Preserving data integrity of encoded medical images: the LAR compression framework

Marie Babel, François Pasteau, Clément Strauss, Maxime Pelcat, Laurent Bédat, Médéric Blestel, Olivier Déforges

Preserving data integrity of encoded medical images: the LAR compression framework

Marie Babel, François Pasteau, Clément Strauss, Maxime Pelcat, Laurent Bédat, Médéric Blestel, Olivier Déforges

Abstract Through the development of medical imaging systems and their integration into a complete information system, the need for advanced joint coding and network services becomes predominant. PACS (Picture Archiving and Communication System) aims to acquire, store and compress, retrieve, present and distribute medical images. These systems have to be accessible via the Internet or wireless channels. Thus protection processes against transmission errors have to be added to get a powerful joint source-channel coding tool. Moreover, these sensitive data require confidentiality and privacy for both archiving and transmission purposes, leading to use cryptography and data embedding solutions.
This chapter introduces data integrity protection and developed dedicated tools of content protection and secure bitstream transmission for medical encoded image purposes. In particular, the LAR image coding method is defined together with advanced securization services.

1 Introduction

Nowadays, easy-used communication systems have emphasized the development of various innovative technologies including digital image handling, such as digital cameras, PDAs or mobile phones. This naturally leads to implement image compression systems used for general purposes like digital storage, broadcasting and display. JPEG, JPEG 2000 and now JPEG XR have become international standards for image compression needs, providing efficient solutions at different complexity levels. Nevertheless, if JPEG 2000 is proved to be the most efficient coding scheme, its intrinsic complexity prevents its implementation on embedded systems that are limited in terms of computational capacity and/or memory. In addition, usages asso-

Marie Babel
European University of Brittany (UEB), France - INSA, IETR, UMR 6164, F-35708 RENNES
e-mail: marie.babel@insa-rennes.fr

ciated with image compression systems are evolving, and tend to require more and more advanced functionalities and services that are not always well addressed by current norms. As a consequence, designing an image compression framework still remains a relevant issue.

The JPEG committee has started to work on new technologies to define the next generation of image compression systems. This future standard, named JPEG AIC (Advanced Image Coding), aims at defining a complete coding scheme able to provide advanced functionalities such as lossy to lossless compression, scalability, robustness, error resilience, embed-ability, content description for image handling at object level.

However, the JPEG committee has decided to first support solutions adapted to particular applications. A call of proposal has been then issued, within the framework of JPEG AIC, and restricted to medical image coders.

Indeed, the introduction of medical imaging management systems to hospitals (PACS : Picture Communication and Information System) is leading to the design of dedicated information systems to facilitate the access to images and provide additional information to help to exploit and understand them. Implementing PACS requires an ad hoc protocol describing the way images are acquired, transferred, stored and displayed. DICOM (Digital Image Communications Management) provides a standard that specifies the way in which to manage these images [31].

The need for efficient image compression quickly becomes apparent. In particular, dataset size is exploding, because of the evolution of medical image acquisition technology together with changes in medical usage [20, 19]. From the compression point of view, the challenge lies in finding coding solutions dedicated to the storage or communication of images and associated information that will be compliant with the memory and computation capacities of the final workstations.

The design of a new medical image compression scheme requires many dedicated services. Medical images usually go with private metadata that have to remain confidential. In particular, to insure reliable transfers, flexible and generic scheduling and identification processes have to be integrated for database distribution purposes to take account of secure remote network access together with future developments in network technologies. Fast browsing tools, including the segmentation process and scalability, are therefore needed.

In this context, we propose the Locally Adaptive Resolution (LAR) codec as a contribution to the relative calls for technologies. The LAR method relies on a dedicated quadtree content-based representation that is exploited for compression purposes. Multiresolution extensions have been developed and have shown their efficiency, from low bit rates up to lossless image compression. In particular, the scalable LAR coder outperforms state-of-the-art solutions as a lossless encoder system for medical images.

An original hierarchical self-extracting region representation has also been elaborated: a segmentation process is automatically run at both coder and decoder using the quadtree knowledge as segmentation cues. This leads to a free segmentation representation well adapted for image handling and encoding at region level. Moreover,

the inherent structure of the LAR codec can be used for advanced functionalities such as content securization purposes. In particular, hierarchical selective encryption techniques have been adapted to our coding scheme and data hiding system based on the LAR multiresolution description allows efficient content protection. In this study, we show the specific framework of our coding scheme for data integrity preservation purposes, both in terms of metadata embedding and secure transmission.

This chapter does not aim at providing an exhaustive state-of-the-art study, but tends to present a content-based coding solution as a response to the medical needs in terms of data integrity preservation. Theses needs are progressively introduced and illustrated all along this chapter. To first understand the different ways to protect content in an image, section 2 introduces first cryptography and data embedding processes. Section 3 looks into securization processes of coded image transmission, where the Long Term Evolution (LTE) use case is presented. Then section 4 shows the LAR medical framework together with its dedicated functionalities.

2 How to protect content in an image?

Huge amount of medical data are stored on different media and are exchanged over various networks. Often, these visual data contain private, confidential or proprietary informations. As a consequence, techniques especially designed for these data are required so that to provide security functionalities such as privacy, integrity, or authentication. Multimedia security is aimed towards these technologies and applications [15].

Despite of the spectacular increase in the Internet bandwidth and the low cost of high storage capacity, compression rates of image codec are still of interest. In this way, an image codec must provide both compression efficiency and additional services. These services are content protection and data embedding. In one hand, content protection consists in preserving data integrity and masking data content. The commonly used methods to obtain these protections are respectively hashing and ciphering. In the other hand, the embedding of hired data aims to protect copyrights or add metadata to a document.

Besides watermarking, steganography, and techniques for assessing data integrity and authenticity, providing confidentiality and privacy for visual data is among the most important topics in the area of multimedia security. Applications range from digital rights management to secured personal communications, such as medical materials.

In this section, basic concepts of image encryption and steganography are given.

2.1 Cryptography

In many situations, there is a strong need for security against unauthorized interpretation of coded data. This secrecy requirement is in fact an imperative functionality that has to be found within medical field when communicating medical information over any untrusted medium.

One of the techniques for ensuring privacy of sensitive data is Cryptography. Cryptography aims at protecting data from theft or alteration and can be also used for user authentication. Three types of cryptographic schemes are typically developed: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. A complete survey of cryptography principles and techniques has been realized in [7].

This section is dedicated to joint cryptography and image coding frameworks.

2.1.1 Cryptography and images

Contrary to classical encryption [59], security may not be the most important aim for an encryption system devoted to images. Depending on the type of applications, other properties (such as speed or bitstream compliance after encryption) might be equally important. In that context, naive or hard encryption consists of putting in the whole image data bitstream into a standard encryption system, without taking care of its nature. However, considering the typical size of a digital image compared to a text message, the naive algorithm usually cannot meet the speed requirements for real-time digital image processing or transmission applications. In contrast, soft or selective encryption trades off security for computational complexity. They are designed to protect multimedia content and fulfil the security requirements for a particular multimedia application.

Research is focused on fast encryption procedures specifically designed to the targeted environment. There are two levels of security for digital image encryption: low level and high-level security encryption. In low-level security encryption, the encrypted image shows degraded visual quality compared to the original one, but the content of the image remains still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable to the viewers at all.

In order to make databases of high resolution images, such as medical or art pictures, accessible over the Internet, advanced functionalities combining scalability and security have to be both integrated. Indeed, scalability is a way to make database browsing easier and allow interactivity, thanks to a specific hierarchical organization of data. As for the confidentiality and privacy of visual data, both are obtained from a dedicated encryption process [70, 27]. The joint use of the two concepts aims at providing hierarchical access to the data, through a protection policy dependant on the levels of hierarchy.

On the other hand, selective encryption techniques process only parts of the compressed data, enabling low computational solutions [3-4]. In spite of the low amount of encrypted data, without the knowledge of the encryption key, the decoding stage only reconstructs noisy images.

2.1.2 Selective cryptography

Because of the large medical image sizes, dedicated scalable encoders have been defined, typically JPEG2000 and SPIHT. Accordingly, encryption processes should also be scalable in terms of level security. Equivalent issue has been described to address IPTV secure transmission problem [37].

Selective encryption [71] thus aims at avoiding the encryption of all bits of a digital image and yet ensuring a secure encryption. The key point is to encrypt only a small part of the bitstream. Consequently, the amount of encrypted data, especially when images are losslessly coded, still remains low in comparison to the global bitstream. The complexity associated with this technique is then naturally low.

The canonical framework for selective encryption has been modeled by Vandroogenbroeck et al [71] and is shown on figure 1.a. The image is first compressed. Afterwards, the algorithm only encrypts part of the bitstream with a well-proven ciphering technique: incidentally, a message (a watermark) can be added at this step. To ensure full compliance with any decoder, the bitstream should only be altered at carefully chosen places. With the decryption key, the receiver decrypts the bitstream and decompresses the image. When the decryption key is unknown, the receiver will still be able to decompress the image, but this image will significantly differs from the original, as depicted in figure 1.b.

Methods for selective encryption [74] proposed recently include DCT-based methods, Fourier-based methods, SCAN-based methods, chaos-based methods and quadtree-based methods. These methods have to be fast to meet the applications requirements and try to keep the compression ratio as good as without encryption.

A complete overview on this topic can be found in [43].

2.2 Data hiding and image coding

Data hiding aims at hiding covert information into a given content. From this matter of fact, two main solutions can be used: steganography and watermarking. Steganography is the process of hiding a secret message, in such a way that an eavesdropper cannot detect the presence hiden data. As for watermarking, it achieves embedding information process into an image so that the message remains difficult to remove [30].

Steganography methods usually do not need to provide strong security against removing or modification of the hidden message. Watermarking methods need to to be very robust to attempts to remove or modify a hidden message.

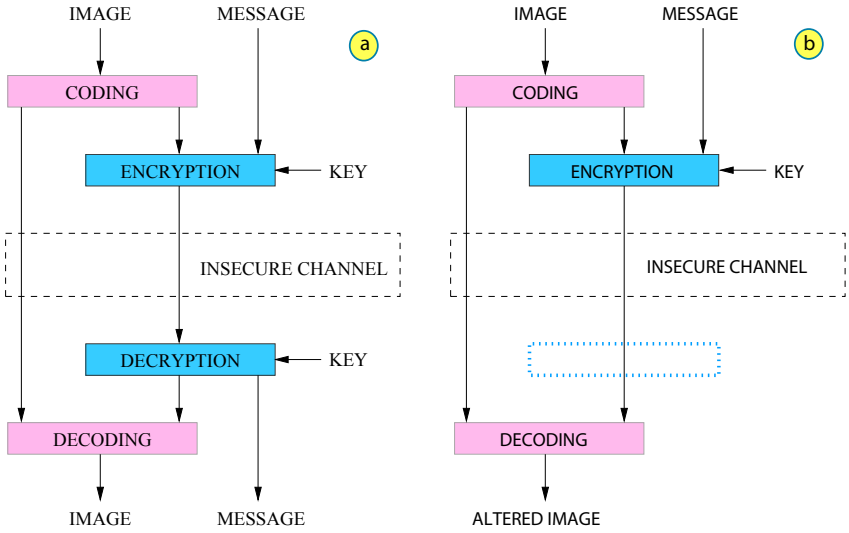


Fig. 1 Selective encryption / decryption mechanism with (a) or without (b) encryption key

The security associated to data hiding remains a key issue. Within the watermark only attack (WOA) framework, robust solutions have been discussed, in particular when using secure spread-spectrum watermarking [44]. Security aspects will not be developed in this section.

