Multiple Image Watermarking Applied to Health Information Management

Aggeliki Giakoumaki, *Member, IEEE*, Sotiris Pavlopoulos, *Member, IEEE*, and Dimitris Koutsouris, *Senior Member, IEEE*

***Abstract*—Information technology advances have brought forth new challenges in healthcare information management, due to the vast amount of medical data that needs to be efficiently stored, retrieved, and distributed, and the increased security threats that explicitly have to be addressed. The paper discusses the perspectives of digital watermarking in a range of medical data management and distribution issues, and proposes a complementary and/or alternative tool that simultaneously addresses medical data protection, archiving, and retrieval, as well as source and data authentication. The scheme imperceptibly embeds in medical images multiple watermarks conveying patient's personal and examination data, keywords for information retrieval, the physician's digital signature for authentication, and a reference message for data integrity control. Experimental results indicate the efficiency and transparency of the scheme, which conforms to the strict requirements that apply to regions of diagnostic significance.**

***Index Terms*—Authentication, image retrieval, integrity, medical confidentiality, multiple watermarking.**

I. Introduction

RECENT advancements in information and communication technologies have established a new context of easier access, manipulation, and distribution of digital data. New challenges arise as a result of implementing these constantly evolving technologies in healthcare systems, by forcing them to deal with a huge and exponentially increasing amount of medical data. Information technology developments have stimulated a continuous expansion and evolution of Digital Libraries in Medicine, which aim to provide fast and efficient data retrieval from enormous databases, in order to foster the creation of new knowledge, and to promote best practice in medical treatment planning. In this context, innovative ways of effectively representing and easily retrieving healthcare-related information are of foremost importance in the knowledge management field [1], [2]. Contemporary information access and distribution technologies raise additional critical issues that urgently need to be addressed, especially those related to security. The sensitive nature of patients' personal data necessitates further measures for medical confidentiality protection against unauthorized access. Source authentication and data integrity are also important matters relating to health data management and distribution [3]–[5]. The research community is mainly concerned nowadays with providing new ways of efficiently and if possible seamlessly, addressing all of the aforementioned issues.

Digital watermarking, a recently emerged research area, has the potential of providing alternatives for different issues associated with medical data management, confronting the new challenges arising from the exponentially expanding amount of information. This technology originally focused on copyright protection, but has since been exploited in a wide range of applications [6]–[11]. Despite the broad literature on various application fields, little work has been done toward the exploitation of health-oriented perspectives of watermarking [12]–[22]. Yet, digital watermarking has the potential of being a value-added tool for a range of issues relevant to health data management systems, such as medical confidentiality protection, patient- and examination-related information hiding, access and data integrity control, and information retrieval.

The present paper aims to reveal the potentials of digital watermarking in medical data management issues and proposes a multiple watermarking scheme, which conforms to the strict specifications regarding health data handling by preserving their quality and diagnostic value. The novelty of the method is that it simultaneously addresses a range of health data management issues through multiple watermarks embedded in medical images. It introduces an all-in-one tool providing alternative and/or complementary solutions to the existing ones regarding protection, archiving, and retrieval of medical data, as well as source and data authentication.

The paper is organized as follows. Section II briefly describes the main characteristics of digital watermarking and outlines the healthcare-related issues that could be approached by this technology. Section III introduces the proposed method and Section IV presents the results of our tests.

II. Health-Oriented Digital Watermarking Perspective

A. Digital Watermarking

Digital watermarking is the direct embedding of additional information through imperceptible modification of either the original data or a transformed version of them [23].

Manuscript received June 24, 2005; revised December 23, 2005. This work was supported in part by the General Secretariat for Research and Technology of the Hellenic Ministry of Development and in part by the European Union under the PENED program.

A. Giakoumaki and D. Koutsouris are with the Biomedical Engineering Laboratory, School of Electrical and Computer Engineering, National Technical University of Athens, Athens 15773, Greece (e-mail: agiakoum@biomed.ntua.gr; dkoutsou@biomed.ntua.gr).

S. Pavlopoulos is with the Institute of Communication and Computer Systems, National Technical University of Athens, Athens 15773, Greece (e-mail: spav@biomed.ntua.gr).

Digital Object Identifier 10.1109/TITB.2006.875655

Watermarking systems are characterized by a set of defining properties, whose relative importance depends on the requirements of the application [24]–[28]. There are various types of watermarks and the application fields of each are determined by the degree to which it meets the properties of imperceptibility, robustness, and capacity [29]. Robust watermarks resist common signal processing and malicious attacks, thus being appropriate for ownership verification and identity authentication applications. In this type of watermark, the amount of information that can be hidden in the host signal, the so-called capacity or payload, is not an important parameter, since the length of the identification code is usually limited to the minimum needed to guarantee uniqueness. On the contrary, a watermark destined to enrich the original data with additional helpful information should primarily meet the capacity criterion, without of course neglecting robustness. Fragile watermarks do not survive any transformations to the original data; therefore they are used for data integrity control and tamper detection.

In order to simultaneously address the above-mentioned range of healthcare applications, a set of conflicting requirements needs to be fulfilled. Since each of these applications requires different levels of robustness and capacity, multiple watermarks should be jointly embedded, each designed according to its corresponding restrictions and desirable properties, and being independently retrieved. So far, the literature on simultaneous embedding of multiple watermarks for different purposes remains limited [30]–[32].

Medical images have special characteristics and requirements; moreover, legal and ethical issues regarding the allowable operations on them are raised, since any compromise on the quality of medical images could result in misdiagnosis [20], [21], [33]. The strict specifications regarding the quality of medical images could be met by invertible watermarking, which allows the recovery of the original image without any loss of information [34], [35]. Another alternative is the selection of regions of interest (ROIs) having diagnostic significance, which are left intact by the embedding procedure [22]. The rest of the image can be used for watermarking with increased robustness and/or capacity, since it is not subjected to the strict imperceptibility requirements that apply to diagnosis-significant regions. However, it is deemed that watermarking methods that use the whole image without causing perceptible distortions can also be adopted in medical applications [21].

B. Medical Data Management Issues

Digital watermarking has the potential of providing alternative/complementary solutions for a number of issues relative to medical data management and distribution. A brief outline of digital watermarking perspectives in the healthcare sector follows.

1) Access Control: Digital watermarking enforces medical confidentiality protection by embedding patient's sensitive data into medical images. In this way, separate transmission and storage of metadata, which would increase memory and transmission bandwidth requirements, is prevented [16]–[18]. In addition, patient- and examination-related data are permanently linked to the image and more protected than in the case of metadata, since access to them is possible only through the use of a key [21], [36]. Hence, watermarking has the potential of being an alternative access control mechanism, since different keys might reveal different information [27].

2) De-identification: Although sensitive data must be kept secret from unauthorized persons, detachment of personal identification marks from medical data would allow their nonclinical use, thus promoting best-practice research. Watermarking enables a form of de-identification, since the embedded personal data remain protected and inaccessible to unauthorized users as long as the proper key is unknown.

3) Captioning: Watermarks serving as captions or annotations help in providing additional information about the patient's health history and other data contributing to a thorough patient status evaluation. Besides captioning and annotation, regions of diagnostic significance in an image can be highlighted through descriptive watermarks for future reference or other physicians' guidance [37].

