Proceedings of the 25th Annual International Conference of the IEEE EMBS
Cancun, Mexico • September 17-21, 2003

A medical image watermarking scheme based on wavelet transform

A. Giakoumaki, S. Pavlopoulos, D. Koutsouris
Biomedical Engineering Laboratory, School of Electrical and Computer Engineering, National Technical University of Athens, Greece

Abstract—**A wavelet-based multiple watermarking scheme is proposed, which addresses the problems of medical confidentiality protection and both origin and data authentication. The scheme embeds multiple watermarks serving different purposes: a robust watermark containing the doctor's digital signature for authentication, a caption watermark with patient's personal and examination related data, and a fragile watermark for the purpose of data integrity control. Thus, the proposed added-value tool offers alternatives for different issues associated with medical data management and distribution. The experimental results demonstrate the efficiency of the watermarking scheme, which fulfills the strict requirements concerning the acceptable alterations of medical images.**

Keywords—**Multiple watermarking, medical images, confidentiality, authentication, integrity**

I. Introduction

Recent advances in information and communication technologies have had a major impact on the development of healthcare systems. Hospital Information Systems (HIS) and Picture Archiving and Communication Systems (PACS) form the cornerstone of the modern integrated healthcare delivery systems, which provide easier access, manipulation, and distribution of medical data. In this context, additional measures are required in order to cope with the increased security risks. Due to the sensitive nature of patients' personal data, it is imperative to prevent unauthorized access and protect medical confidentiality. Furthermore, source authentication should take place, i.e. the doctor who produces and verifies the medical data should authenticate his/her identity. Another issue of critical importance is to safeguard medical data integrity, as unacceptable tampering of the data might result in misdiagnosis.

Digital watermarking is a recently emerged research area, which originally focused on copyright protection, but has since been exploited in a wide range of applications. Although there are only a few medical oriented watermarking studies in the literature to date [1-7], digital watermarking has also the potential of being a valuable tool for a variety of medical applications, such as medical confidentiality protection, patient and examination-related information hiding, data integrity control and source identification. Digital watermarking is the direct embedding of additional information through imperceptible modification of either the original data or some transformed version of them.

There are different kinds of watermarks, which meet the parameters of imperceptibility, robustness, and capacity to different degrees, so the choice of the watermark is application-dependent. Robust watermarks are resistant to both common signal processing and malicious attacks and are therefore appropriate for ownership verification. Capacity, i.e. the amount of information that can be hidden in the host signal, is not an important parameter in this type of watermarks. On the contrary, the purpose of the so-called caption watermarks is not to convey authentication data, but to enrich the original data with additional helpful information, therefore the capacity is of greater importance than the robustness in this case. Fragile watermarks address the problem of data integrity control and tamper detection, as they do not survive any transformations to the original data. There is no way a single watermark could meet the requirements of any application; since imperceptibility, robustness, and capacity conflict with each other, an application-dependent trade-off between them is necessary. So far, few are the methods that have addressed the problem of simultaneous embedding of multiple watermarks for different purposes [8,9].

Medical images have special characteristics and requirements compared to other digital images; moreover, legal issues regarding the allowable operations on them are raised, leading to a set of strict specifications. The proposed wavelet-based watermarking scheme addresses the issues of medical confidentiality protection, data integrity control and source identification, by simultaneously embedding multiple watermarks in an image, explicitly satisfying the strict imperceptibility requirement applied to medical images. The transmitted data include physician's digital signature, patient's personal and examination data, as well as a reference message, a priori known to the recipient, based on which tamper localization and assessment can take place.

II. Proposed Method

Transform domain embedding techniques offer a higher degree of robustness to common image processing operations, compared to spatial domain ones. Wavelet analysis, in particular, has recently received considerable attention due to its ability to provide both spatial and frequency resolution [10]. The dyadic frequency decomposition of the wavelet transform resembles the signal processing of the Human Visual System (HVS) and thus allows adapting the distortion introduced by either

0-7803-7789-3/03/$17.00 ©2003 IEEE

quantization or watermark embedding to the masking properties of the human eye [11]. The HVS splits an image into several frequency channels, which independently process the corresponding signals; a similar image resolution into bands is performed in dyadic frequency wavelet decomposition, which allows independent processing of the resulting components without significant perceptible interaction between them [12].

