Med Bio Eng Comput (2006) 44:619–631
DOI 10.1007/s11517-006-0081-x

ORIGINAL ARTICLE

Secure and efficient health data management through multiple watermarking on medical images

A. Giakoumaki · S. Pavlopoulos · D. Koutsouris

Received: 15 November 2005 / Accepted: 2 June 2006 / Published online: 19 July 2006

Abstract The landscape of healthcare delivery and medical data management has significantly changed over the last years, as a result of the significant advancements in information and communication technologies. Complementary and/or alternative solutions are needed to meet the new challenges, especially regarding security of the widely distributed sensitive medical information. Digital watermarking is a recently established research area with many applications; nevertheless, the potential of this technology to contribute value-added services to medical information management systems has only recently started to be realized by the research community. The paper presents a review of research efforts in the area of medical-oriented watermarking and proposes a wavelet-based multiple watermarking scheme; this scheme aims to address critical health information management issues, including origin and data authentication, protection of sensitive data, and image archiving and retrieval. In accordance with the strict limitations applying to medical images, the scheme allows the definition of a region of interest (ROI) whose diagnostic value is protected, since the only additional information embedded therein aims at integrity control. The robustness of the method is enhanced through a form of hybrid coding, which includes repetitive embedding of BCH encoded watermarks. The experimental results on different medical imaging modalities demonstrate the efficiency and transparency of the watermarking scheme.

Keywords Multiple watermarking · Repetitive BCH encoding · Medical data protection · Authentication · Integrity control · Image retrieval

1 Introduction

Recent innovations in information and communication technologies have led to a new era in healthcare delivery and medical data management. New challenges have arisen as a result of easier access and distribution of digital data, especially regarding security of sensitive medical information. The research community seeks complementary and/or alternative solutions to confront these challenges and to effectively deal with a range of substantial healthcare information management issues.

Digital watermarking is a recently established research area with a plethora of applications [4, 10, 11, 25, 30]; however, its perspectives in the health information management field have just begun to be explored. Digital watermarking has the potential to act as a value-added tool for a range of issues including enhancement of medical confidentiality protection, origin and data authentication, highlighting of diagnostically significant regions, and efficient information retrieval, as discussed in detail in [12]. The paper presents an overview of research efforts in the area of medical data watermarking and describes a medical-oriented wavelet-based watermarking scheme. This

A. Giakoumaki (✉) · D. Koutsouris
Biomedical Engineering Laboratory, School of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece
e-mail: agiakoum@biomed.ntua.gr

S. Pavlopoulos
Institute of Communication and Computer Systems, National Technical University of Athens, Athens, Greece

scheme embeds in medical images multiple watermarks conveying the physician's digital signature for origin authentication, patient's personal and examination data, and keywords for image retrieval through indexing. Finally, a reference watermark, which is a priori known at the receiver's side, allows an overall image integrity control. The scheme conforms to the strict limitations concerning the integrity of medical images, by allowing the definition of a diagnostically significant region of interest (ROI), wherein the only additional information inserted is the reference watermark for integrity checking purposes.

2 Methods

2.1 Description of the scheme

The proposed scheme applies multiple watermarking in medical images, aiming to provide a unified approach towards enhancement of medical confidentiality protection, origin and data authentication, and efficient information retrieval. The multiple watermarks are embedded in the image by applying 4-level discrete wavelet transform (DWT) and a proper quantization of coefficients. Figure 1 illustrates the pyramid structure of a 4-level wavelet decomposition of an image, including a coarse scale image approximation at the highest decomposition level (LL4), and 12 detail images corresponding to the horizontal (HL), vertical (LH), and diagonal (HH) details at each of the four levels. It is well known that transform domain watermarking schemes outperform compared to spatial ones, since they exploit perceptual properties of the human visual system (HVS) [33] in order to achieve an optimal trade-off between robustness and imperceptibility. Wavelet-based schemes particularly have gained great attention in recent years, due to their ability to provide both spatial and frequency resolution [14, 35]; their main advantage, however, is the fact that the dyadic scaling decomposition of the wavelet transform resembles the signal processing of the HVS, thus allowing the distortion induced by quantization and/or watermarking to be adapted to the masking properties of the human eye [22].

In order to enhance medical confidentiality protection and to allow efficient data management, retrieval and integrity control, the scheme simultaneously inserts the following different purpose-specific watermarks:

1. A *signature watermark* comprising the physician's digital signature or identification code for the purpose of origin authentication.
2. An *index watermark* that contains keywords (e.g., ICD-10 diagnostic codes, image acquisition characteristics, etc.) and facilitates image retrieval by database querying mechanisms. The insertion of indices into the images provides an alternative for