4) Origin Identification: A watermark containing the physician's digital signature or identification code might be embedded in the images for identity authentication purposes [16]–[18]. Watermarking can be combined with cryptography, i.e., an encrypted version of the digital signature might be embedded in order to provide more complete protection [18], [27]. In this way, knowledge of both decryption and watermark keys is required for the recipient to obtain the original data, which grants an additional level of security.

5) Integrity Control: Since integrity of medical images is of paramount importance, efficient mechanisms supporting data integrity control are required in healthcare systems [20], [21]. Fragile watermarking provides a means to verify the integrity of transmitted or stored data, and even determines the tampered regions [38]. Comparing the extracted watermark with the original reference one allows the recipient to evaluate the extent of tampering, locate the modified parts, and determine whether the data are trustworthy for a precise diagnosis.

6) Indexing: Watermarks can play the role of keywords, based on which efficient archiving and data retrieval from querying mechanisms take place. Embedding markers and indices into the image eliminates storage and transmission bandwidth requirements [39]; these indices may include patient demographics, diagnostic codes (e.g., ICD-10), image acquisition characteristics, etc. In fact, picture archiving and communication systems (PACS) nowadays retrieve images through indexing [40], [41]. Recently, the use of image inherent characteristics to perform content-based querying in databases has been proposed [42]–[46]. In particular, some novel techniques use wavelet analysis of the image to derive characteristics suitable for image retrieval [47]; methods as the one proposed in this paper, which implement wavelet decomposition to perform image watermarking, could be easily adjusted to accommodate content-based querying.

The above considerations illuminate the potential of digital watermarking as a tool that facilitates data management in healthcare information systems. A method addressing the aforementioned issues by using multiple watermarking is described in the following section.

III. Proposed Method

A. Description of the Method

The proposed method decomposes the image to be watermarked using discrete wavelet transform (DWT). In general, transform-domain techniques outperform in terms of visibility and security, since they exploit perceptual properties in order to increase robustness without compromising imperceptibility [27], [48]. Wavelet analysis, in particular, has recently received considerable attention from the research community due to its ability to provide both spatial and frequency resolution [49], [50]. Besides, there is a considerable resemblance between the dyadic scaling decomposition of the wavelet transform and the signal processing of the human visual system (HVS), which allows adapting the distortion introduced by either quantization or watermark embedding to the masking properties of the human eye [51]. More specifically, the HVS splits an image into several frequency channels, which process the corresponding signals independently from each other; a similar image resolution into bands is performed by dyadic wavelet decomposition, which allows independent processing of the resulting components without significant perceptible interaction among them [52].

The proposed watermarking scheme addresses different issues involved in healthcare management systems, namely medical confidentiality protection, data integrity and access control, and efficient data management and retrieval, explicitly satisfying the strict imperceptibility requirement applied to medical images. Specifically, the method simultaneously embeds four different watermarks, each of them serving a different purpose.

1) A *signature* watermark containing the doctor's identification code is used for source authentication by the recipient.
2) An *index* watermark, comprising of keywords (e.g., ICD-10 diagnostic codes) that can be used for image retrieval by database querying mechanisms, is inserted as a distinct watermark.
3) A *caption* watermark, which contains patient's personal data, as well as additional data useful for the diagnosis, is also embedded; the caption watermark could actually include patient's demographics, health history, diagnostic reports, etc.
4) A *fragile* watermark is embedded in all decomposition levels for the purpose of data integrity control and tampering localization. The fragile watermark is actually a *reference* watermark [53], *a priori* known to the recipient; its extraction and subsequent comparison with the original one gives information on whether and where the image might have been tampered with. Such information could be derived by a difference image, which would map the locations of the distorted fragile watermark bits, and consequently of the possibly tampered image regions.

The watermarks are inserted in different decomposition levels and subbands depending on their type, and in locations specified by a random key; thus, they can be independently embedded and retrieved, without any interference among them. The reference watermark is embedded in coefficients throughout the entire image, in order to provide an overall image integrity control, whereas the signature, index, and caption watermarks are cast into parts of no diagnostic significance. In this way, ROIs carry only the information that is necessary to enable integrity control, thus preventing any compromise on the quality and diagnostic value of the image.

By integrating the tool in different medical image (e.g., CT, MRI, ultrasound) acquisition systems, different applications ranging from remote diagnosis and consultation to efficient medical data management, archiving, and retrieval within a hospital network, can be addressed. For instance, a use case is the following: When the image is acquired, the physician embeds in it information such as: his/her identification code, patient's personal and examination data, keywords for image indexing, and even additional information for other physician's guidance. The image is watermarked with these data and is subsequently stored in the hospital database. Then, the image can be retrieved by the database through querying mechanisms. Any authorized member of the healthcare personnel, having the appropriate key, can extract the embedded watermarks and gain access to information including: the patient's data, the identity of the physician who produced the image and verified the results, the diagnosis, etc. He/she can also extract the fragile watermark and examine the integrity of the image. A telematics use case involves watermarking the acquired image at a mobile unit and transmitting it to a base station (e.g., hospital) where the expert is located, providing an additional level of security to the transmitted data; the expert retrieves the embedded information from the image, makes a primary diagnosis, and gives directions to the mobile healthcare providers on how to handle the incident. The abovementioned use cases are only indicative; the proposed scheme could be used in a range of application scenarios in the medical field, providing an additional level of security and efficient health data management.

B. Algorithm

The multiple watermarks embedding procedure is based on a proper quantization of selected coefficients, which prevents rounding and consequent unacceptable modifications of watermark bits by providing integer changes in the spatial domain. This is possible due to the selection of the Haar wavelet for the image decomposition. The Haar wavelet transform produces coefficients that are dyadic rational numbers, i.e., their denominators are powers of 2 [54]; either addition to or subtraction from them of a multiple of 2^l, where l is the decomposition level, guarantees that the inverse discrete wavelet transform produces an image with integer pixel values [55]. This attribute is exploited in the embedding procedure described later and illustrated in Fig. 1.

In general, a wavelet transform produces detail coefficients, which are real numbers. The concept of the quantization procedure is as follows. Every detail coefficient is assigned a binary number through the quantization function

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

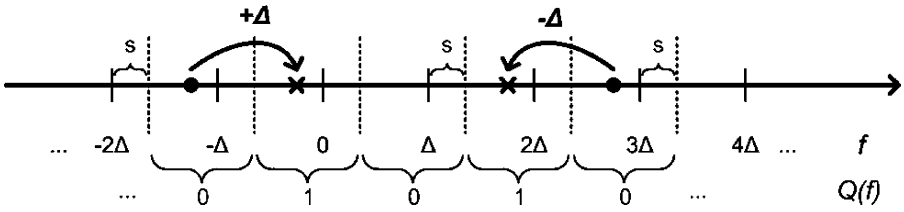


Fig. 1. Quantization procedure.

where k is an integer, s is a user-defined offset for increased security, and Δ, the quantization parameter, is a positive real number.

The above quantization function can also be written as

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

As previously stated, subtraction or addition of a multiple of 2^l to the Haar coefficients results in integer pixel values through the inverse discrete wavelet transform. Exploiting this attribute, the embedding procedure is based on the selection of an appropriate constant, which is either added to or subtracted from the coefficients that are chosen for watermark casting. Specifically, the quantization parameter Δ is defined as: $\Delta = 2^l$, where l, as previously defined, is the decomposition level.