Data embedding hides data (i.e. the payload) in a digital picture so that to be as unnoticeable as possible. For that purpose, image quality should be high after data embedding. The measurement of data embedding algorithm performances is done using three criteria [66]: first, the payload capacity limit, i.e. the maximal amount of data that can be embedded, then visual quality, to measure the distortions introduced by the algorithm, and, at least, complexity, or the computational cost of the algorithm.

In order to fulfill these requirements, techniques have been developed both in the direct domain or in a transformed domain. These latter are both described in following sections.

In terms of pedagogical supports, readers can refer to [17], where lecture notes and associated software are available.

2.2.1 Data embedding in the direct domain

Pixel-based methods rely on pixel modification following specific patterns. The first technique of data embedding consists of modifying the LSB (Least Significant Bit) of pixels in the picture [14]. It has good capacity-distortion performance but with the major drawback of being fragile.

Another solution consists of using patchwork as a statistical approach [14]. Selected pixels are divided in two groups and are modified depending on the group they belong to, in order to respect a specific pattern. The detection uses the difference between mean of pixel values in this two groups. Another kind of methods uses fractal code modification by adding similarities in the image [13]. This method is adapted to watermarking (detection), and is robust to JPEG compression (better robustness with DCT use) but not to geometrical attacks.

Recent developments take into account block structures so that to be fully compliant with standard image and video codecs [40].

2.2.2 Data embedding in the transformed domain

Most of data hiding techniques use the transformed domain, and especially the frequency one. As a matter of fact, the Fourier Transform has very interesting properties of invariance under geometrical transformations [58]. The spread spectrum technique applies successively a FFT (Fast Fourier Transform) and then a FMT (Fourier-Mellin Transform) on the image to reveal invariant areas. Then the payload is spreaded over these areas, which can be either in the amplitude [58] or in the phase [57] of the image.

The frequency domain can be obtained by the DCT (Discrete Cosine Transform). A blind method using DCT coefficients inversion produces quite good invisibility but bad robustness. Ciphered data can also be inserted in DCT coefficients by addition [75]. The problem is that block-based DCT has inner sensitivity to geometrical modifications. Nevertheless, the spread spectrum technique combined to DCT (instead of FFT) shows efficiency and robustness against geometrical attacks [21].

Joint compression-insertion remains a key issue. Corresponding methods are classically frequency-based methods using the transformation performed by the still image coder. As an example, JPEG2000 is based on the DWT (Discrete Wavelet Transform), and dedicated watermarking frameworks appeared. One consists in inserting pseudo-random watermark [73, 36] by addition to the largest coefficients in the subbands. This DWT watermark approach is robust to many distortions like compression, large variance additive noise and resolution reduction, whereas DCT is not [45]. Recent studies based on Human Visual System present solution relied on a tradeoff between invisibility and robustness [61, 5].

Many other methods exist, like watermarking using the DLT [32] (Discrete Laguerre Transform) instead of DCT, with almost the same results, the Fresnel transform [42] (like FFT, but with a multichannel approach), and also data hiding using the IHWT [67] (Integer Haar Wavelet Transform, also called S-Transform) that insert one bit using two integers. Papers based on more complex approaches such as the quaternion Fourier transforms [69] have also demonstrated their efficiency at the expense of algorithm complexity.

3 Secure transmission of encoded bitstreams

Through the development of PACS (Picture Archiving and Communication Systems), health care systems have come to rely on digital information. Furthermore, future medical applications will have to integrate access to generalized databases that contain the personal medical information of each patient. Efficient image management consequently becomes a key issue in designing such a system. Given this situation, two main elements must be considered at the same time: compression and security strategies specific to image handling [51].

Naturally, teleradiology systems integrate the notion of security [63]. In particular, they must guarantee the integrity (to prevent the alteration of data), authentication (to check the sender) and the confidentiality (to prevent unauthorized access) of the medical data at all times. The availability of the information can be ensured by the Internet Protocol (IP). Moreover, wireless transmissions play an increasingly important part in the achievement of this goal, [55, 54, 72] especially in the context of emergency medicine [35, 18]. However, this access to information must be accompanied by security primitives. Typically, for privacy and authentication purposes, the traditional security solutions integrated in the DICOM standard cover encryption processes and digital signatures [53].

In this section, both robust wireless transmission and IP networks are tackled. Classic error resilience tools used as channel coding features are first described. IP packets loss compensation issue is then addressed. Finally, the Long Term Evolution (LTE) telecommunication standard is described as an application case of the latter content protection solution.

3.1 Error resilience and channel coding

Commonly, robust wireless transmission can be achieved through the use of error resilience processes at both source and channel coding. At the source coding side, the entropy coder is often the less robust part of the coder. When using arithmetic entropy coder such as MQ coder used in JPEG2000 format, a single bitshift in the bitstream is enough to create important visual artefacts at the decoding side. Therefore to ensure a proper decoding of the bitstream, different kinds of markers need to be added. First, to prevent the decoder from desynchronizing and therefore error from propagating, synchronisation markers needs to be added. Moreover, specific error detection markers can be used to detect errors during decoding and discard bitstreams affected by this error. Such synchronization and error detection markers have already been implemented as SEGMARK, ERTERM and RESTART markers in the JPEG2000 codec [64] as well as in the LAR codec.

At the channel coding side, error robustness is achieved by using error correcting codes, such as Reed Solomon [56] and convolutive codes [26]. Such error correcting codes add redundant data in the bitstream in order to detect and possibly

correct transmission errors. Depending on the channel characteristics, error correcting codes have to be tuned to achieved good performance in error correction while keeping a small amount of redundant data. These error correcting codes are usually computationnally expensive and fast codes like LDPC and turbo codes can often be used instead.

As described above, at both source and channel coding, error resilience is performed by adding extra data to the bitstream. Such overhead has to be taken in consideration while performing image compression and has to remain as low as possible to maintain an acceptable bit rate.

VCDemo software [62] can be used to illustrate how transmission errors impact the visual quality of decoded images and videos. It contains JPEG and JPEG2000 image codecs as well as MPEG2 and H264 video codecs. Some error correcting mechanisms can be used and their impact on image quality can be observed.

3.2 IP packets securization processes

Very few works cover the loss of entire IP packets in medical data transmissions [48]. In a more general framework such as image transmission, most studies relate to the implementation of error control coding e.g. Reed-Solomon codes to compensate for packet loss by avoiding retransmissions [48, 24].

By adjusting the correction capacities and, thus, the rates of redundancy, it is possible to adapt to both a scalable source and an unreliable transmission channel. This is the purpose of Unequal Error Protection (UEP) codes which are now mature and proposed in standardization processes [25]. The specific problem of medical image integrity is very often the volume of the data being transmitted (cf lossless coding, 3D-4D acquisition etc.). Within this framework, UEP must meet algorithmic complexity requirements to satisfy real time constraints.

Roughly speaking, the most important part of the image is more protected by redundant information than non significant data. Figure 2 illustrates the associated framework. From image coding process, both bitstream data and codec properties are available for an advanced analysis stage. Then, a hierarchy can be extracted from the bitstream, so that the UEP strategy stage can add adequate redundancy. As a consequence, fine granularity can be obtained for good adaptation both to the hierarchy of the image and to the channel properties as joint source channel coding.

A great deal of research work has been done in this area over the past decade. In particular, the working draft of JPEG2000 WireLess (JPWL) [25] proposes concentrated unequal protection on the main header and the tile header with the characteristic that any error on these part of the stream is fatal for decoding. In this solution, conventional Reed-Solomon error correction codes are applied to a symbol level to provide protection [24]. A very strong protection obviously improves the chances of success in decoding when binary losses occur but it also guarantees the integrity of the headers whether the properties of the channel are good or very bad. Furthermore,

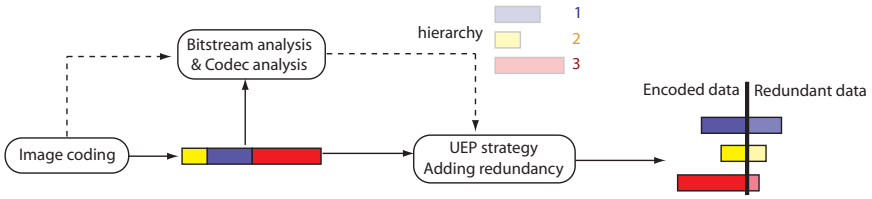


Fig. 2 UEP principles: hierarchy and redundancy

performance evaluation and protection on a symbol level are far removed from the real channels like wireless channels as can be seen for example through the variations in the protocol IEEE802.xx (WLAN or WiMax). Typically, these standards are divided into 7 layers according to the Open Systems Interconnection (OSI) model description, as depicted on figure 3. More precisely, the approach never considers the effectiveness of the mechanisms operated on the level of Media Access Control (MAC) layer and physical (PHY) layer such as the Hybrid ARQ (Automatic Query Request - H-ARQ) combining efficient channel coding (turbo-code) and retransmission. Likewise, the working draft does not consider the exploratory research carried out over the past ten years on unequal error protection [6] or the new representations based on a multiple description of information [39]. Classically, when designing joint source-channel coding UEP schemes, we consider the PHY and MAC layers as effective to deliver true symbols so as to focus all our attention of unequal protection at the transmission unit level *i.e* the packet level.

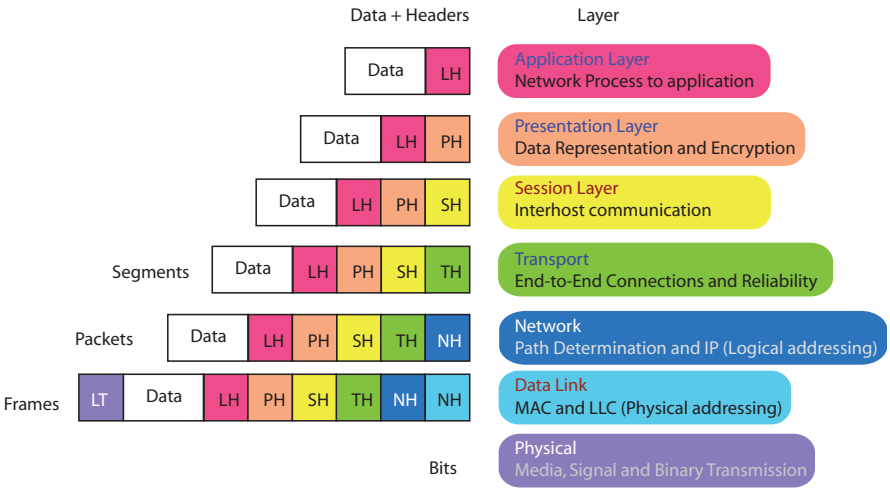


Fig. 3 Open Systems Interconnection (OSI) model description: 7 layers

3.3 LTE standard application case: securization process for advanced functionalities

Nowadays, wireless communications and their applications are undergoing major expansion and they have captured media attention as well as the imagination of the public. However, wireless channels are known to generate a high number of errors which perturb complex multimedia applications such as image or video transmission. For these reasons, designing a suitable system for image transmission over wireless channel remains a major issue. In particular, if the new telecommunication standard, namely the LTE (Long Term Evolution) one, proposes advanced functionalities, it requires accurate securization processes so that to ensure sufficient end-to-end Quality Of Service whatever the transmission conditions are.