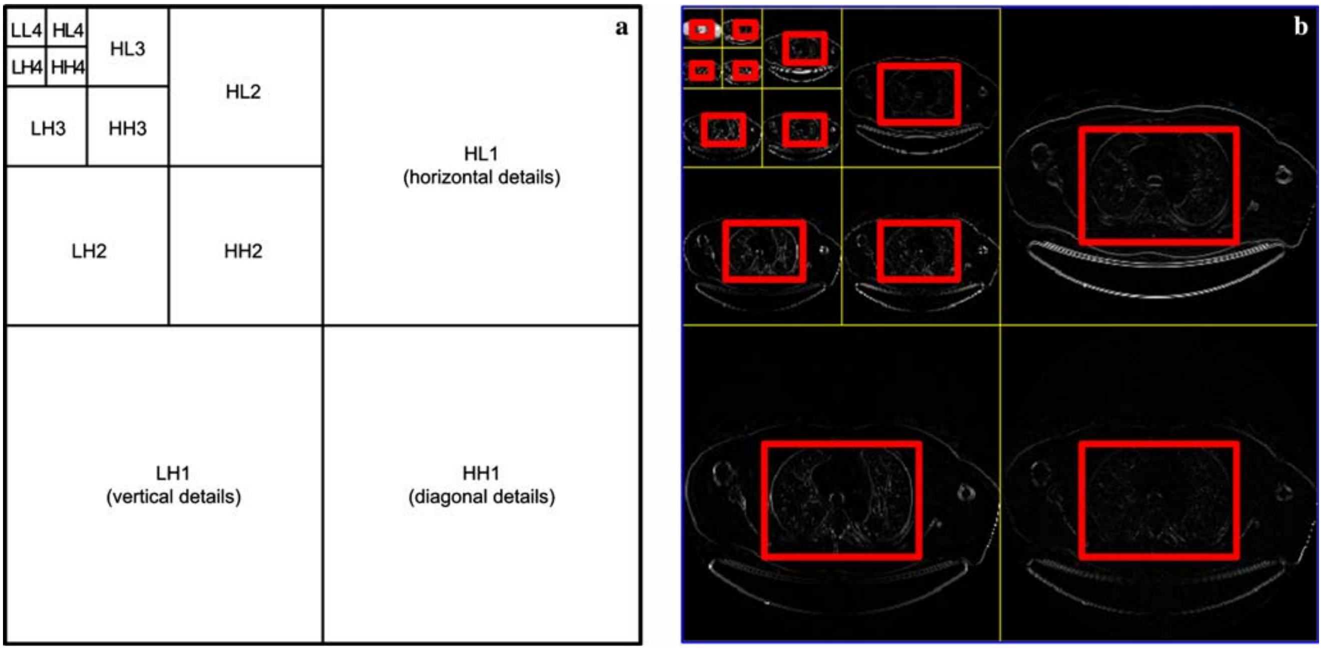

Fig. 1 Multiresolution wavelet decomposition of an image: **a** pyramid structure of 4-level DWT, **b** 4-level Haar DWT of a CT test image

efficient indexing and archiving of digital medical data in hospital information systems, which eliminates storage and transmission bandwidth requirements.

3. A *caption watermark* containing patient's personal and examination data (e.g., demographics, health history, and diagnostic reports), which grants a permanent link between the patient and the medical data, and an additional level of protection; this descriptive watermark provides information contributing to a thorough patient status evaluation and also allows the highlighting of diagnostically significant regions, preventing from separate transmission and storage of metadata that would increase memory and transmission bandwidth requirements.
4. A *reference watermark* is embedded throughout the image for the purpose of data integrity control [18]; the comparison of the extracted reference watermark bits with the originally embedded ones not only provides information on whether the image has been modified, but also indicates the possibly tampered image regions.

The scheme takes into consideration the ethical and legal limitations that apply to medical image manipulation and maintains the integrity of diagnostically significant parts; specifically, it allows the definition of a region of interest whose quality is perceptually preserved throughout the watermarking process, since the only information embedded therein is the integrity-checking reference watermark, which does not affect its diagnostic value.

Different medical applications, ranging from telemedicine to data archiving, storage, and retrieval in picture archiving and communication systems (PACS), could be benefited by integrating the proposed scheme with image acquisition devices, PDAs, PACS viewing stations, etc. Indicatively, in a telemedicine application, the acquired image can be watermarked with the identification code of the mobile unit; also, a mobile healthcare provider can embed patient's personal data and additional information in the image and transmit them with an additional level of security to a base station (e.g., hospital). There, the expert retrieves the watermarks, makes a preliminary diagnosis based on both the image and the extracted information, and provides directions to the mobile paramedics. Another use case involves acquiring an image in a hospital laboratory and watermarking it with information including the physician's identification code, patient's personal and examination data, and keywords to be used for image indexing. The watermarked image is stored in the hospital database and can be retrieved through querying mechanisms. Any authorized medical staff member can extract the embedded watermarks, thus gaining access to information including the primary physician's identity and diagnosis, data concerning the patient and the examination, as well as additional comments for healthcare providers' guidance. A variety of other medical applications could also be addressed by the proposed watermarking scheme, towards secure and efficient health data management.

2.2 The algorithm

As mentioned above, the embedding procedure is based on image decomposition through DWT. The Haar wavelet is selected as the mother wavelet for the image decomposition, in order to exploit the *dyadic rationality* of the resulting coefficients [31] for increased watermark robustness. Specifically, the Haar wavelet coefficients have the attribute that, when modified by addition or subtraction of a multiple of 2^l (where l is the decomposition level), their inverse wavelet transform produces an image with integer pixel values; thus any rounding operation, which could distort the values of certain watermark bits, is avoided [17]. The proposed method exploits this attribute in the quantization scheme used to insert the multiple watermarks in embeddable coefficients. According to the algorithm, any coefficient f selected to cast a watermark bit, is assigned a binary value through the following quantization function:

$$Q(f) = \begin{cases} 0, & \text{if } 2k \cdot \Delta + s \le f < (2k+1) \cdot \Delta + s \\ 1, & \text{if } (2k+1) \cdot \Delta + s \le f < (2k+2) \cdot \Delta + s \end{cases} \tag{1}$$

where k is an integer, s is a user defined offset for increased security, and Δ, the quantization parameter, is chosen to be equal to 2^l in order to exploit the dyadic rationality of Haar coefficients. The above quantization function can be equivalently rewritten as follows:

$$Q(f) = \begin{cases} 0, & \text{if } \lfloor (f-s)/\Delta \rfloor \text{ is even} \\ 1, & \text{if } \lfloor (f-s)/\Delta \rfloor \text{ is odd} \end{cases} \tag{2}$$

where $\lfloor . \rfloor$ is the floor function.

The multiple watermarks embedding procedure includes the following steps:

Step 1: The image is decomposed through 4-level Haar wavelet transform in a coarse scale image approximation at the highest decomposition level and a sequence of detail images (horizontal, vertical, and diagonal) at each of the four levels.

Step 2: The above quantization function is applied to each coefficient f that is to be watermarked. If the resulting binary value is equal to the value of the watermark bit to be embedded, the coefficient is left intact; otherwise, it is modified as follows in order to cast the watermark bit value:

$$f = \begin{cases} f + \Delta, & \text{if } f \leq 0 \\ f - \Delta, & \text{if } f > 0 \end{cases} \tag{3}$$

Step 3: The 4-level inverse wavelet transform is implemented to produce the watermarked image.

The extraction of the multiple watermarks is performed through decomposition of the watermarked image using 4-level Haar wavelet transform and key-based detection of the watermarked coefficients. The multiple watermark bits are subsequently extracted by applying the quantization function to each of these coefficients.