The proposed scheme embeds multiple watermarks in order to provide medical information systems with an additional level of security and physicians with an added-value tool for accurate diagnosis and efficient treatment planning. Specifically, the method embeds a robust watermark containing the physician's digital signature for the purpose of source authentication, and a caption watermark including patient's personal data, health history, diagnosis reports, etc. Additionally, a fragile watermark provides information on whether and where the image might have been tampered with [13].

A. Description of the Scheme

In the simulations for the present paper, both the robust watermark containing the doctor's identification key and the fragile one are randomly generated with a uniform probability distribution. The caption watermark is a binary array produced by the ASCII codes of a text containing patient's personal and examination data. The watermarks are embedded into selected detail coefficients of the host image, the exact locations of which are based on a key. For each decomposition level and spatial location, the key has a corresponding value of 1 or 0 to indicate if any coefficient of the examined location is to be marked or not, respectively.

The image is decomposed into three levels using Haar Discrete Wavelet Transform. The caption and robust watermarks are embedded into key-dependent horizontal detail coefficients of the second and third level respectively, and their associated reference watermarks into the corresponding vertical detail ones. The reference watermarks are actually repeated versions of the fragile watermark, which cover all the selected coefficients. The fragile watermark is also embedded into vertical detail coefficients of the first decomposition level, thus allowing an overall image tampering localization.

A modification of the image is very likely to affect both relative horizontal and vertical detail coefficients, as the corresponding sub-bands have more or less the same characteristics and behavior, in contrast to diagonal detail sub-band [14]. Thus, by selecting them to convey the data and the reference watermark, the latter reflects a potential distortion of the locations used for data embedding.

Since the coarse scale approximation includes most of the energy of the original image, it has a crucial effect on image quality and is therefore not used for embedding. Diagonal detail sub-bands 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 used just for fragile watermarking, in order to provide data integrity control. Since the HVS is less sensitive to noise in high-resolution bands, larger variations of the coefficient values are allowed in descending decomposition levels. 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.

B. The Algorithm

The multiple watermarks embedding procedure is based on a proper quantization of selected coefficients, which prevents rounding and subsequent unacceptable image alterations by providing integer changes in the spatial domain. This is possible due to the fact that the coefficients produced by Haar wavelet transform are dyadic rational numbers, i.e. their denominators are powers of 2 [15]. Thus, the addition or subtraction of a dyadic rational number to the coefficients guarantees that the inverse discrete wavelet transform produces an image with integer pixel values. The concept of the quantization procedure resembles the one introduced in [16] and is as follows: every detail coefficient, which is a real number, is assigned a binary number through the quantization function:

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

where Δ, the quantization parameter, is a positive real number. Considering both the dyadic rational form of the Haar wavelet coefficients and the decreased eye sensitivity to noise in high-resolution bands, the quantization parameter Δ is defined as follows:

$$\Delta = \frac{d}{2^{c+l}} \quad (2)$$

where c, d are user defined positive integers, and l is the decomposition level. The multiple watermarks embedding procedure is described below:

Step 1. The third level Haar wavelet decomposition of the image is performed to produce a gross image approximation at the lowest resolution level and a sequence of detail images at each of the three decomposition levels.

Step 2. In each decomposition level, a coefficient location (m,n) is selected for embedding if the associated value of the key is one. The caption and robust watermark bits are embedded into horizontal detail coefficients of the second and third decomposition levels respectively, and their associated reference watermark bits into the vertical

detail coefficients of the same spatial location (m,n). The fragile watermark bits are embedded into vertical detail coefficients of the first decomposition level. A watermark bit w_i is embedded into the selected coefficient f as follows:

- if $Q(f) = w_i$, the coefficient is not modified
- otherwise, the coefficient is changed so that $Q(f) = w_i$, using the following assignment:

$$f = \begin{cases} f + \Delta, & if\ f \le 0 \\ f - \Delta, & if\ f > 0 \end{cases} \quad (3)$$

Step 3. The watermarked image is produced by the corresponding third level inverse wavelet transform.