3.3.1 Evolution of telecommunication standards

Terrestrial mobile telecommunications started in the early 1980s using various analog systems developed in Japan and Europe. The Global System for Mobile communications (GSM) digital standard was subsequently developed by the European Telecommunications Standards Institute (ETSI) in the early 1990s. Available in 219 countries, GSM belongs to the second generation mobile phone system. It can provide an international mobility to its users by using inter-operator roaming. The success of GSM promoted the creation of the Third Generation Partnership Project (3GPP), a standard-developing organization dedicated to supporting GSM evolution and creating new telecommunication standards, in particular a Third Generation Telecommunication System (3G) [52].

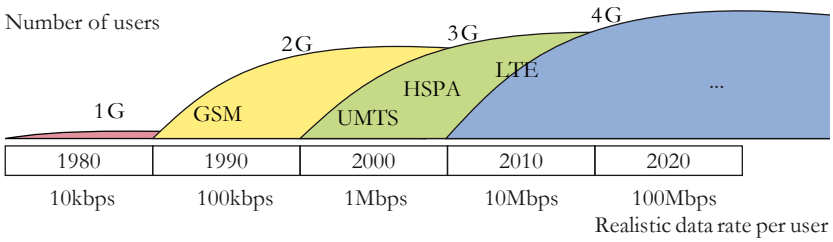


Fig. 4 3GPP Standard Generations

The existence of multiple vendors and operators, the necessity of interoperability when roaming and limited frequency resources justifies the use of unified telecommunication standards such as GSM and 3G. Each decade, a new generation of standards multiplies the data rate available to its user by ten (Figure 4). The driving force behind the creation of new standards is the radio spectrum which is an expensive resource shared by many interfering technologies. Spectrum use is coordinated by ITU-R (International Telecommunication Union, Radio Communication Sector),

an international organization which defines technology families and assigns their spectral bands to frequencies that fit the International Mobile Telecommunications (IMT) requirements. 3G systems including LTE are referred to as ITU-R IMT-2000.

Radio access networks must constantly improve to accommodate the tremendous evolution of mobile electronic devices and internet services. Thus, 3GPP unceasingly updates its technologies and adds new standards. Universal Mobile Telecommunications System (UMTS) is the first release of the 3G standard. Evolutions of UMTS such as High Speed Packet Access (HSPA), High Speed Packet Access Plus (HSPA+) or 3.5G have been released as standards. The 3GPP Long Term Evolution (LTE) is the 3GPP standard released subsequent to HSPA+. It is designed to support the forecasted ten-fold growth of traffic per mobile between 2008 and 2015 [52] and the new dominance of internet data over voice in mobile systems. The LTE standardization process started in 2004 and a new enhancement of LTE named LTE-Advanced is currently being standardized.

A LTE terrestrial base station computational center is known as an evolved NodeB or **eNodeB**, where a NodeB is the name of a UMTS base station. An eNodeB can handle the communication of a few base stations, with each base station covering a geographic zone called a cell. The user mobile terminals (commonly mobile phones) are called User Equipment (**UE**). At any given time, a UE is located in one or more overlapping cells and communicates with a preferred cell; the one with the best air transmission properties. LTE is a duplex system, as communication flows in both directions between UEs and eNodeBs. The radio link between the eNodeB and the UE is called the downlink and the opposite link between UE and its eNodeB is called uplink. These links are asymmetric in data rates because most internet services necessitate a higher data rate for the downlink than for the uplink.

LTE also supports data broadcast (television for example) with a spectral efficiency over 1 bit/s/Hz. The broadcasted data cannot be handled like the user data because it is sent in real-time and must work in worst channel conditions without packet retransmission.

3.3.2 LTE Radio Link Protocol Layers

The information sent over a LTE radio link is divided in two categories:

- the **user-plane** which provides data and control information irrespective of LTE technology,
- the **control-plane** which gives control and signaling information for the LTE radio link.

The protocol layers of LTE are displayed in Figures 5 and 6. User plane and control plane significantly differ but the lower layers remain common for both planes. Both figures associate a unique OSI Reference Model number to each layer. Layers 1 and 2 have identical functions in control-plane and user-plane even if parameters

differ (for instance, the modulation constellation). Layers 1 and 2 are subdivided into different layers that require adapted securization processes, both in terms of **content protection** and **error resilience tools**.

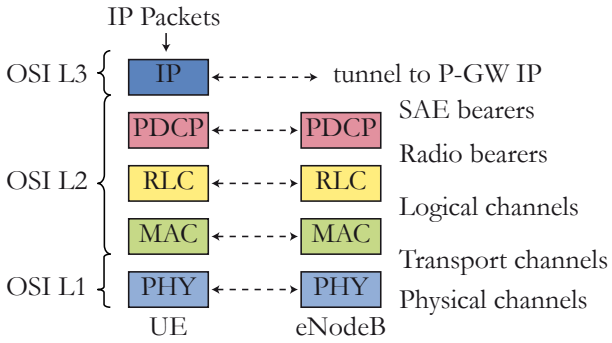


Fig. 5 User plane: Protocol Layers of LTE Radio Link

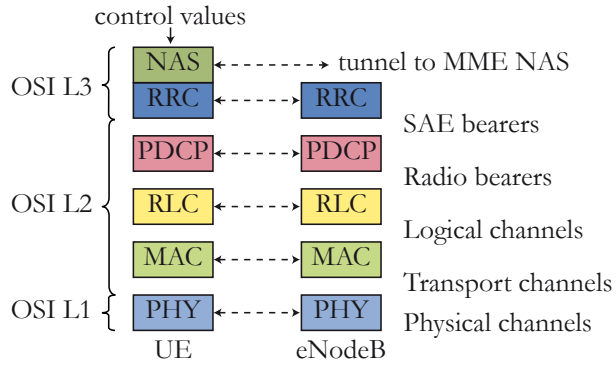


Fig. 6 Control plane: Protocol Layers of LTE Radio Link

In particular, the physical layer organization of the LTE standard is illustrated on Figure 7. It corresponds to the Release 9 LTE physical layer in the eNodeB, i.e. the signal processing part of the LTE standard that 3GPP finalized in December 2009. The physical layer, OSI layer 1, uplink and downlink baseband processing must share the eNodeB digital signal processing resources. The downlink baseband process is itself divided into channel coding that prepares the bit stream for transmission and symbol processing that adapts the signal to the transmission technology. The uplink baseband process performs the corresponding decoding. The OSI layer 2 controls the physical layer parameters.

The role of each layer is defined as follows:

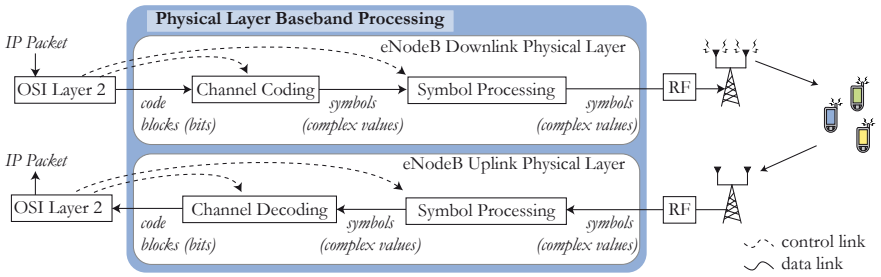


Fig. 7 LTE PHY layer overview (OSI L1)

- **PDCP layer** [4] or layer 2 Packet Data Convergence Protocol is responsible for data ciphering and IP header compression to reduce the IP header overhead.
- **RLC layer** [3] or layer 2 Radio Link Control performs the data concatenation and then generates the segmentation of packets from IP-Packets of random sizes which comprise a Transport Block (TB) of size adapted to the radio transfer. The RLC layer also ensures ordered delivery of IP-Packets; Transport Block order can be modified by the radio link. Finally, the RLC layer handles a retransmission scheme of lost data through a first level of **Automatic Repeat reQuests** (ARQ).
- **MAC layer** [2] or layer 2 Medium Access Control commands a low level retransmission scheme of lost data named Hybrid Automatic Repeat reQuest (HARQ). The MAC layer also multiplexes the RLC logical channels into HARQ protected transport channels for transmission to lower layers. Finally, the MAC layer contains the scheduler, which is the primary decision maker for both downlink and uplink radio parameters.
- **Physical layer (PHY)** [1] or layer 1 comprises all the radio technology required to transmit bits over the LTE radio link. This layer creates physical channels to carry information between eNodeBs and UEs and maps the MAC transport channels to these physical channels.

Layer 3 differs between control and user planes. Control plane handles all information specific to the radio technology while the User plane carries IP data from system end to system end. More information can be found in [22] and [60].

The LTE system exhibits a high reliability while limiting the error correction overhead. Indeed it uses two level of error concealment; HARQ and ARQ. HARQ is employed for frequent and localized transmission errors while ARQ is used for rare but lengthy transmission errors. The retransmission in LTE is determined by the target service: LTE ensures different **Qualities of Service** (QoS) depending on the target service. For instance, the maximal LTE-allowed packet error loss rate is 10^{-2} for conversational voice and 10^{-6} for transfers based on TCP (Transmission Control Protocol). The various QoS imply different service priorities. For example during a TCP/IP data transfer, the TCP packet retransmission system adds a third error correction system to the two LTE ARQs.

The physical layer manipulates bit sequences called Transport Blocks. In the user plane, many block segmentations and concatenations are processed layer after layer

between the original data in IP packets and the data sent over air transmission. Figure 8 summarizes these block operations. Evidently, these operations do not reflect the entire bit transformation process including ciphering, retransmitting, ordering, and so on.