The multiple watermarks embedding procedure is described below.

Step 1: The four-level Haar wavelet decomposition is performed to produce a gross image approximation at the lowest resolution level and a sequence of detail images, corresponding to the horizontal, vertical, and diagonal details at each of the four decomposition levels.

Step 2: On each decomposition level, a watermark bit w_i is embedded into the key-determined coefficient f according to the following:

a) If $Q(f) = w_i$, the coefficient is not modified.

b) Otherwise, the coefficient is changed so that $Q(f) = w_i$, using the following assignment:

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

Step 3: The watermarked image is produced by the corresponding four-level inverse wavelet transform.

It is noteworthy that the nature of the assignment in (3) has been shown by experiments to cause the least visual degradation to the image [55].

The multiple watermarks extraction requires knowledge of the key that was used in the embedding process. The extraction procedure involves four-level Haar wavelet decomposition of the watermarked image and key-based detection of the watermark locations. The multiple watermarks bits are extracted by applying the quantization function to each of the marked coefficients. If the signature watermark contains the physician's identification code encrypted with a private key, the corresponding public key must be applied to the extracted signature watermark in order to obtain the source authentication data.

C. Selection of Embeddable Coefficients

The watermark that contains the doctor's identification code requires great robustness in order to ensure the extraction of an intact digital signature and consequently to allow proper authentication. Capacity is not of paramount importance in the case of these watermarks, since the digital signatures that they convey are of limited length. The design of the scheme has been devised according to the above considerations; thus, the signature watermark is embedded in the fourth decomposition level, with the rationale that the more the decomposition level increases, the more robust the mark is. The capacity in this level is relatively low, but this is not a problem as far as the signature watermarks are concerned, as was previously explained. The need for robustness is also present in the case of the index and caption watermarks, but is not as crucial as in the former case, where even one bit error would result in authentication failure. On the other hand, both index and caption watermarks usually require more length, since they convey many bits of additional information. More specifically, the caption watermark of the scheme is destined to provide patient's personal and examination data or even parts of his/her health history, therefore the capacity requirement is of major concern. The index watermark carries keywords to be used for image retrieval, so the intended degree of capacity for this type of watermark lies between the degrees required for the signature and caption watermarks. Considering the above points, the index watermark is embedded in the third decomposition level of the image that provides an appropriate trade-off between robustness and capacity; the caption watermark on the other hand is embedded in the second decomposition level, which offers greater capacity. Finally, the first decomposition level is used for fragile watermarking to allow data integrity control; in order to provide an overall image modification evaluation, the reference watermark is embedded in selected coefficients of the other three decomposition levels as well.

In general, horizontal and vertical subbands have more or less the same characteristics and behavior, in contrast to diagonal ones [56]. A modification of the image is very likely to affect both horizontal and vertical detail coefficients, therefore these subbands are chosen to convey the data and the reference watermarks, respectively. Specifically in ultrasound images, the modality used in the simulations for this paper, the horizontal detail subbands include a significant energy portion, compared to both the vertical and the diagonal ones; this is

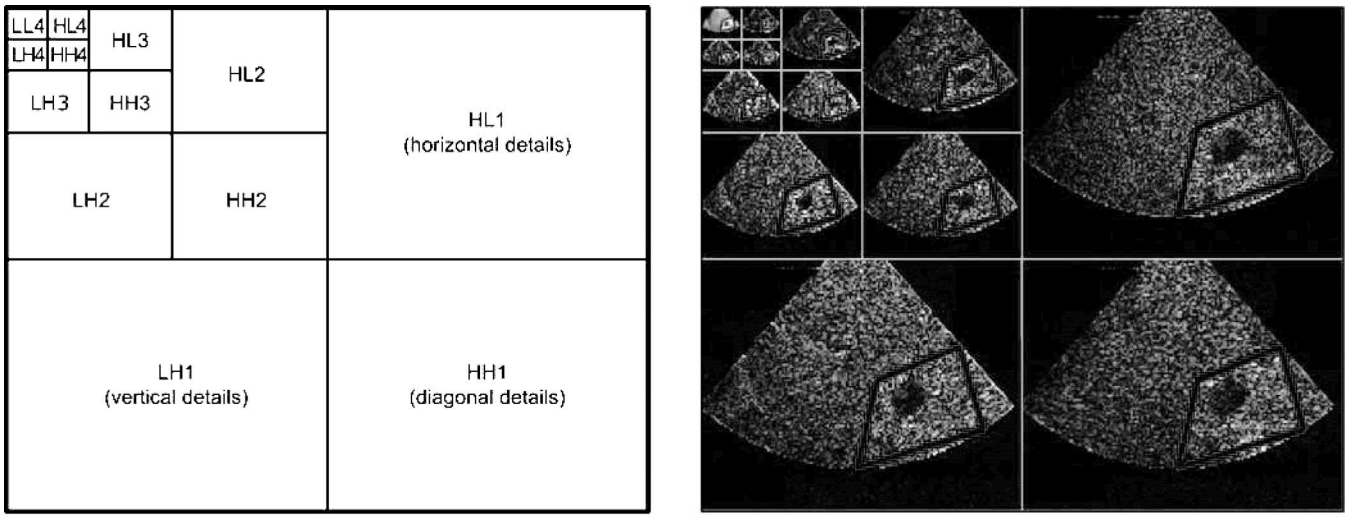


Fig. 2. Multiresolution wavelet decomposition of an image. (a) Pyramid structure of four-level DWT. (b) Four-level Haar DWT of an ultrasound image.

TABLE I
ENERGY OF APPROXIMATION AND DETAIL IMAGES OF A FOUR-LEVEL WAVELET DECOMPOSITION

Subband	Level 1	Level 2	Level 3	Level 4
Approximation	-	-	-	461.15
Horizontal Detail	8.50	13.27	25.85	62.70
Vertical Detail	5.15	10.15	18.92	43.42
Diagonal Detail	4.91	9.30	15.01	26.27

due to the elongation of ultrasound image speckle spots in the horizontal direction [57]. Fig. 2(a) illustrates the pyramid structure of a four-level wavelet decomposition of an image, comprising 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. Table I presents the energy of the approximation and the detail images produced by the four-level Haar DWT of an ultrasound test image shown in Fig. 2(b). The energy is calculated as follows:

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

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 and M_k are their corresponding dimensions. The table demonstrates that the energy is concentrated in the high decomposition levels corresponding to the perceptually significant low frequency coefficients; the low decomposition levels accumulate a minor energy proportion, thus being vulnerable to image alterations. The table also illustrates the fact that the horizontal subbands include remarkably more energy than the vertical and the diagonal ones. Thereupon, watermark embedding in the horizontal subbands guarantees increased robustness, since their energy compaction makes them less vulnerable to attacks. On the other hand, the coarse scale approximation includes most of the energy of the original image and has a crucial effect on image quality; therefore, it is not used for embedding, in order to retain imperceptibility. Aiming to ensure robustness of the watermarks conveying annotation, physician's identification code, and patient's personal data, diagonal detail subbands are not used either, as they have minor effect on image quality, which makes them prone to modification or elimination by common image processing, compression, or attacks. The above operations can easily eliminate the first decomposition level coefficients as well; this is the reason why these coefficients are selected only for fragile watermarking providing data integrity control, and not for signature, index, or caption watermarks embedding. The aforementioned points have been taken into consideration in the design of the watermarking scheme, in order to optimize the performance of robustness and invisibility.