2.3 Selection criteria for watermark embedding locations

The wavelet coefficients to be watermarked are specified based on a random key and the ROI map. Initially, the key selects the embeddable coefficients of all levels and subbands; in the cases of the data watermarks (signature, index, caption) however, the wavelet domain ROI map determines which of the key-selected coefficients will finally be used for embedding, by not belonging to the ROI. In this way, the reference watermark is inserted in coefficients corresponding to the whole image, hence allowing an overall image integrity control, whereas the signature, index, and caption watermarks are cast into parts of no diagnostic significance. Thus, the diagnostically important regions of interest are protected against any compromise on their quality, by being burdened only with the information needed to enable integrity control. The wavelet domain ROI map is produced based on the spatial self-similarity between subbands [29] through the procedure described in [13]. The correspondence among the ROI maps of a wavelet-transformed CT test image in four decomposition levels is illustrated in Fig. 1b.

The multiple watermarks are distributed in different decomposition levels and subbands according to their individual characteristics and requirements. In the case of the signature watermark, robustness is of critical importance, due to the fact that even one error bit could result in authentication failure; on the contrary, the capacity requirements for the specific watermark are quite limited, since its length is restricted to the minimum needed to grant uniqueness of the conveyed identification code. The index and the caption watermarks on the other hand, demand also robustness but mainly increased capacity, since they convey many bits of additional information; as they comprise keywords for image retrieval and patient's personal/examination data respectively, it is evident that especially in the latter case the capacity requirements are even greater. Given the decreasing number of coefficients and consequently the reduced available capacity in ascending decomposition levels, the signature, index, and caption watermarks are embedded in non-ROI coefficients of the fourth, third, and second levels, respectively. The specific distribution of the watermarks is also in accordance with the robustness requirements; due to the fact that most of the energy is concentrated in the high decomposition levels, it is expected that more watermark robustness is achieved in ascending levels. Table 1 illustrates the energy distribution of a CT test image in its approximation and detail images, produced by 4-level Haar DWT. The energy is calculated using the following equation:

$$e_k = \frac{1}{N_k \cdot M_k} \sum_i \sum_j |I_k(i,j)| \tag{4}$$

where k denotes the approximation and the detail images at each of the decomposition levels, I_k are the coefficients of the subband images, and N_k, M_k are their corresponding dimensions. The table shows the increasing energy concentration in ascending decomposition levels, with the coarse scale image approximation accumulating the major energy proportion. As also evident from the table, the horizontal detail subbands concentrate more energy than the vertical and much more so than the diagonal subbands, a fact that indicates their minor vulnerability to attacks and motivates their use for embedding of the signature, index, and caption watermarks.

Due to the generally resembling behavior of horizontal and vertical subbands [15], an image modification is very likely to affect them in a similar way; therefore, the selection of vertical subbands for reference watermark embedding provides a reflection of the potential tampering of the image. For imperceptibility reasons, the coarse scale image approximation is left intact by the embedding procedure, because of its crucial effect on image quality resulting from the large energy concentration. Besides, the first decomposition level coefficients are used exclusively for reference watermarking and not for signature, index, and caption

Table 1 Energy of approximation and detail images of a 4-level wavelet decomposition of a CT image

Subband	Level 1	Level 2	Level 3	Level 4
Approximation	–	–	–	440.17
Horizontal detail	1.93	5.95	16.72	44.50
Vertical detail	1.30	3.60	9.45	26.63
Diagonal detail	0.59	2.17	6.52	18.19

watermarks embedding, due to their minor effect on image quality that makes them susceptible to common image processing, compression, or attacks. In order to enable a comprehensive image distortion report, the reference watermark is embedded in selected coefficients of the other three decomposition levels as well; in this way, it can be extracted from specific frequencies and/or spatial regions, in order to reflect their potential tampering.

It should be noted that, despite the fact that the energy allocation in subbands and decomposition levels depends on the characteristics of the image, some attributes are common in different imaging modalities; based on these attributes, as well as the individual robustness and capacity requirements of the multiple watermarks, their distribution in the subbands was devised as illustrated in Table 2. The particular allocation of the watermarks optimizes the trade-off among robustness, capacity, and imperceptibility, being efficient and applicable to different imaging modalities without adaptation. The table presents the maximum available capacity in the selected subbands for images of size 512 × 512 pixels, which corresponds to the amount of embeddable coefficients when no ROI is defined; in any other case, the available capacity in the horizontal subbands is determined by the extent of the ROI, since only horizontal coefficients belonging to the non-ROI are allowed to carry watermark bits.

Table 2 Allocation of watermarks according to robustness and capacity criteria

Subband	Capacity (embeddable coefficients)	Embedded watermark	
		Type	Robustness requirement
LH1	65,536	Reference	Low
HL2	16,384	Caption	High
LH2	16,384	Reference	Low
HL3	4,096	Index	High
LH3	4,096	Reference	Low
HL4	1,024	Signature	Very high
LH4	1,024	Reference	Low

3 Results

The algorithm was tested on different medical imaging modalities (CT, MRI, MRA, PET), with each test set containing 20 images of size 512 × 512 pixels. The algorithm embeds watermarks that are binary arrays from the set {0, 1}; in our simulations, the signature and the reference watermarks were produced by a uniform random number generator, whereas the index and caption ones were derived by ASCII coding of text files containing keywords and patient's data, respectively. The length of the signature watermark was selected to be 128 bits, which is sufficient to grant uniqueness to the conveyed identification code [27]. The sets of keywords and patient's data used for index and caption watermarks generation, were arbitrarily selected to comprise 52 and 208 characters respectively; this corresponds to index and caption watermarks of length 364 and 1,456 bits, respectively, by assigning seven bits per character through ASCII coding.

In order to increase robustness of the watermarks carrying additional data (signature, index, caption), a form of *hybrid coding* including repetitive embedding of BCH encoded watermarks was implemented; specifically, each of the three watermarks was split into parts of equal length, which were then incorporated into suitably selected BCH codes. Afterwards, the BCH encoded watermarks were embedded three times each; this hybrid coding provides the possibility to correct some errors using repetition decoding, before BCH decoding is performed, thus increasing the robustness of the watermarks [38]. Repetition decoding is actually a majority vote process and refers to forming the output watermark based on the most common bit values extracted from the three embedded watermark copies. Table 3 presents the BCH encoding schemes used in these simulations, as well as the number of BCH codes needed in order to comprehend the whole watermarks. In general, a binary BCH code with parameters (n, k, l) represents a codeword of length n, which includes k bits of the watermark array, and can correct up to l bit errors. For instance, BCH (255, 91, 25) comprises a codeword of 255 bits, which includes 91 bits of the watermark to be embedded, and has an error correction capability of 25 bits. In order

Table 3 BCH encoding schemes for each type of watermark

Type of watermark	Number of bits	BCH scheme	Iterations	Total number of embedded bits
Signature	128	(31, 16, 3)	8	248
Index	364	(255, 91, 25)	4	1,020
Caption	1,456	(255, 91, 25)	16	4,080

for example to encode the 1,456-bits caption watermark using BCH (255, 91, 25), the watermark is split into 16 equal parts, and a separate BCH code is used for each part; this results in a total number of 4,080 codeword bits that need to be embedded.