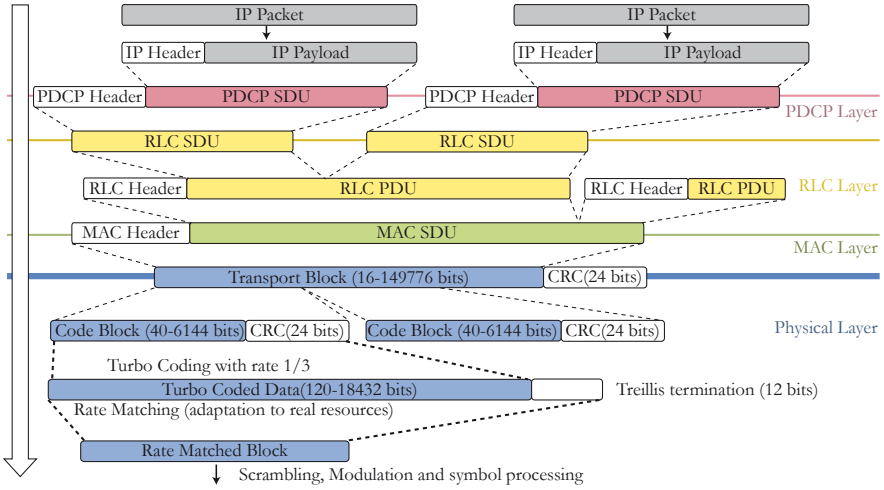


Fig. 8 Data Blocks Segmentation and Concatenation

A very interesting implementation of a LTE simulator has been developed by TU Wien's Institute of Communications and Radio Frequency Engineering [46] and can be download on the laboratory's web site. The simulators are released under the terms of an academic, non-commercial use license.

The LTE provides a transmission framework with efficient error resilience mechanisms. However, recent researches have been more focused on complete joint source-channel coding scheme so that to ensure an even higher QoS. Typically, since error can remain from the transmission, the source codec must also contain error concealment mechanisms.

4 Application example: LAR medical framework

PACS-based systems tend to manage secure and heterogeneous networks such as wire and / or wireless ones, together with innovative image compression schemes. The design of a new medical image compression scheme requires then many dedicated services. Medical images usually go with private metadata that have to remain confidential. In particular, to insure reliable transfers, flexible and generic scheduling and identification processes have to be integrated for database distribution purposes to take account of secure remote network access together with future devel-

opments in network technologies. Fast browsing tools, including the segmentation process and scalability, are therefore needed.

This is the background against which IETR Laboratory proposes the content-based Locally Adaptive Resolution (LAR) codec. The LAR method has already been proposed as a response to the call for contributions of technologies [9, 10] within the JPEG committee. In this section, we focus on LAR medical image processing, and give some specific uses allowed by our compression systems. The LAR coding scheme can be seen as a package of coding tools aiming at different levels of user services. In this context, we focus on a specific scheme called Interleaved S+P and its associated data protection tools.

4.1 LAR codec overview

The LAR method was initially introduced for lossy image coding [23]. The philosophy behind this coder is not to outperform JPEG2000 in compression; the goal is to propose an open source, royalty free, alternative image coder with integrated services. While keeping the compression performances in the same range as JPEG2000 or JPEG XR, but with lower complexity, our coder also provides services such as scalability, cryptography, data hiding, lossy to lossless compression, region of interest, free region representation and coding. In this paragraph, we focus on content protection features.

The LAR codec is based on the assumption that an image can be represented as layers of basic information and local texture, relying then on a two-layer system (Figure 9). The first layer, called Flat coder, leads to construct a low bit-rate version of the image with good visual properties. The second layer deals with the texture that is encoded through a texture coder through DCT-based system (spectral coder) or pyramidal system, aiming at visual quality enhancement at medium/high bit-rates. Therefore, the method offers a natural basic SNR scalability.

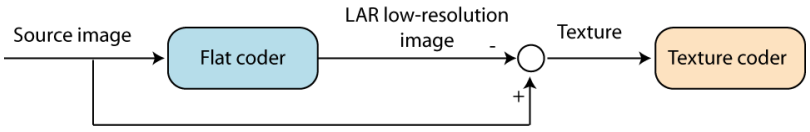


Fig. 9 General scheme of two-layer LAR coder

The LAR codec tries to combine both efficient compression in a lossy or lossless context and advanced functionalities and services. For this purpose, we defined three different profiles for user-friendly usage (Figure 10).

The baseline profile is dedicated to low bit-rate encoding. In the context of medical image compression, this profile is clearly not appropriate. As medical image compression requires lossless solutions, we then focus the discussion on functionalities and technical features provided by the pyramidal and extended profiles ded-

icated to content protection: cryptography, steganography, error resilience, hierarchical securized processes. In this context, the Interleaved S+P coding tool, based on a two interlaced pyramidal representation, is used for coding purposes [11].

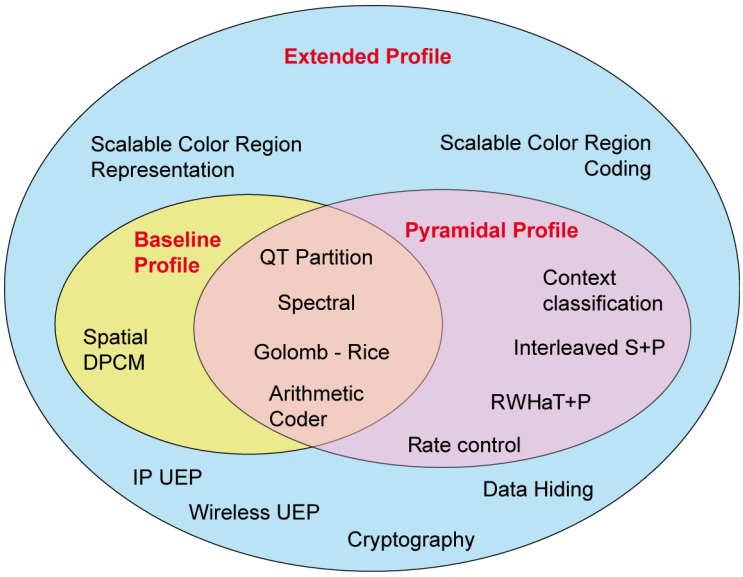


Fig. 10 Specific coding parts for LAR profiles

4.2 Principles and properties

The LAR codec relies on a two-layer system. The first layer, called FLAT coder, constructs a low bit-rate version of the image. The second layer deals with the texture that is encoded through a texture coder, aimed at visual quality enhancement at medium/high bit-rates. Therefore, the method offers a natural basic SNR scalability.

The basic idea is that local resolution, in other words pixel size, can depend on local activity, estimated through a local morphological gradient. This image decomposition into two sets of data is thus performed conditionally to a specific quadtree data structure, encoded in the Flat coding stage. Thanks to this type of block decomposition, their size implicitly gives the nature of the given block: smallest blocks are located upon edges whereas large blocks map homogeneous areas (Figure 11). Then, the main feature of the FLAT coder consists of preserving contours while smoothing homogeneous parts of the image.

This quadtree partition is the key system of the LAR codec. Consequently, this coding part is required whatever the chosen profile.

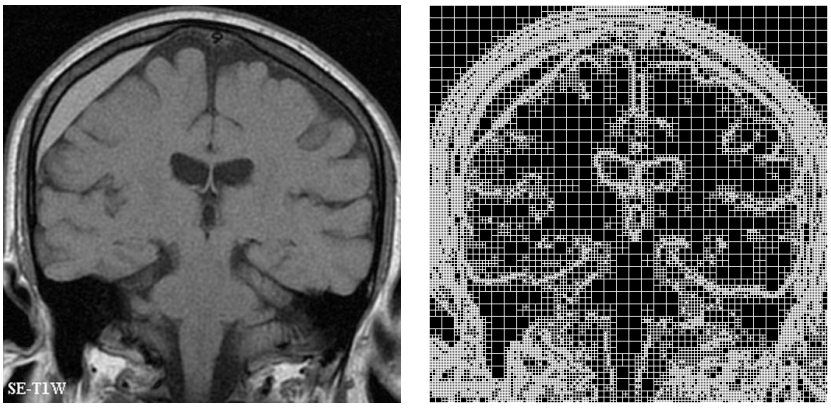


Fig. 11 Original image and associated Quadtree partitions obtained with a given value of activity detection parameter

4.2.1 Lossy to lossless scalable solution

Scalable image decompression is an important feature in the medical field, which sometimes uses very large images. Scalability enables progressive image reconstruction by integrating successive compressed sub-streams in the decoding process.

Scalability is generally first characterized by its nature: resolution (multi-size representation) and/or SNR (progressive quality enhancement). Just like JPEG2000, the LAR codec supports both of them. The main difference is that the LAR provides multiresolution ”edge oriented” quality enhancement. The lossy or lossless coding process involves two-pass dyadic pyramidal decomposition. The first pass, leading to a low bit-rate image, encodes the overall information in the image, preserving main contours, while smoothing homogeneous areas. The second pass adds the local texture in these areas as shown on Figure 12.

The second important feature for scalability concerns granularity. Scalability granularity defines which elementary amount of data can be independently decoded. Among existing standards, JPEG2000 offers the finest grain scalability. On the other hand, JPEG provides no scalability at all (except in its progressive mode), while JPEG-XR enables up to 4 scalability levels. In LAR, the number of dyadic resolution levels N is adjustable, with two quality levels per resolution. Therefore, the number of elementary scalable sub-streams is 2N.

The first pyramid pass provides an image with variable-sized blocks. LAR also contains some interpolation / post-processing steps that can smooth homogeneous areas while retaining sharp edges.

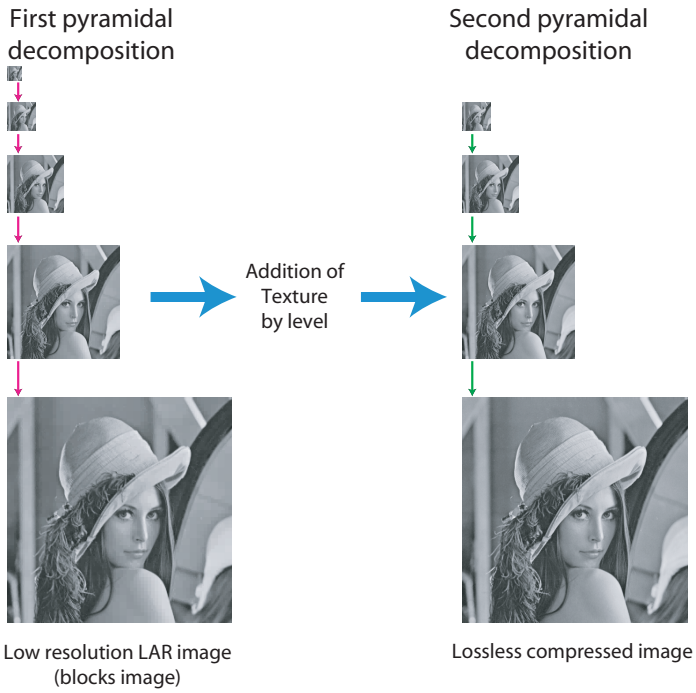


Fig. 12 Pyramidal representation of an image

4.2.2 Hierarchical colour region representation and coding

For colour images, we have designed an original hierarchical region-based representation technique adapted to the LAR coding method. An initial solution was proposed in [23]. To avoid the prohibitive cost of region shape descriptions, the most suitable solution consists of performing the segmentation directly, in both the coder and decoder, using only a low bit-rate compressed image resulting from the FLAT coder (or first partial pyramidal decomposition). Natural extensions of this particular process have also made it possible to address medium and high quality encoding and the region-level encoding of chromatic images. Another direct application for self-extracting region representation is found in a coding scheme with local enhancement in Regions Of Interest (ROI). Actual works aim at providing a fully multiresolution version of our segmentation process: indeed this region representation can be connected to the pyramidal decomposition in order to build a highly scalable compression solution.