In fear of a misdiagnosis, strict limitations apply to the acceptable alterations of medical images and especially of diagnosis-significant parts. Taking this into account, the proposed scheme allows the definition of a ROI and provides the option of using it exclusively for reference watermark embedding, thus reflecting its potential tampering. The rest part of the image, which is not subjected to the strict limitations of ROI, can be marked with all the watermarks. Usually, ROIs are defined when the images are acquired or archived; if this is not the case, an extended region can be defined to cover all potential diagnostically significant parts, in order to exploit the option of minimally watermarking the crucial region. It should be noted though that even when no ROI is defined and the whole image is used for multiple watermarking, there is no compromise on image fidelity; this will be discussed in more detail in Section IV.

Considering the increasing watermark robustness and the decreasing available capacity in ascending decomposition levels, the caption, index, and signature watermarks are embedded into key-dependent non-ROI horizontal detail coefficients of the second, third, and fourth level, respectively. The reference watermark is embedded into key-determined vertical detail coefficients of all four levels, corresponding to the whole image, thus

TABLE II
ALLOCATION OF WATERMARKS ACCORDING TO ROBUSTNESS AND CAPACITY CRITERIA

Selected Subband	Capacity (embeddable coefficients)	Embedded Watermark	
		Type	Robustness Requirement
LH1	20,480	Reference	Low
HL2	5,120	Caption	High
LH2	5,120	Reference	Low
HL3	1,280	Index	High
LH3	1,280	Reference	Low
HL4	320	Signature	Very High
LH4	320	Reference	Low

allowing an overall image tampering localization. The slight modification of single, sporadic vertical detail coefficients, even belonging to high decomposition levels, is expected to cause a minimal, imperceptible distortion, which does not affect the ROI fidelity; this assumption was validated in practice by our tests, as will be shown in Section IV. In case of tamper detection, computing fragile watermark similarity of each decomposition level provides a detailed distortion report. Table II presents the subbands used for each type of watermark and their corresponding capacity, i.e., the number of their coefficients, which represents the maximum amount of watermark bits that they can carry. The table illustrates the allocation of the four types of watermarks in the selected subbands according to both capacity and robustness criteria. It should be noted though that the capacity assigned to the horizontal subbands is the maximum one, which is available only when no ROI is defined; in any other case, the extent of ROI determines the amount of embeddable coefficients at each horizontal subband that are allowed to carry watermark bits, by not belonging to ROI.

As previously mentioned, the coefficients that will carry the watermarks are determined by a key. In fact, the key determines which vertical detail coefficients are to be marked with the reference watermark, regardless of whether they belong to ROI or not. In the case of the data watermarks, however, the selection of the embeddable horizontal detail coefficients is based on both the key and the ROI map: the key determines whether a specific coefficient is to be watermarked or not, but the latter will be used only if it belongs to non-ROI.

The wavelet-domain ROI map that determines the embeddable coefficients is derived from the spatial-domain ROI map, based on the spatial self-similarity between wavelet subbands [58]. Specifically, the spatial ROI map is divided into blocks of 16×16 pixels. If any pixel of the block belongs to ROI, the corresponding block of size 8×8 in the first decomposition level belongs to ROI as well. This corresponds successively to a block of 4×4 coefficients in the second level, a block of 2×2 in the third level, and a single coefficient in the fourth decomposition level. The correspondence among the ROI maps of a wavelet-transformed ultrasound image in four decomposition levels is illustrated in Fig. 2(b).

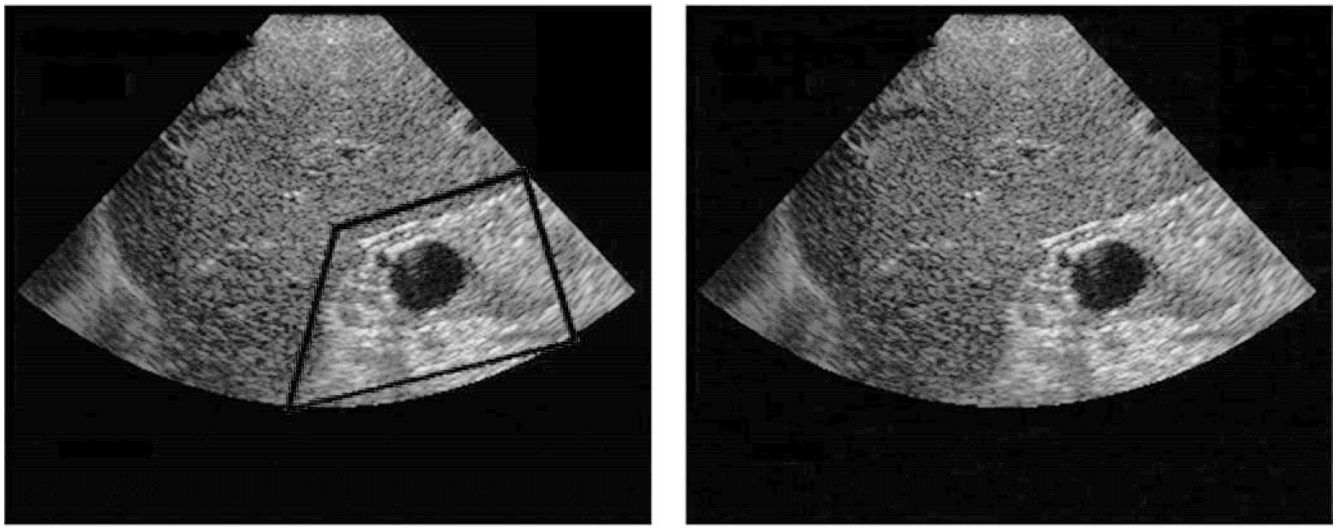
IV. RESULTS

The test set consisted of 50 ultrasound images of size 256×320 pixels; all images were collected by the same physician using the same equipment and ultrasound system settings, in order to avoid deviation in image statistics. All the watermarks are binary arrays from the set $\{0, 1\}$; in the simulations for the present paper specifically, the signature watermark containing the doctor's identification key is a 128-b watermark, randomly generated with a uniform probability distribution. The selected length of the identification key is sufficient to grant uniqueness to the key [32], [59]. The reference watermark is a binary array produced also by a uniform random number generator and has variable length, adequate to cover all the key-determined embeddable vertical coefficients. The index and caption watermarks are binary arrays produced by the ASCII codes of text files containing respectively, keywords and patient-/examination-related data. The set of keywords consisted of six words and a total of 52 characters, and the patient's data comprised of 23 words, of 208 characters in total. The resulting binary watermarks derived from these texts were of length 364 and 1456 b, respectively, due to the assignment of 7 bits per character by ASCII coding. Use of other sets of keywords and medical data for generating the index and caption watermarks would obviously result in different watermark lengths. In order to increase robustness of the embedded data (signature, index, caption), error correction coding was implemented; specifically, BCH encoding schemes were applied to the three watermarks [60]. Each watermark was split into parts of equal length, which were incorporated into suitably selected BCH codes. Table III illustrates the BCH coding schemes used for the above sets of data, as well as the number of their applications needed in order to comprehend the whole watermark arrays. 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 l bit errors. For instance, BCH (255, 91, 25) comprises a codeword of 255 b, which includes 91 b of the watermark to be embedded, and has an error correction capability of 25 b. Thus, in order for example to encode the 1456-b caption watermark using the specific BCH code, the watermark is split into 16 equal parts, and a separate BCH (255, 91, 25) is used for each part; this results in a total number of 4080 codeword bits that need to be embedded.