Given the strict limitations regarding the acceptable modifications of medical images, a thorough evaluation of the scheme performance in terms of transparency is necessary; therefore, both perceptual and signal qualities need to be assessed. Peak signal-to-noise-ratio (PSNR), although not well correlated with perceptual quality, provides an efficient measure of image distortion in terms of numerical values [5, 19, 20], which convey important information in medical applications, for instance in diagnosis support systems. Table 4 presents the obtained average PSNR values of the watermarked images, for each of the four imaging modalities tested.

The watermarked images were compared with the original ones by a physician who concluded that the visual difference between them was negligible; special attention was paid to the evaluation of the ROI, whose quality was found to be preserved, as the minor distortion due to reference watermark embedding in sporadic ROI coefficients did not cause any image degradation that could affect its fidelity and diagnostic value. Figures 2, 3, 4, and 5 illustrate four test images (CT, MRI, MRA, PET, respectively), each with a specified ROI, and the corresponding watermarked images resulting from the proposed scheme. The high PSNR values obtained, combined with the adequate perceptual quality of the watermarked images, illustrate the transparency of the scheme.

Table 4 Performance of the scheme in terms of PSNR

Image modality	PSNR (dB)
CT	46.47 ± 0.06
MRI	46.37 ± 0.05
MRA	45.96 ± 0.04
PET	46.66 ± 0.20

The performance of the scheme in terms of robustness of the data watermarks (signature, index, caption) was evaluated through JPEG compression of the watermarked images; JPEG compression was selected as an indicative attack applied to the whole image and with varying quality factors, thus reflecting the tolerance of the watermarks in different levels of image distortion. Tables 5, 6, 7, and 8 demonstrate the performance of the scheme for each of the imaging modalities tested. The watermarked images were subjected to JPEG compression with different quality factors and the three watermarks carrying the additional data were extracted and subsequently compared with the originally embedded ones; the tables show the percentage of bit errors in the extracted watermarks. As evident from these tables, the results in terms of robustness were satisfactory; indicatively, the watermark conveying the signature was extracted intact from all imaging modalities tested, even when the watermarked images were subjected to JPEG75 compression. The index watermark resisted JPEG compression with quality factors of at least 80, and particularly in the cases of MRA and PET images, it was extracted intact even after JPEG75 compression. As expected, the tolerance of the caption watermark to JPEG compression was less, due to the decreasing robustness in descending decomposition levels.

Tables 9, 10, 11, and 12 demonstrate the effects of applying JPEG compression with different quality factors to the watermarked images of CT, MRI, MRA, and PET modalities, respectively. In order to evaluate the degree of distortion, we selected the normalized hamming distance (NHD) as the similarity measure:

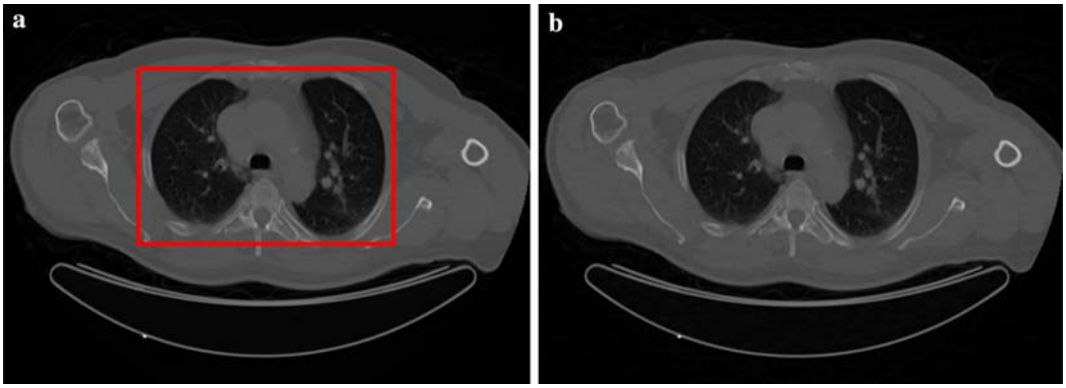

Fig. 2 Original and watermarked CT images: **a** original image with a specified ROI, **b** resulting watermarked image

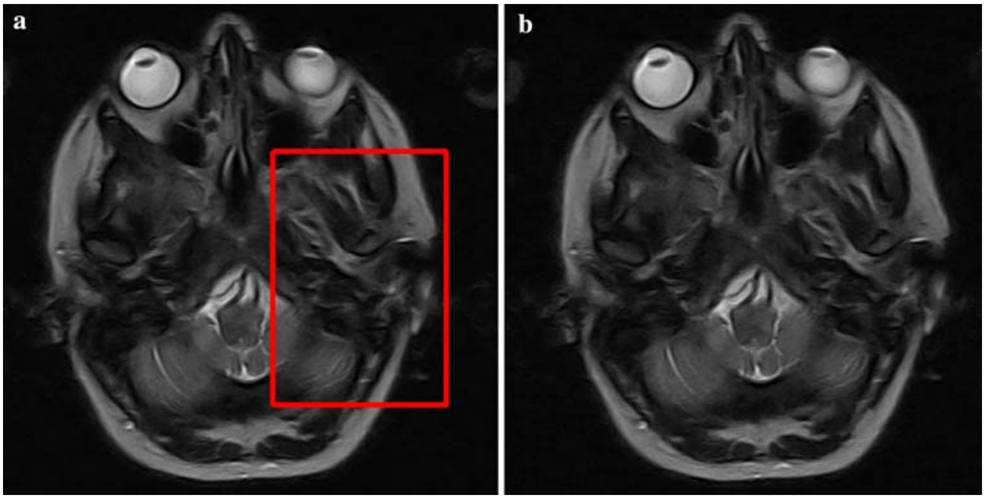

Fig. 3 Original and watermarked MRI images: **a** original image with a specified ROI, **b** resulting watermarked image