The extended profile also proposes the use of dedicated steganography and cryptography processes, which will be presented in next sections. To sum up, the interoperability of coding and representation operations leads to an interactive coding tool. The main features of the LAR coding parts are depicted in Figure 13.

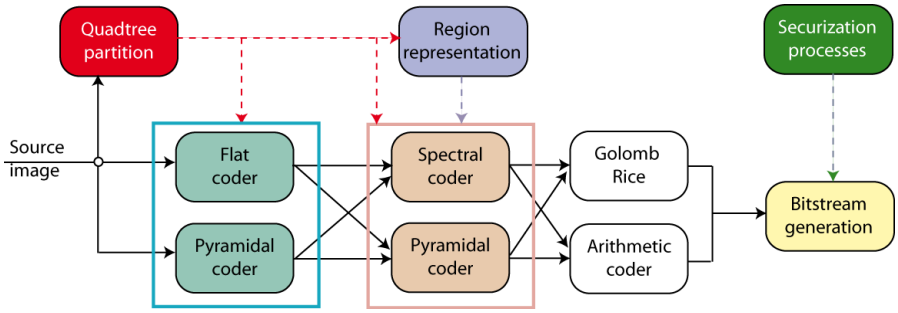


Fig. 13 Block diagram of extended LAR coder profile

4.2.3 Region and object representation

Current image and video compression standards rely only on information theory. They are based on prediction and decorrelation optimization techniques without any consideration of source content. To get higher semantic representation, Kunt first introduced the concept of second generation image and video coding [41]. It refers to content-based representation and compression at region/object level. To obtain a flexible view with various levels of accuracy, a hierarchical representation is generally used, going from a fine level comprising many regions, to a coarse level comprising only a few objects.

Regions are defined as convex parts of an image sharing a common feature (motion, textures, etc). Objects are defined as entities with a semantic meaning inside an image. For region representation, two kinds of information are necessary: shape (contours) and content (texture). For video purposes, motion constitutes a third dimension.

The region-based approach tends to link digital systems and human vision as regards image processing and perception. This type of approach provides advanced functionalities such as interaction between objects and regions, or scene composition. Another important advantage is the ability, for a given coding scheme, of both increasing compression quality on highly visually sensitive areas of images (ROI) and decreasing the compression quality on less significant parts (background). The actual limited bandwidth of channels compared to the data volume required for image transmission leads to a compromise between bit-rate and quality. Once the ROIs are defined and identified, this rate/quality bias can be not only generally but also locally adjusted for each ROI: compression algorithms then introduce only low visual distortions in each ROI, while the image background can be represented with high visual distortions.

Despite the benefits of region-based approaches in terms of high level semantic description, some limitations to common techniques have restricted their use.

The first one is the generally limited compression performances achieved, due to the region description cost: most of the existing methods suggest sending a segmentation map from the coder to the decoder. As the number of regions increases,

the overhead costs become significant. The second limitation concerns complexity: most of the existing methods rely on complex segmentation processes. Despite increasing improvements in terms of processing performance, most of the state-of-the-art region / object representation techniques are still too time consuming.

Indeed, LAR provides an unusual method for low cost region-level coding, based on the concept of self-extracting region representation. It consists of a segmentation process performed only from highly compressed images in both the coder and the decoder. This solution prevents costly transmission of the segmentation map to provide the region shapes. An original segmentation algorithm has been designed, leading to an efficient hierarchical region-based description of the image. The process ensures full compliance between the shape of regions and their content encoding. One direct issue is ROI coding: an ROI is rapidly and easily defined as a set of regions in either the coder or the decoder. Local image quality enhancement is then achieved by allowing the second pyramidal decomposition pass only for blocks inside the ROI. Another application of an ROI description is a full encryption process (see below), which can be applied only to the ROI.

The segmentation process is optional. It can be performed on-line or off-line. From a complexity point of view, the segmentation process is of low complexity compared with common segmentation techniques. The main reason is that the LAR segmentation process starts from the block-level representation, given by the quadtree, instead of elementary pixels.

As the LAR solution relies on a compromise between coding and representation, coding key issues are partially solved. In particular, the complexity of the segmentation process has been evaluated and restricted, so that it has been pipelined and prototyped onto embedded multicore system platforms [28].

To avoid the segmentation process at the decoder side, another solution consists of transmitting the binary ROI map. The corresponding cost is limited, as ROIs are described at block-level: a full region-map composed of 120 regions is encoded at around 0.07 bpp, whereas the cost of a binary ROI image, whatever the ROI shape, is less than 0.01 bpp.

JPEG2000 also proposes ROI functionalities, but its technical solution significantly differs from the LAR one. To sum up, ROI in LAR has improved features, for example:

- ROI can represent any shape,
- ROI enhancement accurately matches the shape,
- the encoding cost of the shape is insignificant (a few bytes),
- several ROIs can be defined in the same image,
- any quality ratio between ROI and background can be defined.

4.3 Content protection features

Whatever the storage or channel transmission used, medical applications require secure transmission of patient data. Embedding them in an invisible way within the image itself remains an interesting solution.

We also deal with security concerns by encrypting the inserted data. Whereas the embedding scheme can be made public, the use of a decryption key will be mandatory to decipher the inserted data.

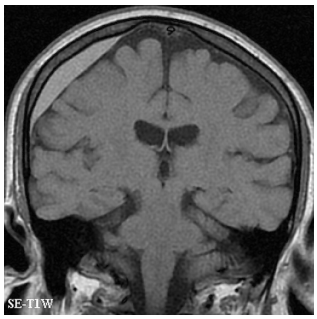
4.3.1 Steganography

Data embedding is one of the new services expected within the framework of medical image compression. It consists of hiding data (payload) in a cover image. Applications of data embedding range from steganography to metadata insertion. They differ in the amount of data to be inserted and the degree of robustness to hacking.

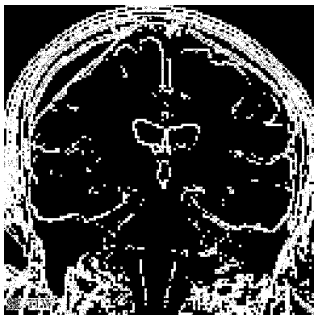
From a signal processing point of view, it uses the image as a communication channel to transmit data. The capacity of the channel for a specific embedding scheme gives the size of the payload that can be inserted. A fine balance has to be achieved between this payload and the artifacts introduced in the image. This being so, different embedding schemes are compared on a payload vs. PSNR basis. Of course, the overall visual quality can be assessed. The target application is the storage of data related to a given medical image. That data can consist of patient ID, time stamps, or the medical report, transcribed or in audio form. The idea is to avoid having to store several files about specific images by having all the necessary information directly stored within the image data.

We therefore propose a data embedding service that aims to insert a high payload in an image seen either as a cover or a carrier, such as a medical report in audio form. For this purpose, audio data, after coding and ciphering, is inserted in a corresponding medical image. The embedded image is then transmitted using usual channels. Of course, this scheme is compliant with any error protection framework that might be used. When retrieval of audio data is requested, the data embedding scheme is reversed, and both the original image and the audio data are losslessly recovered. To avoid significant perceptually distortions, the data hiding mapping is powered by the quadtree: distortions are less perceptible in homogeneous areas than upon edges as shown in figure 14.

In this context, we studied the Difference Expansion (DE) method, introduced by Tian [68] that embeds one bit per pixel pair based on S Transform. As the LAR Interleaved S+P algorithm and DE both use S-Transform during their computation, we have combined both techniques to perform the data insertion without degrading coding performance. In order to adjust the DE algorithm to LAR Interleaved S+P, some minor modifications are introduced compared with the original DE method. In particular, we power the insertion process by the quadtree partition, which means that the insertion is dependent on the image content. Another important improvement is that in the initial DE method, positions of possible ”extensible” difference

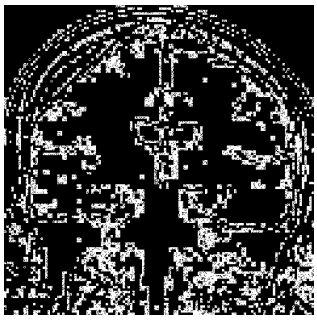


(a) 2×2 blocks, $\mathscr{P} = 19528$ bits, PSNR=35 dB

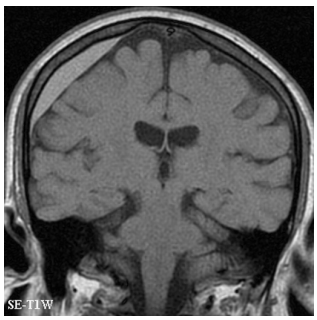


(b) 2×2 blocks

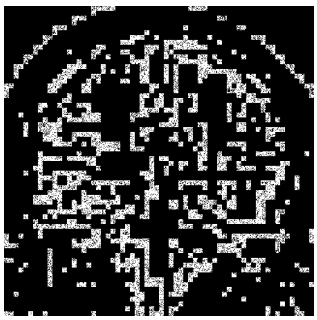
(c) 4×4 blocks, $\mathscr{P} = 29087$ bits, PSNR=44 dB



(d) 4×4 blocks



(e) 8×8 blocks, $\mathscr{P} = 27971$ bits, PSNR=48 dB



(f) 8×8 blocks

(g) 4×4 up to 16×16 blocks, $\mathscr{P} =$ 90126 bits, PSNR=42 dB

(h) 4×4 up to 16×16 blocks

Fig. 14 Visual quality versus watermarked block sizes. For each image, position of modified pixels has been extracted (in white onto black background).

have to be encoded, adding a significant overhead. In our coding scheme, these positions can be directly deduced from the quadtree, and are then not transmitted [49].

We show preliminary results on an angiography 512-squared medical image (Figure 15). A payload of 63598 bits is inserted, with a PSNR of 40 dB. Considering a 1 MP image, the payload can be up to 300 kbits. It corresponds roughly to an audio message of 200 s when using a 1.5 kbits voice compression rate. Of course, as many images are taken during the same medical examination, the length of the corresponding audio files is extended. Our embedding scheme is an efficient adaptation of a useful technique to our image coder. It performs well, allowing high payload and minimum distortion, as shown on zoomed parts of the images from the figure 15. From a compression point of view, the data hiding process does not affect the coding efficiency: the total coding cost is about equal to the initial lossless encoding cost of the source image plus the inserted payload.