TABLE III
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

Both perceptual and signal qualities were assessed, due to the strict requirements concerning the acceptable alterations of medical images. A physician evaluated the perceptual quality of the watermarked images and found no visual difference between them and the original ones. Fig. 3(a) and (b) illustrates a test image and the resulting watermarked one, respectively. The quantitative assessment of the quality of the watermarked images was conducted using both the peak signal-to-noise ratio (PSNR) and the weighted PSNR metrics. The PSNR is not well correlated with perceptual quality, however, it provides an



(a) (b)

Fig. 3. Original and watermarked ultrasound images. (a) Original image. (b) Resulting watermarked image.

efficient measure of image distortion in terms of numerical values [33], [61], [62], which convey important information in medical applications, e.g., in the case of diagnosis support systems. The PSNR is measured in decibels and is defined as follows:

$$\mathrm{PSNR}(I,\hat{I}) = 10\log_{10}\left[\frac{\left(\max\limits_{\forall(m,n)} I(m,n)\right)^2}{\frac{1}{N_\mathrm{I}}\sum_{\forall(m,n)}(\hat{I}(m,n)-I(m,n))^2}\right] \quad (5)$$

where I and $\hat{I}$ are the original and watermarked images, respectively, N_I is the number of pixels in the image, and $\max\limits_{\forall(m,n)} I(m,n)$ is the maximum gray value of the original image. The denominator of the PSNR is the average sample mean squared error. The weighted PSNR (wPSNR) is a quality metric that assigns different weights to the perceptually different image regions, based on the noise visibility function (NVF) [63], [64]. The NVF reflects the masking properties of the HVS using a Gaussian model to estimate how much texture exists in any area of the image. For flat regions, the NVF value is close to 1, whereas for edge or textured regions, it is closer to 0. The wPSNR, also measured in decibels, is defined as follows:

$$w\mathrm{PSNR}(I,\hat{I}) = 10\log_{10} \times \left[\frac{\left(\max\limits_{\forall(m,n)} I(m,n)\right)^2}{\frac{1}{N_I}\sum_{\forall(m,n)}[(\hat{I}(m,n)-I(m,n))\cdot NVF(m,n)]^2}\right] \quad (6)$$

where $\mathrm{NVF}(m,n)$ is the NVF value corresponding to the pixel (m,n) and the other variables are defined as in (5).

Our experiments resulted in an average PSNR value of 45.70 dB, with a standard deviation of 0.10 dB, and an average wPSNR value of 47.41 dB, with a standard deviation of 0.21 dB.

TABLE IV
PERFORMANCE OF WATERMARKED AND JPEG IMAGES IN TERMS OF PSNR

Type of Image Processing		PSNR (dB)
Watermarked Image		45.70 ± 0.10
JPEG Compressed Original Image	Quality Factor 95	44.70 ± 0.50
	Quality Factor 90	39.99 ± 0.78
	Quality Factor 85	37.37 ± 0.92
	Quality Factor 80	35.65 ± 1.02
	Quality Factor 75	34.38 ± 1.10

TABLE V
PERFORMANCE OF WATERMARKED AND JPEG IMAGES IN TERMS OF WPSNR

Type of Image Processing		wPSNR (dB)
Watermarked Image		47.41 ± 0.21
JPEG Compressed Original Image	Quality Factor 95	47.09 ± 0.37
	Quality Factor 90	43.54 ± 0.60
	Quality Factor 85	41.39 ± 0.73
	Quality Factor 80	40.02 ± 0.80
	Quality Factor 75	39.06 ± 0.83

Although watermarked images are not compressed images, a comparison between the distortion induced by applying watermarks and the distortions introduced by image compression is intriguing [16], [17]. Tables IV and V present comparative evaluations of the distortions induced by applying the embedding scheme and JPEG compression with different quality factors, in terms of PSNR and wPSNR, respectively. As illustrated in the tables, the watermarking method introduces less distortion than the JPEG compression with quality factors of up to 95. The adequate perceptual quality of the watermarked images, combined with the high PSNR and wPSNR values obtained, demonstrates the transparency of the proposed scheme.

We have also tested the scenario that no ROI is defined and the multiple watermarks are embedded throughout the image. Using

TABLE VI
NORMALIZED HAMMING DISTANCE VALUES AS A FUNCTION OF JPEG QUALITY FACTOR

Quality Factor of JPEG Compressed Watermarked Image	Normalized Hamming Distance			
	Level 1	Level 2	Level 3	Level 4
95	0.44 ± 0.01	0.19 ± 0.01	0.09 ± 0.02	0.05 ± 0.02
90	0.48 ± 0.01	0.29 ± 0.02	0.14 ± 0.02	0.07 ± 0.03
85	0.49 ± 0.01	0.37 ± 0.02	0.16 ± 0.02	0.10 ± 0.03
80	0.50 ± 0.01	0.42 ± 0.02	0.17 ± 0.03	0.14 ± 0.04
75	0.50 ± 0.01	0.46 ± 0.02	0.24 ± 0.02	0.16 ± 0.04

TABLE VII
PERCENTAGE OF ERROR BITS IN EXTRACTED WATERMARKS

Type of Watermark		Signature	Index	Caption
Level of Embedding		4	3	2
JPEG Quality Factor	100	0	0	0
	95	0	0	14.90
	90	0	5.22	26.10
	85	0	15.93	33.17
	80	3.13	16.76	38.05
	75	4.69	17.86	39.08

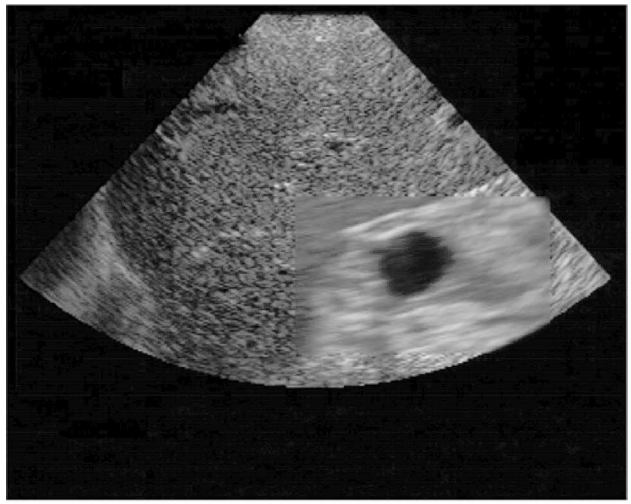
the same signature, index, and caption watermarks as in the ROI-based scenario, the PSNR and wPSNR values fell within the standard deviation of the above-presented results. This was anticipated, since the total amount of embedded information was the same in the two cases. The only difference lies in the distribution of the data watermarks (signature, index, caption) in the image; in the case of no ROI definition, certain coefficients of the diagnostically significant parts were watermarked, but still, no perceptible distortion that could alter the diagnostic content was revealed, as evaluated by the physician.