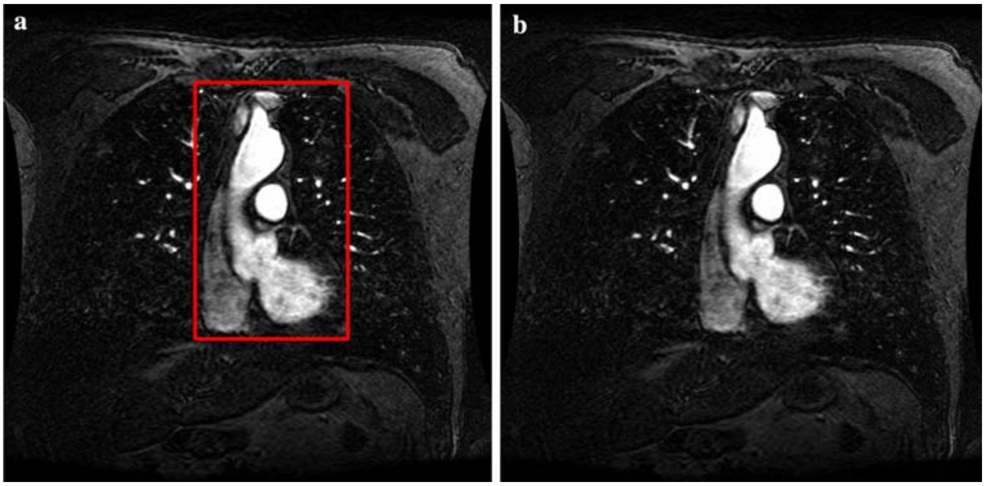

Fig. 4 Original and watermarked MRA images: **a** original image with a specified ROI, **b** resulting watermarked image

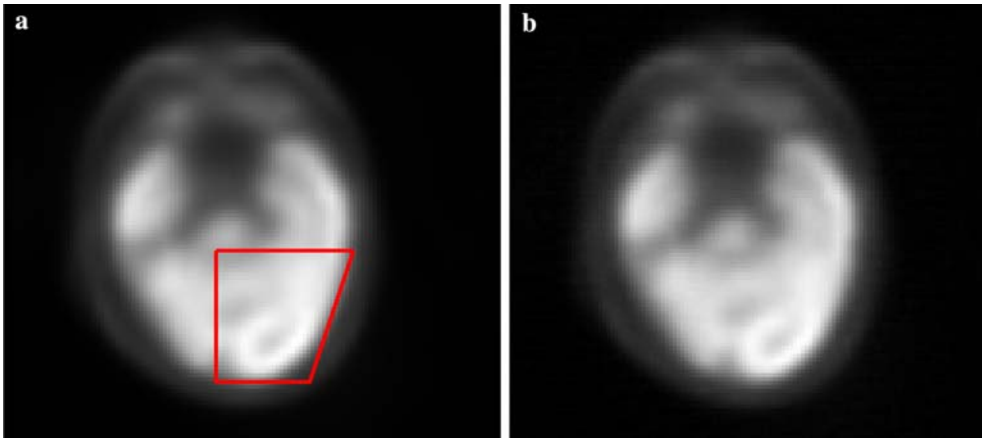

Fig. 5 Original and watermarked PET images: **a** original image with a specified ROI, **b** resulting watermarked image

$$\mathrm{NHD}(w,\tilde{w}) = \frac{1}{N_w}\sum_{i=1}^{N_w} w(i) \oplus \tilde{w}(i) \tag{5}$$

where w and $\tilde{w}$ are the original and extracted reference watermarks respectively, N_w is the length of the watermark, and $\oplus$ is the exclusive-OR operator. The distance ranges between (0, 1) and the decision on the data integrity is application dependent. As obvious, in medical applications the distance value should not exceed a small threshold, thus indicating negligible

Table 5 Percentage of bit errors in watermarks extracted from CT images (%)

Type of watermark	Signature	Index	Caption
JPEG quality factor			
95	0	0	2.0
90	0	0	13.5
85	0	0	20.4
80	0	0	30.9
75	0	5.5	37.8

Table 6 Percentage of bit errors in watermarks extracted from MRI images (%)

Type of watermark	Signature	Index	Caption
JPEG quality factor			
95	0	0	0
90	0	0	13.8
85	0	0	23.4
80	0	0	30.5
75	0	4.4	39.3

Table 7 Percentage of bit errors in watermarks extracted from MRA images (%)

Type of watermark	Signature	Index	Caption
JPEG quality factor			
95	0	0	0
90	0	0	15.9
85	0	0	25.3
80	0	0	35.8
75	0	0	43.6

Table 8 Percentage of bit errors in watermarks extracted from PET images (%)

Type of watermark	Signature	Index	Caption
JPEG quality factor			
95	0	0	0
90	0	0	12.6
85	0	0	20.9
80	0	0	30.8
75	0	0	36.0

image modifications. As expected, JPEG compression with decreasing quality results in increasing NHD values. The tables also illustrate the decrease of the NHD value in ascending decomposition levels, which is due to the increased robustness.

The above presented experimental results demonstrate the efficiency of the scheme in terms of robustness, imperceptibility, and integrity control capability, and its potential to provide value-added services in health data management systems.

4 Discussion

The paper discusses the perspectives of digital watermarking in health information management and proposes a medical-oriented wavelet-based multiple watermarking scheme; this scheme simultaneously embeds four types of watermarks into medical images, intending to enhance protection of sensitive data, provide origin and data authentication capability, and allow efficient image archiving and retrieval. In order to increase robustness of the watermarks conveying signature, index, and caption data, a combination of BCH encoding and repetitive embedding is performed. The experimental results demonstrate the efficiency of the scheme in terms of robustness, imperceptibility, and integrity control capability.

4.1 Comparison with literature

A plethora of studies regarding digital watermarking techniques and applications have enriched the literature over the last decade; nevertheless, the exploitation of digital watermarking perspectives in medical applications is still in its infancy. A brief overview of the main medical-oriented watermarking studies conducted so far is presented below:

Macq and Dewey [21] focused on the issue of the "trusted header" and proposed a reversible watermarking technique for the purpose of DICOM header verification through insertion of the header hash in the medical image. The method uses "pseudo-sums" and "pseudo-differences" of adjacent image pixels for the insertion of the hash, the comparison of which with the hash corresponding to the received image allows the reliability control of the link between the header and the image.