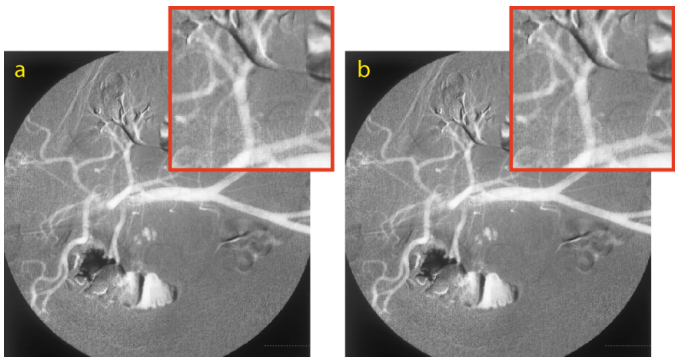


Fig. 15 a) Source image - b) Image with inserted payload

4.3.2 Cryptography

Besides watermarking, steganography, and techniques for assessing data integrity and authenticity, the provision of confidentiality and privacy for visual data is one of the most important topics in the area of multimedia security in the medical field. Image encryption lies somewhere between data encryption and image coding. Specifically, as the amount of data to be considered is several orders of magnitude greater than the amount for ordinary data, more challenges are to be dealt with. The main challenge is the encryption speed, which can be a bottleneck for some applications in terms of computation time or in terms of computer resources required. A secondary challenge is to maintain the compliance of the encrypted bitstream with the chosen image standard used to compress it. Partial encryption addresses the first aforementioned challenge. Our partial encryption scheme is based mainly on the following idea: the quadtree used to partition the image is necessary to rebuild the image. This has been backed up by theoretical and experimental work. As a result,

the quadtree partition can be considered to be the key itself, and there is no need to encrypt the remaining bitstream.

The key obtained is thus as long as usual encryption key and its security has been shown to be good. If further security is requested, the quadtree partition can be ciphered using a public encryption scheme, to avoid the transmission of an encryption key, as depicted in Figure 16 [50]. This system has the following properties: it is embedded in the original bit-stream at no cost, and allows for multilevel access authorization combined with a state-of-the-art still picture codec. Multilevel quadtree decomposition provides a natural way to select the quality of the decoded picture.

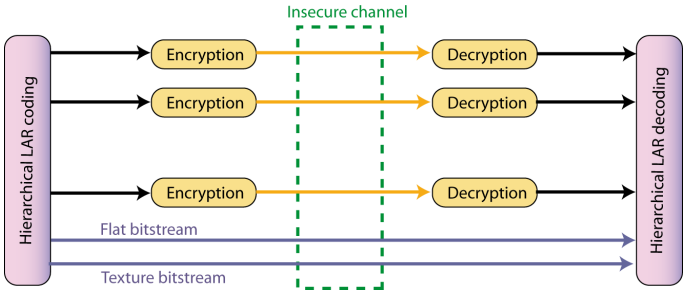
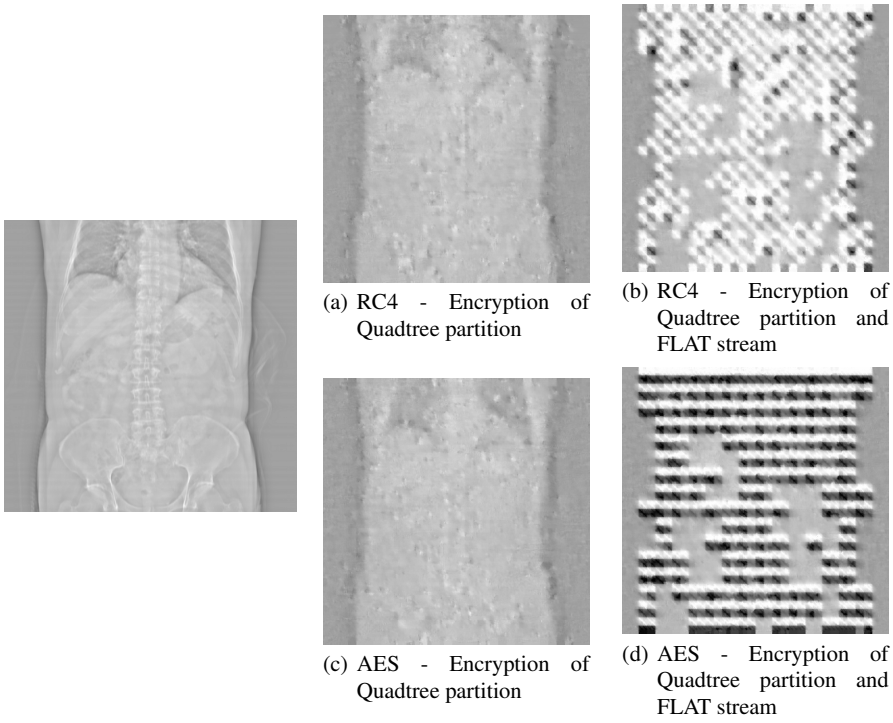


Fig. 16 LAR hierarchical selective encryption principle

Selective encryption goes a bit further than partial encryption. The idea is to cipher only a small fraction of the bitstream, the main component, which gives the added advantage of obtaining a valid compliant bitstream. This property allows the user to see a picture even without the key. Of course, the picture must be as different to the original one as possible.

Our selective encryption scheme uses also the quadtree partition as a basis [29]. The data required in the compression framework to build the flat picture are also used. The general idea is to encrypt several levels of the hierarchical pyramid. The process begins at the bottom of the pyramid. Depending on the depth of the encryption, the quality of the image rebuilt without the encryption key varies. The encryption itself is performed by a well-known secure data encryption scheme. One main property of our selective encryption scheme is that the level of encryption (i.e. the level of the details remaining visible to the viewer) can be fully customized. Hierarchical image encryption is obtained by deciding which level will be decrypted by supplying only the keys corresponding to those levels. This refines the quality of the image given to different categories of viewers. The encryption of a given level of the partition prevents the recovery of any additional visually-significant data (Figure 17). From a distortion point of view, it appears that encrypting higher levels (smaller blocks) increases the PSNR, and at the same time, the encrypting cost. From a security point of view, as the level increases, the search space for a brute force attack increases drastically.

As our research is focused on fast encryption procedures specifically tailored to the target environment, we use the pyramidal profile with Interleaved S+P configu-



(a) RC4 - Encryption of Quadtree partition

(b) RC4 - Encryption of Quadtree partition and FLAT stream

(c) AES - Encryption of Quadtree partition

(d) AES - Encryption of Quadtree partition and FLAT stream

Fig. 17 Visual comparison between original image and image obtained from partially encrypted LAR encoded streams without encryption key.

ration. Our encryption tools allow a fine selection of tradeoffs between encryption computing cost, hierarchical aspects, compliance and the quality of encrypted pictures.

4.3.3 Scalable ROI protection and encoding for medical use

Designing semantic models becomes a key feature in medical image management [65]. Different scenarios can be investigated. We present only one scenario suitable for image storage and off-line decoding. This scenario involves the following processing steps.

1. At the coder side, the specialist defines the ROI in the image and chooses the option ”lossless mode with encrypted ROI”. The resultant substream is given in Figure 18.
2. At the decoder side, the image can be partially decoded until the lossless ROI has been reconstructed or fully decoded. Figure 18 shows the overall process.

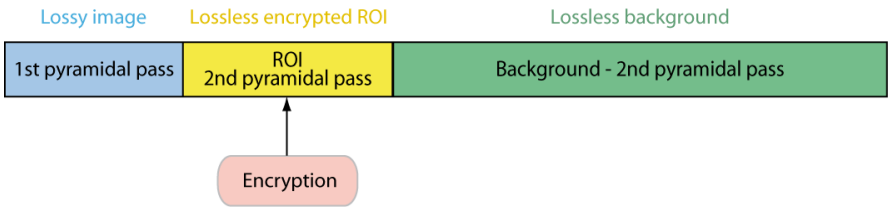


Fig. 18 Substream composition for lossless compression with an encrypted ROI

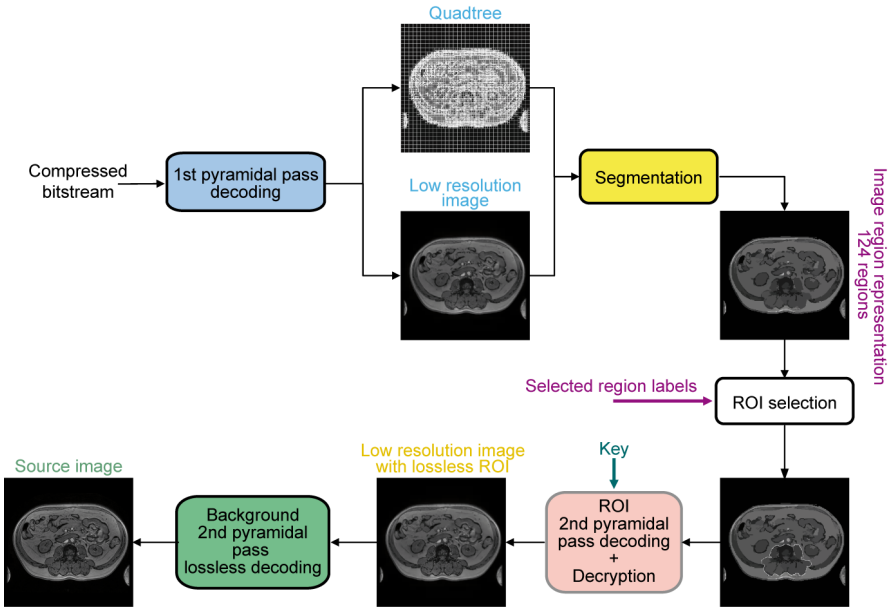


Fig. 19 Overall decoding scheme for lossless compression with an encrypted ROI

4.3.4 Client-server application and hierarchical access policy

For medical use, together with PACS systems, images and videos databases are a powerful collaborative tool. However, the main concern when considering these applications lies in the secure accessing of images. The objective is therefore to design a medical image database accessible through a client-server process that includes and combines a hierarchical description of images and a hierarchical secured access.

A corresponding client-server application [8] has been then designed. Every client will be authorized to browse the low-resolution image database and the server application will verify the user access level for each image and ROI request. ROIs can be encrypted or not, depending on the security level required.

If a client application sends a request that does not match the user access level, the server application will reduce the image resolution according to access policy. The exchange protocol is depicted in Figure 20.

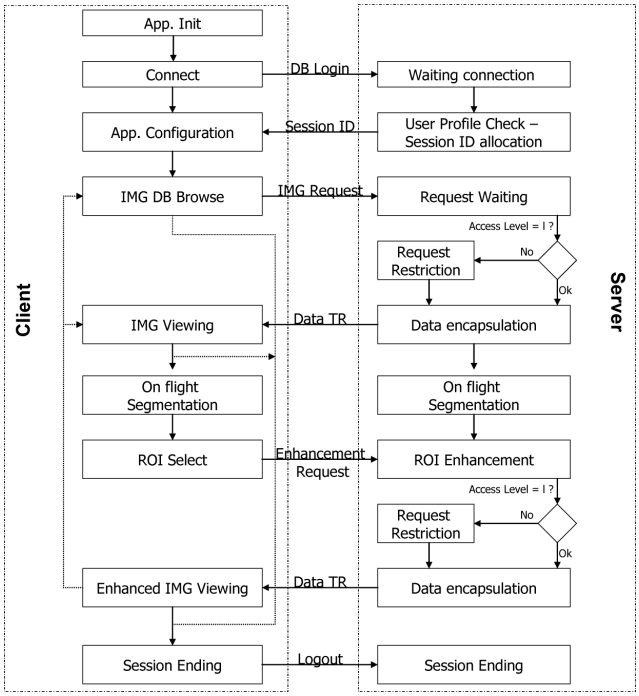


Fig. 20 Exchange protocol for client-server application

4.4 Transmission error protection - error resilience

Interest in remote medical applications has been rapidly increasing. Telemedicine aims to speed up the diagnosis process, reduce risks of infection or failure, enhance mobility and reduce patient discomfort.

