer, 2004, pp. 175–193.
- [363] P. Barreto and V. Rijmen, “The Whirlpool hashing function,” in *First open NESSIE Workshop, Leuven, Belgium*, vol. 13, 2000, p. 14.
- [364] H. Dobbertin, A. Bosselaers, and B. Preneel, “RIPEMD-160: A strengthened version of RIPEMD,” in *Fast Software Encryption*. Springer, 1996, pp. 71–82.
- [365] D. Eastlake and P. Jones, “US Secure Hash Algorithm 1 (SHA1),” IETF RFC 3174. Accessed in November 2015 <http://goo.gl/HOIXQE>, September 2001.
- [366] D. Johnson, A. Menezes, and S. Vanstone, Standards for efficient cryptography, SEC 1: elliptic curve cryptography, version 2.0. Accessed in November 2015, <http://goo.gl/tXhz2h>, May 2009.
- [367] D. W. Kravitz, FIPS PUB 186-2: Digital Signature Standard (DSS). Accessed in November 2015 <http://goo.gl/GgSDKe>, January 2000.
- [368] W. Dai, Crypto++ 5.6.0 Benchmark. Accessed in November 2015 <http://goo.gl/XJXbtr>, 2009.
- [369] O. J. Rubio, A. Alesanco, and J. García, “Secure information embedding into 1D biomedical signals based on SPIHT,” *Journal of Biomedical Informatics*, vol. 46, no. 4, pp. 653–664, 2013.

- [370] M. Martínez-Espronceda, I. Martínez, L. Serrano, S. Led, J. D. Trigo, A. Marzo, J. Escayola, and J. García, "Implementation methodology for interoperable personal health devices with low-voltage low-power constraints," *IEEE Transactions on Information Technology in Biomedicine*, vol. 15, no. 3, pp. 398–408, 2011.
- [371] M. Martínez-Espronceda, J. D. Trigo, S. Led, H. G. Barrón-González, J. Redondo, A. Baquero, and L. Serrano, "Event-driven, pattern-based methodology for cost-effective development of standardized personal health devices," *Computer methods and programs in biomedicine*, vol. 117, no. 2, pp. 168–178, 2014.
- [372] H. Barrón-González, M. Martínez-Espronceda, J. Trigo, S. Led, and L. Serrano, "Proposal of a novel remote command and control configuration extension for interoperable Personal Health Devices (PHD) based on ISO/IEEE 11073 standard," in *36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, Aug 2014, pp. 6312–6315.
- [373] A. Alesanco and J. García, "A simple method for guaranteeing ECG quality in real-time wavelet lossy coding," *EURASIP Journal Applied Signal Processing*, vol. 2007, January 2007.
- [374] A. Alesanco and J. García, "Automatic real-time ECG coding methodology guaranteeing signal interpretation quality," *IEEE Transactions on Biomedical Engineering*, vol. 55, no. 11, pp. 2519–2527, November 2008.
- [375] G. Moody and R. Mark, "The impact of the MIT-BIH Arrhythmia Database," *IEEE Engineering in Medicine and Biology Magazine*, vol. 20, no. 3, pp. 45–50, May-June 2001.
- [376] A. Delorme and S. Makeig, "EEGLAB: an open source toolbox for analysis of single-trial EEG dynamics including independent component analysis," *Journal of Neuroscience Methods*, vol. 134, no. 1, pp. 9–21, 2004.
- [377] P. Ullsberger and A. Delorme, EEGLAB studyset. Accessed in November 2015, <http://goo.gl/fe3PZh>, September 2007.
- [378] Y. Zigel, A. Cohen, and A. Katz, "The weighted diagnostic distortion (WDD) measure for ECG signal compression," *IEEE Transactions on Biomedical Engineering*, vol. 47, no. 11, pp. 1422–1430, November 2000.
- [379] J. L. Cárdenas-Barrera, J. V. Lorenzo-Ginori, and E. Rodríguez-Valdivia, "A wavelet-packets based algorithm for EEG signal compression," *Informatics for Health and Social Care*, vol. 29, no. 1, pp. 15–27, 2004.
- [380] G. Higgins, S. Faul, R. McEvoy, B. McGinley, M. Glavin, W. Marnane, and E. Jones, "EEG compression using JPEG2000: How much loss is too much?" in *2010 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, September 2010, pp. 614–617.
- [381] A. Panayides, M. Pattichis, C. Pattichis, C. Loizou, M. Pantziaris, and A. Pitsillides, "Atherosclerotic plaque ultrasound video encoding, wireless transmission, and quality assessment using H.264," *IEEE Transactions on Information Technology in Biomedicine*, vol. 15, no. 3, pp. 387–397, May 2011.
- [382] "ITU-R recommendation BT.601-7: studio encoding parameters of digital television for standard 4:3 and wide-screen 16:9 aspect ratios," Accessed in November 2015, <http://goo.gl/ZL4z5p>, 2011.
- [383] T. Helleseth, "Golomb's randomness postulates," in *Encyclopedia of Cryptography and Security*. Springer, 2011, pp. 516–517.
- [384] L. M. Adleman and H. W. Lenstra, "Finding irreducible polynomials over finite fields," in *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, ser. STOC. ACM, 1986, pp. 350–355.
- [385] F. Ono, W. Rucklidge, R. Arps, and C. Constantinescu, "JBIG2-the ultimate bi-level image coding standard," in *Proceedings of the International Conference on Image Processing*, vol. 1, 2000, pp. 140–143.
- [386] J. L. Muñoz, J. Forné, and J. C. Castro, "Evaluation of certificate revocation policies: OCSP vs. overissued-CRL," in *Proceedings 13th International Workshop on Database and Expert Systems Applications*. IEEE, 2002, pp. 511–515.
- [387] "DICOM sample image sets, provided by OsiriX DICOM Viewer," Accessed in November 2015, <http://goo.gl/Yuwd40>, 2013.

- [388] R. W. Hamming, "Error detecting and error correcting codes," *Bell System technical journal*, vol. 29, no. 2, pp. 147–160, 1950.
- [389] Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, April 2004.
- [390] "Z. Wang, Software implementations of the SSIM index for image quality assessment," Accessed in November 2015, <http://goo.gl/VNVTUe>, 2011.
- [391] R. Bose and D. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Information and Control*, vol. 3, no. 1, pp. 68–79, 1960.
- [392] C. E. Shannon, "Communication theory of secrecy systems\*," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [393] T. Kalker, "Considerations on watermarking security," in *IEEE Fourth Workshop on Multimedia Signal Processing*, 2001, pp. 201–206.
- [394] T. H. N. Le, K. H. Nguyen, and H. B. Le, "Literature survey on image watermarking tools, watermark attacks and benchmarking tools," in *Second International Conferences on Advances in Multimedia*, 2010, pp. 67–73.
- [395] M. Tanha, S. Torshizi, M. Abdullah, and F. Hashim, "An overview of attacks against digital watermarking and their respective countermeasures," in *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, June 2012, pp. 265–270.
- [396] A. F. Martins, D. F. Santos, A. Perkusich, and H. O. Almeida, "IEEE 11073 and connected health: Preparing personal health devices for the Internet," in *IEEE International Conference on Consumer Electronics (ICCE)*, 2014, pp. 274–275.
- [397] Y. F. Gomes, D. F. Santos, H. O. Almeida, and A. Perkusich, "Integrating MQTT and ISO/IEEE 11073 for health information sharing in the Internet of Things," in *IEEE International Conference on Consumer Electronics (ICCE)*, 2015, pp. 200–201.