Coatrieux et al. [9] proposed the use of watermarking techniques as a complementary measure to the existing ones for protecting medical images; they pinpointed the necessary requirements a watermarking system has to conform to in order to be accepted in a medical environment, as well as its complementary role to the existing security systems. Two different application scenarios were presented, which involved image authentication and tracing, and health record integrity control, respectively. In a latter study, Coatrieux et al. [8] discussed again the role of watermarking in the context of security of health information systems and focused on the issue of medical image integrity control; they proposed to separate the images into two parts, the one comprising the regions of diagnostic significance (ROI), and the other representing a region of non-interest. In order to preserve the diagnostic

Table 9 Normalized hamming distance values as a function of JPEG quality factor for CT images

QF of JPEG compressed watermarked image	Normalized hamming distance			
	Level 1	Level 2	Level 3	Level 4
75	0.49 ± 0.01	0.43 ± 0.01	0.20 ± 0.01	0.12 ± 0.02
80	0.49 ± 0.01	0.38 ± 0.01	0.14 ± 0.01	0.11 ± 0.01
85	0.48 ± 0.01	0.31 ± 0.01	0.13 ± 0.01	0.08 ± 0.01
90	0.47 ± 0.01	0.25 ± 0.01	0.12 ± 0.01	0.06 ± 0.01
95	0.40 ± 0.01	0.18 ± 0.01	0.09 ± 0.01	0.03 ± 0.01

Table 10 Normalized hamming distance values as a function of JPEG quality factor for MRI images

QF of JPEG compressed watermarked image	Normalized hamming distance			
	Level 1	Level 2	Level 3	Level 4
75	0.50 ± 0.01	0.42 ± 0.01	0.19 ± 0.01	0.12 ± 0.01
80	0.49 ± 0.01	0.39 ± 0.01	0.13 ± 0.01	0.11 ± 0.01
85	0.49 ± 0.01	0.33 ± 0.01	0.12 ± 0.01	0.08 ± 0.01
90	0.47 ± 0.01	0.25 ± 0.01	0.11 ± 0.01	0.06 ± 0.01
95	0.42 ± 0.01	0.16 ± 0.01	0.07 ± 0.01	0.04 ± 0.01

Table 11 Normalized hamming distance values as a function of JPEG quality factor for MRA images

QF of JPEG compressed watermarked image	Normalized hamming distance			
	Level 1	Level 2	Level 3	Level 4
75	0.50 ± 0.01	0.45 ± 0.01	0.20 ± 0.01	0.12 ± 0.02
80	0.50 ± 0.01	0.42 ± 0.01	0.16 ± 0.01	0.10 ± 0.02
85	0.50 ± 0.01	0.38 ± 0.01	0.13 ± 0.01	0.09 ± 0.01
90	0.50 ± 0.01	0.30 ± 0.01	0.10 ± 0.01	0.06 ± 0.01
95	0.48 ± 0.01	0.18 ± 0.01	0.06 ± 0.01	0.04 ± 0.01

Table 12 Normalized hamming distance values as a function of JPEG quality factor for PET images

QF of JPEG compressed watermarked image	Normalized hamming distance			
	Level 1	Level 2	Level 3	Level 4
75	0.50 ± 0.01	0.43 ± 0.01	0.14 ± 0.01	0.09 ± 0.02
80	0.50± 0.01	0.36 ± 0.01	0.09 ± 0.01	0.08 ± 0.02
85	0.49 ± 0.01	0.27 ± 0.01	0.08 ± 0.01	0.07 ± 0.01
90	0.48 ± 0.01	0.19 ± 0.01	0.07 ± 0.01	0.06 ± 0.01
95	0.39 ± 0.01	0.11 ± 0.01	0.04 ± 0.01	0.03 ± 0.01

value of the image, they suggested the insertion of the watermarks exclusively in non-ROI parts. They also examined three alternative schemes for extraction of verification signatures and compared their tamper detection performance.

Kong and Feng [16] compared three well-known watermarking techniques in terms of signal integrity verification in an electroencephalogram (EEG) monitoring application for brain injury detection. More specifically, they evaluated patchwork, least significant bit (LSB) replacement, and quantization-based watermarking methods with respect to sensitivity to noise contamination, robustness to EEG signal characteristics changes due to brain injury, and consistency under various communication channel models. They implemented autoregressive modeling to the EEG signal and inserted the authentication watermark in the residual sequence. The result of their study was that the patchwork method outperforms compared with the other two techniques, providing lower error bit passing probability and higher signal-to-noise-ratio (SNR) in conditions of moderate bit error rate in the communication channel.

Acharya et al. [1] proposed the embedding of an encrypted version of the electronic patient record (EPR) in medical images, by replacing the LSB of the gray levels of pixels. The text file containing patient's data was encrypted using the logarithm of the ASCII codes of the text, whereas the encryption of the heart rate signal was based on predictive coding techniques, such as differential pulse code modulation (DPCM) and adaptive delta modulation (ADM). The authors pointed out the reduction of storage and transmission overheads as a result of inserting patient information in medical images. In a latter study, Acharya et al. [2] repeated their tests using error control coding, in order to enhance the reliability of image transmission and storage in the presence of noise or other interference. Subsequently, Acharya et al. [3] performed watermark embedding by LSB replacement in the frequency domain. More specifically, they applied discrete cosine transform (DCT) into image blocks of size 8 × 8 pixels and replaced the LSBs of DCT coefficients belonging to a mid-frequency range with the bits of the array which resulted from the encryption of EPR data. Nayak et al. [24] presented a comparative evaluation of the results deriving from applying the LSB method to the spatial and frequency domains, the latter including not only DCT, but also discrete fourier transform (DFT) and DWT. It is worth mentioning though that, despite the minimal degradation of image quality and the low complexity, the LSB watermarking method is not applicable in practice due to its well-known fragility.

Miaou et al. [23] and Chao et al. [7] also proposed a watermarking technique based on LSB replacement, aiming to provide origin authentication and protection of the patient's health record. They applied an algorithm using a bipolar multiple-number base in order to embed a watermark consisting of an ECG signal, a diagnostic report, and the physician's seal. It is noteworthy however to mention that the extraction of the watermark requires the knowledge of the original, unwatermarked image, a fact that invalidates the worth of the system in practice.