Table VI demonstrates the effects of applying JPEG compression with different quality factors to the watermarked images. In order to evaluate the degree of distortion, we selected the normalized hamming distance (NHD) as the similarity measure

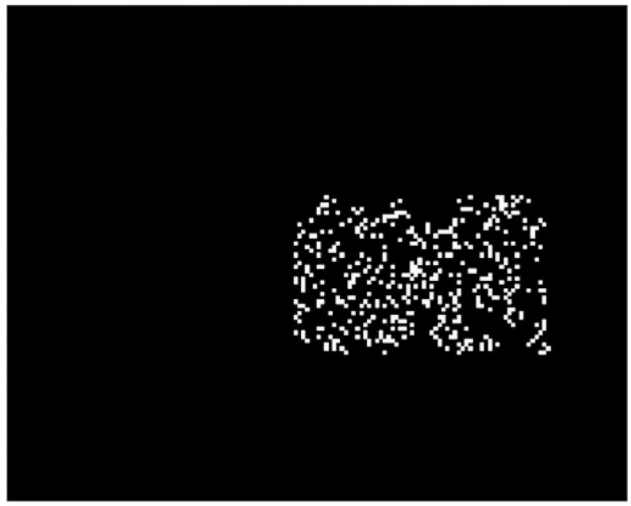
$$\mathrm{NHD}(w, \tilde{w}) = \frac{1}{N_{\mathrm{w}}} \sum_{i=1}^{N_{\mathrm{w}}} w(i) \oplus \tilde{w}(i) \tag{7}$$

where w and $\tilde{w}$ are the original and extracted fragile watermarks, respectively, N_{w} is the length of the watermark, and $\oplus$ is the exclusive-OR operator. The distance ranges between (0, 1) and application-dependent decision can be made concerning the integrity of the data. Obviously, in medical applications it should not exceed a small value, which would represent limited and negligible modifications of the image. Image modifications for specific spatial locations and/or frequencies can be evaluated by extracting the fragile watermark only from the corresponding watermarked coefficients. As expected, JPEG compression with lower quality results in larger NHD values.

The scheme was also tested in terms of robustness of the data watermarks to JPEG compression. Table VII illustrates the robustness of the watermarks conveying signature, index, and caption data, which were extracted from an ultrasound image after it was JPEG-compressed with different quality factors. As shown in the table, the signature watermark carrying the physician's identification code was extracted intact after JPEG compression with quality factor of at least 85. As expected, the tolerance of the index and caption watermarks to JPEG compression was less, due to the decreasing robustness in descending decomposition levels. It is noteworthy that, given the capacity provided by the specific image dimensions, the payload corresponding to the data sets used in these simulations restricts the error correction ratio. As far as uncompressed or slightly compressed images are concerned, the results of error correction are satisfactory. For further compression however, in order to achieve correct watermark extraction, we need to reduce the length of the watermarks and increase the number of redundant bits that will be used for a more effective BCH encoding. On the other hand, images of larger dimensions, e.g., 512×512 pixels, which is a typical size for many medical image modalities, offer greater flexibility in



(a)



(b)

Fig. 4. (a) Ultrasound image with a blurred region. (b) Tampering detection through the difference image of the 1st decomposition level reference watermark.

trade-off between conveying extended watermark arrays and an adequate amount of redundant bits providing enhanced correction ratio capability.

In order to demonstrate the potential of the reference watermark to locate a tampered region of the image, an ultrasound image was subjected to a blurring attack. Fig. 4(a) shows the original image which has a blurred region and Fig. 4(b) depicts the tampering detection derived from the difference between the embedded and extracted reference watermarks of the first decomposition level.

The above-presented experimental results of the performed tests demonstrate the efficiency of the proposed scheme in terms of robustness, transparency, and integrity control capability. It is noteworthy that the method has been tested on other medical imaging modalities too, namely MRA, CT, MRI, and PET, and the results were also satisfactory [65], [66]. Specifically, for all the imaging modalities tested, the watermarking scheme caused no distortion that could compromise the quality and diagnostic value of the images; besides its transparency, its satisfactory performance in terms of robustness and integrity control capability was also validated. Conclusively, the efficiency and applicability of the scheme in a range of medical imaging modalities, illustrate its potential to act as a value-added tool in health data management.

V. Conclusion

Digital watermarking has the potential to provide complementary and/or alternative solutions in a range of issues of critical importance to health informatics, namely origin and data authentication, and efficient medical data management, storage, and retrieval. The proposed multiple watermarking scheme addresses the above issues by imperceptibly embedding four types of watermarks into the wavelet coefficients of medical images. The experimental results demonstrate the efficiency of the scheme, which could be extended and integrated into healthcare information systems, in order to provide an additional level of security and a supportive tool for accurate diagnosis and best practice treatment. Given that the algorithm is based on wavelet decomposition and insertion of each type of watermark in a single subband, it could be efficiently coupled with JPEG2000 compression; this is due to the fact that it can fit the independent block coding strategy of the wavelet-based JPEG2000 standard, which precludes structures across subbands. Future work involves integration of the watermarking scheme with JPEG2000 compression, in order to provide a value-added tool for efficient storage and transmission of medical images.

References

[1] Y. C. Li, "Toward a medical information collective: Trends in the development of digital libraries in medicine," in *Yearbook of Medical Informatics 2001*, R. Haux and C. Kulikowski, Eds. Stuttgart, Germany: Schattauer, 2001, pp. 77–82.

[2] S. Chu, "Information retrieval and health/clinical management," in *Yearbook of Medical Informatics 2002*, R. Haux and C. Kulikowski, Eds. Stuttgart, Germany: Schattauer, 2002, pp. 271–275.

[3] *Security and Privacy: An Introduction to HIPAA*, Privacy and Security Committee, Medical Imaging Informatics Section, NEMA [Online]. Available: http://medical.nema.org/privacy/privacy.html

[4] Official Journal of the European Communities, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data*, [Online], L 281, pp. 31–50. Available: http://europa. eu.int/comm/transport/themes/air/english/library/directive-9546.pdf

[5] ACR Technical Standard for Digital Image Data Management. (2001). American College of Radiology Standard, Reston, VA. [Online]. Available: http://www.acr.org/s_acr/bin.asp?CID=541&DID=12210&DOC=FILE.PDF

[6] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proc. IEEE*, vol. 86, no. 6, pp. 1064–1087, Jun. 1998.

[7] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, no. 3–4, pp. 313–336, 1996.

[8] I. J. Cox and M. L. Miller, "The first 50 years of electronic watermarking," *EURASIP J. Appl. Signal Process.*, vol. 2002, no. 2, pp. 126–132, Feb. 2002.

[9] J. J. Eggers, R. Bauml, R. Tzschoppe, and J. Huber, "Applications of information hiding and digital watermarking," presented at the Proc. ECDL Workshop Generalized Documents, Darmstadt, Germany, Sep. 2001.