Although wire networks are traditionally used for teleradiology or telesurgery purposes, the rapid growth of wireless technologies provides new potential for remote applications. To ensure optimal visualization of transmitted images, there are two possible ways of protecting the bitstreams.

Firstly, protecting the encoded bit-stream against error transmission is required when using networks with no guaranteed quality of service (QoS). In particular, the availability of the information can be ensured by the Internet protocol (IP). We

focused our studies on two topics, namely the loss of entire IP packets and the transmission over wireless channel.

Secondly, we develop error resilience strategies adapted to our compression scheme. UEP solutions used together with proper resynchronization processes and robust encoding naturally leads to optimal conditions for the transmission of sensitive data.

4.4.1 UEP strategies

Limited bandwidth and SNR are the main features of a wireless channel. Therefore, both compression and secure transmission of sensitive data are simultaneously required. The pyramidal version of the LAR method and an Unequal Error Protection strategy are applied respectively to compress and protect the original image. The UEP strategy takes account of the sensitivity of the substreams requiring protection and then optimizes the redundancy rate. In our application, we used the Reed Solomon Error Correcting Code RS-ECC, mixed with symbol block interleaving for simulated transmission over the COST27 TU channel [34] (Figure 21). When compared to the JPWL system, we show that the proposed layout is better than the JPWL system, especially transmission conditions are bad (SNR ¡ 21 dB).

Other simulation tests have been designed for MIMO systems using a similar framework, and have shown the ability of our codec to be easily adapted to bad transmission conditions, while keeping reasonable additional redundancy. At this point, comparisons with other methods remain difficult. Both SISO and MIMO transmissions simulation tools were provided by the French X-LIM Laboratory [16].

Current developments are focused on the study of the LTE transmission system [47], and its combination with LAR coded bitstreams.

These preliminary tests have been carried out without implementing basic error resilience features, such as resynchronization process, that should greatly improve our results. Some related solutions are presented below.

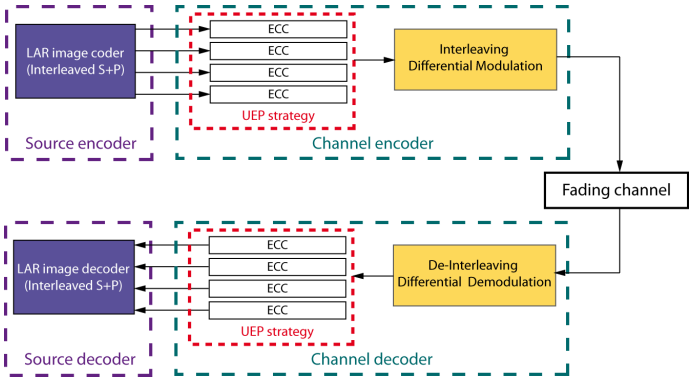


Fig. 21 Overall layout of the multi-layer transmission/compression system

In other words, compensating IP packet loss also requires a UEP process, which uses an exact and discrete Radon transform, called the Mojette transform [12]. The frame-like definition of this transform allows redundancies that can be further used for image description and image communication (Figure 22), for QoS purposes.

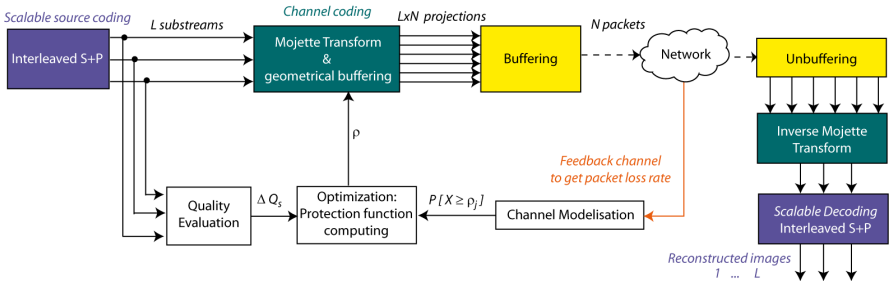


Fig. 22 General joint LAR-Mojette coding scheme

4.4.2 Error resilience

When only considering source coding, some simple adapted solutions of error resilience can be implemented. Introducing resynchronization markers remains the easiest way of adding error resilience to an encoding process. In this respect, the idea is to adapt marker definition to the used entropy coder. Although generic markers that fit any entropy encoder can be implemented, we have designed specific markers adapted to our particular arithmetic Q15-like coder [38] together with the LAR bistream organization. Hence, different intra and inter substream markers have been defined. These distinct markers can also be used as stream identifiers to design an intelligent resynchronization process: if we consider entire IP packet loss, the system is automatically able to identify the lost packet and ask for its retransmission.

In addition, to adjust the required computational complexity of our system, we then simply adapt the classic Golomb-Rice coder, for low complex application, and the arithmetic coder, or adaptive MQ like coder, or adaptive Q15 coder, for better compression results. A semi-adaptative Huffman coder is also available. One-pass solution can be implemented with an a priori codebook: for medical images of same type (e.g. mammograms) which share the same statistics, a unique codebook can be used. Two-passes methods lead to build an adapted codebook, so that to reduce the final rate. If exact codebook is computed from real errors, two solutions can be envisaged to transmit this codebook to the decoder. First, the entire codebook can be sent, implying a natural consequent overhead. Secondly, the codebook can be efficiently estimated from five different parameters, which characterized the distribution law of the codebook symbols.

Moreover, internal error detection is freely realized thanks to the introduction of forbidden codewords within the Huffman coder.

Online entropy decoding can also take advantage of the properties of the coded residual errors. These errors are naturally bounded by the adaptive quadtree decomposition. As soon as this bound is not respected, an error can be detected. Thus an intrinsic MQF like decoding process [33] is also available for free.

In terms of complexity, the Q15-LAR coder is 2.5 times faster than the arithmetic coder, and the semi-adaptive Huffman coder is 2 times faster than the Q15-LAR coder.

Finally, as previously mentioned, these error resilience techniques can be coupled with UEP strategies, for optimal protection features.

5 Conclusion

This chapter was dedicated to joint medical image coding and securization framework. General principles and notions have been described and the joint source-channel coding context has been emphasized. Cryptography and data hiding were shown to be efficient solutions for content securization. In terms of error resilience, source-based together with channel-based coding have been developed. As an example of standard implementation of transmission process, the Long Term Evolution has been studied.

In the medical context, the LAR coding scheme has been developed to face the secure transmission issues. Embedded functionalities such as adapted selective cryptography, human vision-based steganography coupled with Unequal Error Protection and error resilience tools have been designed. The idea is to maintain good coding properties together with embedded Quality Of Service oriented system. This framework has been evaluated by the JPEG committee and has shown its global efficiency.

However, the exchange of medical data remains a key research topic. As for the moment, PACS oriented frameworks have limitations in terms of securization process durability. If classical medical frameworks use image coding schemes such as JPEG, JPEG2000, JPEGXR, securization processes act as only additional features. A complete joint system should be built in such a manner that both coding and secure properties would benefit from each other. This remains an open research area!

Acknowledgements This work is supported by the French National Research Agency as part of the CAIMAN project (ANR-08-VERS-002).

References

1. 36.211, G.T.: Evolved Universal Terrestrial Radio Access (E-UTRA); physical channels and modulation (Release 9) (2009)
2. 36.321, G.T.: Evolved Universal Terrestrial Radio Access (E-UTRA); medium access control (mac) protocol specification (Release 9) (2009)
3. 36.322, G.T.: Evolved Universal Terrestrial Radio Access (E-UTRA); radio link control (rlc) protocol specification (Release 9) (2009)
4. 36.323, G.T.: Evolved Universal Terrestrial Radio Access (E-UTRA); packet data convergence protocol (pdcp) specification (Release 9) (2009)
5. Abdulfetah, A.A., Sun, X., ans Nur Mohammad, H.Y.: Robust Adaptive Image Watermarking using Visual Models in DWT and DCT Domain. Information Technology Journal **9**(3), 460–466 (2010)
6. Albanese, A., Blmer, J., Edmonds, J., Luby, M., Sudan, M.: Priority Encoding Transmission. IEEE Transaction on Information Theory **42**(6), 1737–1744 (1996)
7. Anderson, R.: Security Engineering - A Guide to Building Dependable Distributed Systems. Wiley (2008)
8. Babel, M., Bédat, L., Déforges, O., Motsch, J.: Context-Based Scalable Coding and Representation of High Resolution Art Pictures for Remote Data Access. In: Proc. of the IEEE International Conference on Multimedia and Expo, ICME'07, pp. 460–463 (2007). Projet ANR TSAR
9. Babel, M., Déforges, O.: WG1N4870 - Response to call for AIC techniques and evaluation methods. Tech. rep., ISO/ITU JPEG commitee, San Francisco (2009)
10. Babel, M., Déforges, O., Bédat, L., Strauss, C., Pasteau, F., Motsch, J.: WG1N5315 - Response to Call for AIC evaluation methodologies and compression technologies for medical images: LAR Codec. Tech. rep., ISO/ITU JPEG commitee, Boston, USA (2010)
11. Babel, M., Déforges, O., Ronsin, J.: Interleaved S+P Pyramidal Decomposition with Refined Prediction Model. In: IEEE International Conference on Image Processing, ICIP'05, vol. 2, pp. 750–753. Genova,Italy (2005)
12. Babel, M., Parrein, B., Déforges, O., Normand, N., Guédon, J.P., Coat, V.: Joint source-channel coding: secured and progressive transmission of compressed medical images on the Internet. Computerized Medical Imaging and Graphics **32**(4), 258–269 (2008)
13. Bas, P., marc Chassery, J., Davoine, F.: Using the fractal code to watermark images. In: in Proc. Int. Conf. Image Processing (ICIP, pp. 469–473 (1998)
14. Bender, W., Butera, W., Gruhl, D., Hwang, R., Paiz, F.J., Pogreb, S.: Applications for data hiding. IBM Systems Journal **39**, 547–568 (2000)
15. Bender, W., Gruhl, D., Morimoto, N., Lu, A.: Techniques for data hiding. IBM Systems Journal **35**(3/4), 313 – 336 (1996)
16. Boeglen, H.: IT++ library for numerical communications simulations. http://herve.boeglen.free.fr/ itpp_windows/ (2007)
17. Cayre, F., Chappelier, V., Jegou, H.: Signal processing and information theory library. `http://www.balistic-lab.org/` (2010)
18. Chu, Y., Ganz, A.: Wista: a wireless telemedicine system for disaster patient care. Mobile Networks and Applications **12**, 201–214 (2007)
19. Clunie, D.: DICOM Research Applications, Life at the Fringe of Reality. In: SPIE Medical Imaging. USA (2009)
20. Clunie, D.: DICOM support for compression schemes - more than JPEG. In: 5th Annual Medical Imaging Informatics and Teleradiology Conference. USA (2009)
21. Cox, I.J., Member, S., Kilian, J., Leighton, F.T., Shamoon, T.: Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing **6**, 1673–1687 (1997)
22. Dahlman, E., Parkvall, S., Skold, J., Beming, P.: 3G Evolution: HSPA and LTE for Mobile Broadband. Academic Press Inc (2007)