The lack of robustness of LSB-replacement watermarking techniques to both malicious attacks and common image processing operations has not deterred other researchers to also implement them in medical applications; Zhou et al. [37] used an LSB watermarking scheme in order to verify the authenticity and the integrity of digital mammography images. They embedded the health record in the image by replacing the LSBs of randomly selected pixels with the bits of the array comprising the record. This array included patient's data, as well as the digital signature resulting from the encrypted image digest, thus allowing the data authenticity and integrity control. In order to avoid any distortion of the image digest due to watermarking, the LSBs of the image pixels were excluded from the procedure of digest calculation. Cao et al. [6] presented the existing context of medical data protection in PACS based on the DICOM standard and discussed the advantages and disadvantages of the LSB watermarking technique with respect to the existing security measures.

Wakatani [34] proposed the embedding of a signature image in non-ROI regions of the original image in order to avoid any compromise on its diagnostic value. The signature was encoded using embedded zerotree wavelet (EZW) progressive coding and the resulting bit array was embedded in the image by replacing the bits of a randomly selected bit plane of the pixels. The watermark was inserted in a spiral way around the ROI, with the most significant information of the signature embedded in the nearest to the ROI area. By dividing the contour of the ROI in several regions and inserting the signature in each region, the signature image could be extracted from a clipped image including only a part of the ROI.

Trichili et al. [32] suggested the addition of a virtual border to the image by mirror effect, in order to embed the watermark in pixels not belonging to the image itself, thus guaranteeing its integrity. The watermark included the patient's name, age, and the image acquisition laboratory, and was embedded in the LSBs of the virtual border. The authors claim that the original image can be extracted from the watermarked one due to the reversibility of the method; still, the disadvantages of LSB embedding are applied to this approach as well.

Yang and Bao [36] presented a brief overview of reversible watermarking methods that have been proposed in the literature and proposed a method which is exclusively applicable to the authentication of an Electronic Clinical Brain Atlas. Their method uses for embedding the border between different structures of the atlas, and modifies in a reversible way the color of specific pixels of the border in order to embed the binary sequence.

Recently, Puech and Rodrigues [28] proposed the combination of encryption and watermarking techniques for the purpose of safe transmission of medical images. The suggested methodology includes ciphering of the image using a secret key, which is encrypted with a public-private key method and is subsequently embedded in the ciphered image. A DCT-based watermarking technique was applied in order to embed the encrypted key. The authors claim that their stream cipher method is robust to moderate noise like JPEG compression with high quality factor.

Osborne et al. [26] developed a semi-fragile watermarking technique aiming to verify the integrity of the ROI of medical images after transmission. They used a quantization-based method to multiply embed a signature into the region of background (ROB). The signature was extracted by comparing the coefficient values of pseudo-random pairs of DCT blocks belonging to the ROI. The authors focused on the robustness of the method to both JPEG compression and image transmission over error-prone mobile channels.

According to our extensive literature review, medical-oriented watermarking approaches have focused on specific applications, whereas multiple watermarking of medical images, aiming to provide a unified approach to different healthcare applications, is an innovative concept. On the other hand, our multiple watermarking scheme simultaneously addresses a range of health data management issues having different characteristics and requirements.

4.2 Attributes of the scheme

The proposed scheme provides a value-added tool for secure and efficient health data management through the use of multiple purpose-specific watermarks; different types of data are conveyed in each watermark, providing source identification, indexing and patient/examination information, as well as data integrity control. Each of the embeddable watermarks has different characteristics in terms of robustness and capacity, depending on the purpose that it addresses and consequently on the nature and size of the information that it needs to accommodate. The signature watermark allows the identification of the source of the medical data, be it the physician, the code of the mobile unit, etc. The index watermark carries keywords, based on which efficient image retrieval from image databases can take place. For instance, an image can be watermarked with indexing information along with other additional data at the point of acquisition, be it a remote health center or a laboratory. Subsequently, the image can be transmitted to the hospital server and subjected to index watermark extraction prior to its storage in the hospital image database; this indexing information can afterwards be used for efficient database querying. It is noteworthy to mention that the wavelet-analytic nature of the algorithm provides the potential of deriving image inherent characteristics that could be used for content-based database querying. On the other hand, the insertion of patient's personal data directly into the image using the caption watermark, guarantees a permanent link between the patient and his/her medical data and enhances medical confidentiality protection. Since only authorized users having the appropriate watermark key can extract the sensitive information, watermarking provides data access control and enables a form of de-identification; given that the personal identification marks are detached from the images and embedded in them using a key, the images can be distributed without the risk of revealing sensitive data to unauthorized users. Both the embedding and extraction procedures are time-efficient, thus providing the authorized user with the capability of easily accessing the embedded data, and if necessary, updating the information and re-embedding it in the image. Moreover, the fact that reference watermarking reveals the possibly tampered image parts and allows the physician to evaluate the extent of the modification by examining its impact in all the decomposition levels, further justifies the value-added functionality of the watermarking scheme.

4.3 Future work

Future work involves exploiting the wavelet-analytic nature of the algorithm to derive image inherent characteristics, in order for the proposed scheme to accommodate content-based image querying. Moreover, the algorithm can be easily integrated with the wavelet-based JPEG2000 compression standard to allow efficient storage and transmission of medical images. Conforming to the strict limitations regarding manipulation of diagnostically significant image regions, the scheme has the potential to be integrated into health information systems, in order to provide value-added services for secure and efficient health data management.

Acknowledgments This work has been supported by the General Secretariat for Research and Technology of the Hellenic Ministry of Development and the European Union under the PENED program.

References

1. Acharya RU, Anand D, Bhat SP, Niranjan UC (2001) Compact storage of medical images with patient information. IEEE Trans Inf Technol Biomed 5:320–323