[10] N. Nikolaidis and I. Pitas, "Digital image watermarking: An overview," in *Proc. ICMCS99*, Florence, Italy, vol. 1, Jun. 7–11, 1999, pp. 1–6.

[11] F. Bartolini, A. Tefas, M. Barni, and I. Pitas, "Image authentication techniques for surveillance applications," *Proc. IEEE*, vol. 89, no. 10, pp. 1403–1418, Oct. 2001.

[12] W. Puech and J. M. Rodrigues, "A new crypto-watermarking method for medical images safe transfer," in *Proc. 12th Eur. Signal Process. Conf.*, Vienna, Austria, Sep. 2004, pp. 1481–1484.

[13] D. Osborne, D. Abbott, M. Sorell, and D. Rogers, "Multiple embedding using robust watermarks for wireless medical images," presented at the 2004 Proc. 3rd Int. Conf. Mobile Ubiquitous Multimedia, MA, Oct. 2004.

[14] M. Penedo, W. A. Peraman, P. G. Tahoces, M. Souto, and J. J. Vidal, "Embedded wavelet region-based coding methods applied to digital mammography," *Proc. IEEE Int. Conf. Image Process.*, vol. 2, pp. 197–200, Sep. 2003.

[15] B. Planitz and A. Maeder, "Medical image watermarking: A study on image degradation," presented at the Proc. Australian Pattern Recognition Society (APRS) WDIC, Brisbane, Australia, Feb. 2005.

[16] H.-M. Chao, C.-M. Hsu, and S.-G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Trans. Inf. Technol. Biomed.*, vol. 6, no. 1, pp. 46–53, Mar. 2002.

[17] S.-G. Miaou, C.-M. Hsu, Y.-S. Tsai, and H.-M. Chao, "A secure data hiding technique with heterogeneous data combining capability for electronic patient records," in *Proc. 22nd Annu. Int. Conf. IEEE EMBC*, vol. 1, Chicago, IL, Jul. 23–28, 2000, pp. 280–283.

[18] U. R. Acharya, D. Anand, P. S. Bhat, and U. C. Niranjan, "Compact storage of medical images with patient information," *IEEE Trans. Inf. Technol. Biomed.*, vol. 5, no. 4, pp. 320–323, Dec. 2001.

[19] X. Kong and R. Feng, "Watermarking medical signals for telemedicine," *IEEE Trans. Inf. Technol. Biomed.*, vol. 5, no. 3, pp. 195–201, Sep. 2001.

[20] A. Wakatani, "Digital watermarking for ROI medical images by using compressed signature image," presented at the Proc. 35th Annu., HICSS, Big Island, HI, 2002.

[21] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, "Relevance of watermarking in medical imaginga," in *Proc. 3rd Conf. ITAB'00*, Arlington, VA, pp. 250–255.

[22] G. Coatrieux, H. Maitre, and B. Sankur, "Strict integrity control of biomedical images," in *Proc. SPIE Security Watermarking Multimedia Contents III, SPIE 2001*, San Jose, CA, vol. 4314, Jan.2001, pp. 229–240.

[23] C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," *IEEE Signal Process. Mag.*, vol. 18, no. 4, pp. 33–46, Jul. 2001.

[24] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan Kaufmann, 2002, pp. 26–36.

[25] M. L. Miller, I. J. Cox, J.-P. M. G. Linnarzt, and T. Kalker, "A review of watermarking principles and practices," in *Digital Signal Processing in Multimedia Systems*, K. K. Parhi and T. Nishitani, Eds. New York: Marcell Dekker, 1999, pp. 461–485.