23. Déforges, O., Babel, M., Bédat, L., Ronsin, J.: Color LAR Codec: A Color Image Representation and Compression Scheme Based on Local Resolution Adjustment and Self-Extracting Region Representation. IEEE Trans. on Circuits and Systems for Video Technology **17**(8), 974–987 (2007)
24. Dufaux, F., Nicholson, D.: JWL: JPEG 2000 for wireless applications. In: SPIE Proc. Applications of Digital Image Processing XXVII, vol. 5558, pp. 309–318 (2004)
25. Editors, J.: JPEG 2000 image coding system - Part 11: Wireless JPEG2000 Committee Draft. in ISO/IEC CD 15444-11 / ITU-T SG8 (2004)
26. Elias, P.: Coding for Noisy Channels. Convention Record **4**, 37–49 (1955)
27. Ferguson, N., Schneier, B.: Practical Cryptography. Wiley (2003)
28. Flécher, E., Raulet, M., Roquier, G., Babel, M., Déforges, O.: Framework For Efficient Cosimulation And Fast Prototyping on Multi-Components With AAA Methodology: LAR Codec Study Case. In: Proc. of the 15th European Signal Processing Conference (Eusipco 2007), pp. 1667–1671. Poznań, Poland (2007)
29. Fonteneau, C., Motsch, J., Babel, M., Déforges, O.: A Hierarchical Selective Encryption Technique in a Scalable Image Codec. In: Proc. of International Conference in Communications (2008)
30. Furon, T., Cayre, F., Fontaine, C.: Watermarking Security in Digital Audio Watermarking Techniques and Technologies: Applications and Benchmarks. Idea Group Publishing, Cvejic and Seppanen Eds. (2007)
31. Gibaud, B.: The DICOM standard : a brief overview. In: Molecular imaging: computer reconstruction and practice, NATO Science for Peace and Security Series, pp. 229–238. Springer (2008)
32. Gilani, M., Skodras, A.N.: DLT-Based Digital Image Watermarking. In: Proc. First IEEE Balkan Conference on Signal Processing, Communications, Circuits and Systems. Istanbul, Turkey (2000)
33. Grangetto, M., Magli, E., Olmo, G.: A syntax-preserving error resilience tool for JPEG 2000 based on error correcting arithmetic coding. IEEE Trans. on Image Processing **15**(4), 807–818 (2006)
34. Hamidouche, W., Olivier, C., Babel, M., Déforges, O., Boeglen, H., Lorenz, P.: LAR Image transmission over fading channels: a hierarchical protection solution. In: Proc. of The Second International Conference on Communication Theory, Reliability, and Quality of Service, pp. 1–4. Colmar France (2009)
35. Hashmi, N., Myung, D., Gaynor, M., Moulton, S.: A sensorbased, web service-enabled, emergency medical response system. In: workshop on End-to-end, sense-and-respond systems, applications and services, pp. 25–29 (2005)
36. Hsu, C.T., Wu, J.L.: Multiresolution watermarking for digital images. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing **45**(8), 1097 –1101 (1998)
37. Hwang, S.O.: Content and service protection for iptv. Broadcasting, IEEE Transactions on **55**(2), 425 –436 (2009)
38. ITU-T: ITU-T T.81 (JPEG-1)-based still-image coding using an alternative arithmetic coder. Tech. rep., ISO/ITU JPEG commitee (2005)
39. J.K. Wolf A.D. Wyner, J.Z.: Source coding for multiple description. Bell System Technical Journal **59**(8), 1417–1426 (1980)
40. Kang, J.S., You, Y., Sung, M.Y.: Steganography using block-based adaptive threshold. In: 22nd international symposium on Computer and information sciences, ISCIS2007, pp. 1 –7 (2007)
41. Kunt, M., Ikonomopoulos, A., Kocher, M.: Second Generation Image Coding Techniques. Proceedings of the IEEE **73**(4), 549–575 (1985)
42. Li, J., Zhang, X., Liu, S., Ren, X.: An adaptive secure watermarking scheme for images in spatial domain using fresnel transform. In: 1st International Conference on Information Science and Engineering (ICISE), pp. 1630 –1633 (2009)
43. Liu, X., Eskicioglu, A.M.: Selective encryption of multimedia content in distribution networks: challenges and new directions. In: Conf. Communications, Internet, and Information Technology, pp. 527–533 (2003)

44. Mathon, B., Bas, P., Cayre, F., Macq, B.: Comparison of secure spread-spectrum modulations applied to still image watermarking. Annals of Telecommunication **11-12**, 810–813 (2009)
45. Meerwald, P., Uhl, A.: A survey of wavelet-domain watermarking algorithms. In: in Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III, pp. 505–516. SPIE (2001)
46. Mehlführer, C., Wrulich, M., Ikuno, J.C., Bosanska, D., Rupp, M.: Simulating the long term evolution physical layer. In: Proc. of the 17th European Signal Processing Conference (EUSIPCO 2009). Glasgow, Scotland (2009)
47. Mehlführer, C., Wrulich, M., Ikuno, J.C., Bosanska, D., Rupp, M.: Simulating the Long Term Evolution Physical Layer. In: Proc. of the 17th European Signal Processing Conference (2009)
48. Mohr, A., Riskin, E.A., Ladner, R.E.: Unequal Loss Protection : Graceful degradation of image quality over packet erasure channels through forward error correction. Journal on Selected Areas in Communications **18**(6), 819–828 (2000)
49. Motsch, J., Babel, M., Déforges, O.: Joint Lossless Coding and Reversible Data Embedding in a Multiresolution Still Image Coder. In: Proc. of European Signal Processing Conference, EUSIPCO, pp. 1–4. Glasgow UK (2009)
50. Motsch, J., Déforges, O., Babel, M.: Embedding Multilevel Image Encryption in the LAR Codec. In: IEEE Communications International Conference 06. Bucharest, Romania (2006)
51. Norcen, R., Podesser, M., Pommer, A., Schmidt, H.P., Uhl, A.: Confidential storage and transmission of medical image data. Computers in Biology and Medicine **33**(3), 277–297 (2003)
52. Norman, T.: The road to LTE for GSM and UMTS operators. Tech. rep., Analysys Mason (2009)
53. Oosterwijk, H.: The DICOM standard, overview and characteristics. Tech. rep., Ringholm Whitepapers (2004)
54. Pattichis, C., Kyriacou, E., Voskarides, S., Pattichis, M., R.Istepanian, Schizas, C.: Wireless telemedicine systems: An overview. IEEE Antennas and Propagation Magazine **44**(2), 143–153 (2002)
55. Pedersen, P.C., Sebastian, D.: Wireless Technology Applications in a Rural Hospital. In: 2004 American Telemedicine Association Annual Meeting (2004)
56. Reed, I., Solomon, G.: Polynomial Codes Over Certain Finite Fields. Journal of the Society of Industrial and Applied Mathematics (SIAM) **2**, 300–304 (1960)
57. Ruanaidh, J., Dowling, W., Boland, F.: Phase watermarking of digital images. In: International Conference on Image Processing, vol. 3, pp. 239–242 (1996)
58. Ruanaidh, J.J.K.., K, J.J., Ruanaidh, O., Pun, T., D'informatique, C.U.: Rotation, scale and translation invariant digital image watermarking. In: in IEEE International Conference on Image Processing ICIP1997, pp. 536–539 (1997)
59. Schneier, B.: Applied Cryptography, second edn. John Wiley & Sons (1996)
60. Sesia, S., Toufik, I., Baker, M.: LTE, The UMTS Long Term Evolution: From Theory to Practice. Wiley (2009)
61. Shinohara, M., Motoyoshi, F., Uchida, O., Nakanishi, S.: Wavelet-based robust digital watermarking considering human visual system. In: Proceedings of the 2007 annual Conference on International Conference on Computer Engineering and Applications, pp. 177–180 (2007)
62. Signal & Information Processing Lab, D.U.o.T.: Image and Video Compression Learning Tool VcDemo. `http://siplab.tudelft.nl/content/image-and-video-compression-learning-tool-vcdemo` (2004)
63. Sneha, S., Dulipovici, A.: Strategies for Working with Digital Medical Images. In: HICSS'06: Proceedings of the 39th Annual Hawaii International Conference on System Sciences, vol. 5, p. 100.1 (2006)
64. Taubman, D.S., Marcellin, M.W.: JPEG2000: Image Compression Fundamentals, Standards, and Practice. Kluwer Academic Publishers (2001)
65. Temal, L., Dojat, M., Kassel, G., Gibaud, B.: Towards an ontology for sharing medical images and regions of interest in neuroimaging. Journal of Biomedical Informatics **41**(5), 766–778 (2008)
66. Tian, J.: Reversible data embedding using a difference expansion. In: IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, pp. 890–896 (2003)

67. Tian, J., Wells R.O., J.: Reversible data-embedding with a hierarchical structure. In: Image Processing, 2004. ICIP '04. 2004 International Conference on, vol. 5, pp. 3419–3422 (2004)
68. Tian, J., Wells, R.O.: Reversible data-embedding with a hierarchical structure. In: ICIP, vol. 5, pp. 3419–3422 (2004)
69. Tsui, T.K., Zhang, X.P., Androutsos, D.: Color image watermarking using multidimensional fourier transforms. IEEE Transactions on Information Forensics and Security **3**(1), 16 –28 (2008)
70. Uhl, A., Pommer, A.: Image and Video Encryption - From Digital Rights Management to Secured Personal Communication, *Advances in Information Security*, vol. 15. Springer (2005)
71. Van Droogenbroeck, M., Benedett, R.: Techniques for a selective encryption of uncompressed and compressed images. In: ACIVS Advanced Concepts for Intelligent Vision Systems, pp. 90–97. Ghent, Belgium (2002)
72. Vucetic, J.: Telemedicine: The Future of Wireless Internet Applications. In: Southeast Wireless'03 (2003)
73. Xia, X.G., Boncelet, C.G., Arce, G.R.: A multiresolution watermark for digital images. In: IEEE International Conference on Image Processing (ICIP), pp. 548–551 (1997)
74. Yang, M., Bourbakis, N., Li, S.: Data, image and video encryption. IEEE Potentials pp. 28–34 (2004)
75. Zhao, J., Koch, E.: Embedding robust labels into images for copyright protection. In: Proceedings of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, pp. 242–251 (1995)