2. Acharya RU, Bhat SP, Kumar S, Min LC (2003) Transmission and storage of medical images with patient data. Comput Biol Med 33:303–310
3. Acharya RU, Niranjan UC, Iyengar SS, Kannathal N, Min LC (2004) Simultaneous storage of patient information with medical images in the frequency domain. Comput Methods Programs Biomed 76:13–19
4. Bartolini F, Tefas A, Barni M, Pitas I (2001) Image authentication techniques for surveillance applications. Proc IEEE 89:1403–1418
5. Bruckmann A, Uhl A (1998) Selective medical image compression using wavelet techniques. J Comput Inform Technol Special Issue on Biomed Image Processing and Analysis 6:203–213
6. Cao F, Huang HK, Zhou XQ (2003) Medical image security in a HIPAA mandated PACS environment. Comput Med Imaging Graph 27:185–196
7. Chao HM, Hsu CM, Miaou SG (2002) A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. IEEE Trans Inf Technol Biomed 6:46–53
8. Coatrieux G, Maitre H, Sankur B (2001) Strict integrity control of biomedical images. Proceedings of the SPIE security and watermarking of multimedia contents III, vol 4314. San Jose, pp 229–240
9. Coatrieux G, Maitre H, Sankur B, Rolland Y, Collorec R (2000) Relevance of watermarking in medical imaging. Proceedings of the 3rd conference on information technology application in biomedicine. Arlington, pp 250–255
10. Cox IJ, Miller ML (2002) The first 50 years of electronic watermarking. EURASIP J Appl Signal Process 2002:126–132
11. Eggers JJ, Bauml R, Tzschoppe R, Huber J (2001) Applications of information hiding and digital watermarking. Proceedings of the ECDL workshop on generalized documents. Darmstadt, Germany
12. Giakoumaki A, Pavlopoulos S, Koutsouris D (2004) A multiple watermarking scheme applied to medical image management. Proceedings of the 26th IEEE-EMBS annual international conference on engineering in medicine and biology. San Francisco, pp 3241–3244
13. Giakoumaki A, Pavlopoulos S, Koutsouris D (2005) Multiple digital watermarking applied to medical imaging. Proceedings of the 27th IEEE-EMBS annual international conference on engineering in medicine and biology. Shanghai, China, pp 3444–3447
14. Hartung F, Kutter M (1999) Multimedia watermarking techniques. Proc IEEE Special Issue on Identification and Protection of Multimedia Information 87:1069–1107
15. Kim BS, Kwon KK, Kwon SG, Park KN, Song KI, Lee KI (2002) A robust wavelet-based digital watermarking using statistical characteristic of image and human visual system. Proceedings of the international conference on circuits systems computers and communications. Phuket, Thailand, pp 1019–1022
16. Kong X, Feng R (2001) Watermarking medical signals for telemedicine. IEEE Trans Inf Technol Biomed 5:195–201
17. Kundur D, Hatzinakos D (1999) Digital watermarking for telltale tamper proofing and authentication. Proc IEEE 87:1167–1180
18. Kundur D, Hatzinakos D (2001) Diversity and attack characterization for improved robust watermarking. IEEE Trans Signal Process 49:2383–2396
19. Kutter M, Hartung F (2000) Introduction to watermarking techniques. In: Katzenbeisser S, Petitcolas FAP (eds) Information hiding techniques for steganography and digital watermarking. Artech House, Norwood pp 97–120
20. Kutter M, Petitcolas FAP (1999) A fair benchmark for image watermarking systems. Proceedings of the SPIE electronic imaging, security and watermarking of multimedia contents, vol 3657. San Jose, California, pp 226–239
21. Macq B, Dewey F (1999) Trusted headers for medical images. Proceedings of the DFG VIII-DII watermarking workshop. Erlangen, Germany
22. Meerwald P, Uhl A (2001) A survey of wavelet-domain watermarking algorithms. Proceedings of the SPIE security and watermarking of multimedia contents, vol 4314. San Jose, pp 505–516
23. Miaou SG, Hsu CM, Tsai YS, Chao HM (2000) A secure data hiding technique with heterogeneous data combining capability for electronic patient records. Proceedings of the 22nd annual international conference on IEEE engineering in medicine and biology society. Chicago, pp 280–283
24. Nayak J, Bhat SP, Acharya RU, Niranjan UC (2004) Simultaneous storage of medical images in the spatial and frequency domain: a comparative study. Biomed Eng 3(1):17. Available via http://www.biomedical-engineering-online.com/content/3/1/17. Accessed 16 June 2004
25. Nikolaidis N, Pitas I (1999) Digital image watermarking: an overview. Proceedings of the international conference on multimedia computing and systems, vol 1. Florence, Italy, pp 1–6
26. Osborne D, Abbott D, Sorell M, Rogers D (2004) Multiple embedding using robust watermarks for wireless medical images. Proceedings of the 3rd international conference on mobile and ubiquitous multimedia. College Park, Maryland, pp 245–250
27. Paquet AH, Ward RK (2002) Wavelet-based digital watermarking for image authentication. Proceedings of the IEEE Canadian conference on electrical and computer engineering, vol 2. Winnipeg, Canada, pp 879–884
28. Puech W, Rodrigues JM (2004) A new crypto-watermarking method for medical images safe transfer. Proceedings of the 12th European signal processing conference. Vienna, Austria, pp 1481–1484
29. Su PC, Wang HJ, Kuo CCJ (1999) Digital image watermarking in regions of interest. Proceedings of the IS&T conference on image processing, image quality, image capture systems. Savannah, Georgia, pp 295–300
30. Swanson M, Kobayashi M, Tewfik A (1998) Multimedia data-embedding and watermarking technologies. Proc IEEE 86:1064–1987
31. Tian J (2002) Wavelet based reversible watermarking for authentication. Proceedings of the SPIE security and watermarking of multimedia contents, vol 4675. San Jose, pp 679–690
32. Trichili H, Bouhlel M, Derbel N, Kamoun L (2002) A new medical image watermarking scheme for a better telediagnosis. Proceedings of the IEEE international conference on systems, man and cybernetics, vol 1. Hammamet, Tunisia, pp 556–559
33. Unser M, Aldroubi A (1996) A review of wavelets in biomedical applications. Proc IEEE 84:626–638
34. Wakatani A (2002) Digital watermarking for ROI medical images by using compressed signature image. Proceedings of the 35th annual Hawaii international conference on system sciences. Big Island, Hawaii.

35. Wang HJM, Su PC, Kuo CCJ (1998) Wavelet-based digital image watermarking. Opt Express 3:491–496
36. Yang Y, Bao F (2003) An invertible watermarking scheme for authentication of Electronic Clinical Brain Atlas. Proceedings of the IEEE international conference on acoustics, speech, and signal processing. Hong Kong, pp 533–536
37. Zhou XQ, Huang HK, Lou SL (2001) Authenticity and integrity of digital mammography images. IEEE Trans Med Imaging 20:784–791
38. Zinger S, Jin Z, Maitre H, Sankur B (2001) Optimization of watermarking performances using error correcting codes and repetition. Proceedings of the joint conference on communications and multimedia security issues of the new century. Darmstadt, Germany, pp 229–240