[26] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[27] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, no. 7, pp. 1069–1107, Jul. 2006.
[28] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," *Proc. IEEE*, vol. 87, no. 7, pp. 1108–1126, Jul. 1999.
[29] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Process. Mag.*, vol. 17, no. 5, pp. 20–46, Sep. 2000.
[30] F. Mintzer and G. W. Braudaway, "If one watermark is good, are more better?" in *Proc. Int. ICASSP'99*. Phoenix, AZ, Mar. 15–19, 1999, pp. 2067–2070.
[31] X. S. Hua, J. F. Feng, and Q. Y. Shi, "Public multiple watermarking resistant to cropping," presented at the 6th Int. Conf. Pattern Recognition and Information Processing, PRIP'2001, Minsk, Belarus.
[32] C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Proc.*, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.
[33] A. Bruckmann and A. Uhl, "Selective medical image compression using wavelet techniques," *J. Comput. Inf. Technol.*, vol. 6, no. 2, pp. 203–213, 1998.
[34] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding for all image formats," in *Proc. SPIE Photonics West, Security Watermarking Multimedia Contents*, San Jose, CA, vol. 4675, Jan.2002, pp. 572–583.
[35] ——, "Invertible authentication," in *Proc. SPIE Photonics West, Security Watermarking Multimedia Contents*, San Jose, CA, vol. 3971, 2001, pp. 197–208.
[36] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 474–481, May 1998.
[37] S. Shaw. (1999, Aug.). *Overview of Watermarks, Fingerprints, and Digital Signatures,* JISC Technology Applications Programme (JTAP). [Online]. Available: http://www.jisc.ac.uk/uploaded_documents/jtap-034.doc
[38] E. T. Lin and E. J. Delp, "A review of fragile image watermarks," in *Proc. ACM Multimedia Security Workshop*, Orlando, FL, Oct.1999, pp. 47–51.
[39] N. F. Johnson, "In search of the right image: Recognition and tracking of images in image databases, collections, and the internet," Center Secure Inf. Syst., George Mason Univ.Tech. Rep., Jun. 1999.
[40] G. P. Robinson, H. D. Tagare, J. S. Duncan, and C. C. Jaffe, "Medical image collection indexing: Shape-based retrieval using KD-trees," *Comput. Med. Imag. Graph.*, vol. 20, no. 4, pp. 209–217, Jul.–Aug. 1996.
[41] A. Corboy, W. Tsang, D. Raicu, and J. Furst, "Texture-based image retrieval for computerized tomography databases," in *Proc. 18th IEEE Int. Symp. CBMS'05* Jun. 23–24, 2005, pp. 593–598.
[42] H. D. Tagare, C. C. Jaffe, and J. Dunkan, "Medical image databases: A content-based retrieval approach," *J. Am. Med. Inform. Assoc.*, vol. 4, no. 3, pp. 184–198, May 1997.
[43] T. M. Lehmann, B. B. Wein, and H. Greenspan, "Integration of content-based image retrieval to picture archiving and communication systems," presented at the Proc. Medical Informatics Europe, MIE 2003, St. Malo, France, May 2003.
[44] C. Traina, A. J. M. Traina, R. R. Santos, and E. Y. Senzako, "A support system for content-based medical image retrieval in object oriented databases," *J. Med. Syst.*, vol. 21, no. 6, pp. 339–352, 1997.
[45] W. D. Bidgood *et al.*, "Image acquisition context: Procedure description attributes for clinically relevant indexing and selective retrieval of biomedical images," *J. Am. Med. Inform. Assoc.*, vol. 6, no. 1, pp. 61–75, Jan. 1999.
[46] T. Lehmann, B. Wein, J. Dahmen, J. Bredno, F. Vogelsang, and M. Kohnen, "Content-based image retrieval in medical applications: A novel multi-step approach," in *Proc. SPIE, Storage Retrieval Media Databases*, San Jose, CA, Jan. 2000, vol. 3972, pp. 312–320.
[47] E. Loupias, N. Sebe, S. Bres, and J. M. Jolion, "Wavelet-based salient points for image retrieval," in *Proc. ICIP*, Vancouver, Canada, vol. 2, Sep. 10–13, 2000, pp. 518–521.
[48] H. J. M. Wang, P. C. Su, and C. C. J. Kuo, "Wavelet-based digital image watermarking," *Opt. Express*, vol. 3, no. 12, pp. 491–496, Dec. 1998.
[49] M. Unser and A. Aldroubi, "A review of wavelets in biomedical applications," *Proc. IEEE*, vol. 84, no. 4, pp. 626–638, Apr. 1996.
[50] X. G. Xia, C. G. Boncelet, and G. R. Arce, "Wavelet transform based watermark for digital images," *Opt. Express*, vol. 3, no. 12, pp. 497–511, Dec. 1998.
[51] P. Meerwald and A. Uhl, "A survey of wavelet-domain watermarking algorithms," in *Proc. SPIE Security Watermarking Multimedia Contents III, SPIE2001*, San Jose, CA, vol. 4314, Jan. 2001, pp. 505–516.
[52] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," in *Proc. ICASSP'98*, Seattle, WA, vol. 5, pp. 2969–2972.
[53] ——, "Improved robust watermarking through attack characterization," *Opt. Express*, vol. 3, no. 12, pp. 485–490, Dec. 1998.
[54] J. Tian, "Wavelet based reversible watermarking for authentication," in *Proc. SPIE Security Watermarking Multimedia Contents IV, SPIE2002*, San Jose, CA, vol. 4675, Jan.2002, pp. 679–690.
[55] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," in *Proc. IEEE*, vol. 87, no. 7, Jul. 1999, pp. 1167–1180
[56] B. S. Kim, K. K. Kwon, S. G. Kwon, K. N. Park, K. I. Song, and K. I. Lee, "A robust wavelet-based digital watermarking using statistical characteristic of image and human visual system," in *Proc. 17th ITC-CSCC2002*, Phuket, Thailand, pp. 1019–1022.
[57] E. Chiu, J. Vaisey, and M. S. Atkins, "Wavelet based space-frequency compression of ultrasound images," *IEEE Trans. Inf. Technol. Biomed.*, vol. 5, no. 4, pp. 300–310, Dec. 2001.
[58] P. C. Su, H. J. Wang, and C. C. J. Kuo, "Digital image watermarking in regions of interest," in *Proc. IS&T Conf. Image PICS 99*, Savannah, GA, Apr. 25–28, 1999, pp. 295–300.
[59] A. H. Paquet and R. K. Ward, "Wavelet-based digital watermarking for image authentication," in *Proc. IEEE CCECE 2002*, Winnipeg, Canada, vol. 2, May 12–15, 2002, pp. 879–884.
[60] S. Zinger, Z. Jin, H. Maitre, and B. Sankur, "Optimization of watermarking performances using error correcting codes and repetition," in *Proc. 5th Joint Conf. Commun. Multimedia Security Issues of the New Century, IFIP TC6/TC11 CMS'01*, Darmstadt, Germany: Kluwer, May 2001, pp. 229–240.
[61] M. Kutter and F. A. P. Petitcolas, "A fair benchmark for image watermarking systems," in *Proc. SPIE Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, San Jose, CA, vol.3657, Jan.1999, pp. 226–239.
[62] M. Kutter and F. Hartung, "Introduction to watermarking techniques," in *Information Hiding Techniques for Stenography and Digital Watermarking*, S. Katzenbeisser and F. A. P. Petitcolas, Eds. Norwood, MA: Artech House, 2000, pp. 97–120.
[63] S. Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun, "Attack modelling: Towards a second generation watermarking benchmark," *Signal Process.*, vol. 81, no. 6, pp. 1177–1214, Jun. 2001.
[64] S. Voloshynovskiy, A. Herrigel, N. Baumgaertner, and T. Pun, "A stochastic approach to content adaptive digital image watermarking," in *Proc. Int. Workshop Inf. Hiding*, Dresden, Germany, Sep. 29–Oct. 1,1999, pp. 211–236.
[65] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Multiple digital watermarking applied to medical imaging," in *Proc. 27th Annu. Int. Conf. IEEE EMBC'05*, Shanghai, China, Sep. 1–4, 2005, pp. 3444–3447.
[66] ——, "Health data management through multiple watermarking of medical images," in *Proc. 3rd Eur. Med. Biol. Eng. IFMBE Conf., EMBEC'05*, vol. 11, Prague, Czech Republic, Nov. 20–25, 2005.

Aggeliki Giakoumaki (S'04–M'06) was born in Rhodes, Greece. She received the Diploma and the Ph.D. degrees in electrical and computer engineering from the National Technical University of Athens (NTUA), Athens, Greece, in 1999 and 2006, respectively.

Since 1999, she has been a Research Assistant at the Institute of Communication and Computer Systems, NTUA. Currently, she is with the Biomedical Engineering Laboratory, School of Electrical and Computer Engineering, NTUA. Her research interests include digital watermarking in medical applications, medical informatics, digital image processing, and telemedicine.

Dr. Giakoumaki is a member of the Technical Chamber of Greece and the IEEE Engineering in Medicine and Biology Society.

Sotiris Pavlopoulos (S'88–M'91) received the degree in electrical engineering from the University of Patras, Patras, Greece, in 1987 and the Ph.D. degree in biomedical engineering jointly from Rutgers University, New Brunwick, NJ, and Robert Wood Johnson Medical School, Piscataway, NJ, in 1992.

He is a Research Associate Professor at the Institute of Communication and Computer Systems, National Technical University of Athens, Athens, Greece. He has been active in a number of European and National R&D programs in the field of telematics applications in healthcare. He has published 8 book chapters, more than 40 journal articles, and more than 60 refereed conference papers. His research interests include medical informatics, telemedicine, medical image and signal processing, and bioinformatics.

Dimitris Koutsouris (M'96–SM'98) was born in Serres, Greece. He received the diploma in electrical engineering from the Technical University of Patras, Patras, Greece, in 1978, the DEA degree in biomechanics from the Rene Descartes University, Paris, France, in 1979, the Ph.D. degree in genie biologie medicale from the University of Paris XIII, Paris, France, and the Doctorat d' Etat degree in biomedical engineering from the University of Paris V, Paris, France, in 1984.

Since 1986, he has been a Research Associate with the University of California in Los Angeles, and the Rene Descartes in Paris, France. He was the Chairman of the Department of Electrical and Computer Engineering at the National Technical University of Athens (NTUA), Athens, Greece, from 1998 to 2000 and of the Greek Society of Biomedical Engineering from 1996 to 2000. Currently, he is a Professor of Biomedical Engineering at the NTUA. He has published over 100 research articles and book chapters and more than 150 conference communications. His research interests include medical informatics, telemedicine, clinical engineering, and biorheology.

Prof. Koutsouris is a member of the Technical Chamber of Greece, the International Society of Biomedical Engineering, and the European Society of Engineering in Medicine and Biology.