The multiple watermark extraction is performed by third level Haar wavelet decomposition of the watermarked image and key-based detection of the watermark locations. The multiple watermark bits are extracted by applying the quantization function to each of the marked coefficients.

The similarity measure used to evaluate the degree of distortion is the Normalized Hamming Distance, defined as follows:

$$NHD(w,\tilde{w}) = \frac{1}{N_w}\sum_{i=1}^{N_w} w(i) \oplus \tilde{w}(i) \quad (4)$$

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. As obvious, in medical applications it should not exceed a small value, indicating limited and negligible modifications of the image.

III. Results

The test set consisted of forty 256 x 320 ultrasound images, collected by the same physician using the same equipment and ultrasound system settings, in order to avoid deviation in image statistics. The lengths of the fragile, caption, and robust watermarks used in the experiments were 512, 696, and 128 bits respectively, and the chosen values of the quantization parameters are: $c = 2$, $d = 1$. Given that the two additional reference watermarks have the same length as their associated caption and robust ones, the total number of the watermark bits was raised up to 2,160. Due to the strict requirements concerning the acceptable alterations of medical images, both perceptual and signal qualities were assessed. Peak signal-to-noise-ratio (PSNR), although not well correlated with perceptual quality, is an efficient measure of image distortion in terms of numerical values, which convey important information in medical applications, e.g. in the case of diagnosis support systems. PSNR is measured in decibels and is defined as follows:

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

where I and $\hat{I}$ are the original and watermarked images respectively, N_I is the number of pixels in the image, and $\max_{\forall(m,n)} I(m,n)$ is the maximum gray-value of the original image.

Our experiments resulted in an average PSNR value of 41.93 dB, with a standard deviation of 0.62 dB. The perceptual quality of the obtained watermarked images was evaluated by a physician, who found no visual difference between them and the original ones. Fig. 1(a) shows a test image, the resulting watermarked image of which is illustrated in Fig. 1(b). Table I presents a comparative evaluation of the distortions induced by applying the embedding scheme and JPEG compression with different quality factors. As illustrated in the table, the embedding method introduces less distortion than the JPEG compression with quality factors of 75, 80, 85, and 90. The large PSNR values obtained, combined with the adequate perceptual quality of the watermarked images, demonstrate the efficiency of the proposed scheme.

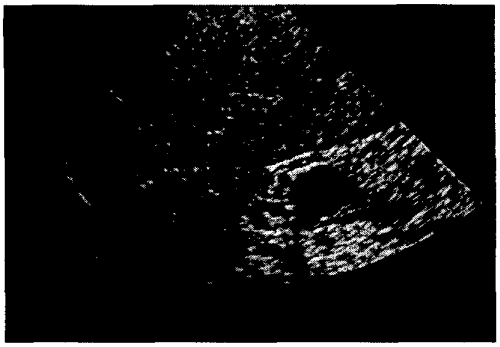
IV. Discussion

The proposed scheme addresses issues of critical importance to health informatics, namely medical confidentiality, identity authentication, and data integrity. Future work involves extensive embedding of the fragile watermark throughout all the decomposition levels, in order to provide a comprehensive tamper assessment. Besides, indices and markers could be inserted, in order to allow easy data retrieval by hospital database querying systems. This scheme could be extended and integrated into healthcare information systems, in order to provide an additional level of security, as well as a physician decision support tool for accurate diagnosis and efficient treatment planning.

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

Type of Image Processing		PSNR (dB)
Watermarked Image		41.93 ± 0.62
JPEG Compressed Original Image	Quality Factor 75	34.77 ± 1.30
	Quality Factor 80	36.03 ± 1.24
	Quality Factor 85	37.71 ± 1.15
	Quality Factor 90	40.29 ± 0.99
	Quality Factor 95	44.88 ± 0.68

(a)



(b)

Fig. 1. Original and watermarked ultrasound images. (a) Original image. (b) Resulting watermarked image.

V. CONCLUSION

A multiple watermarking scheme appropriate for medical images is proposed, which addresses the problems of medical confidentiality protection and authentication of both origin and data. The method uses Haar discrete wavelet transform to imperceptibly embed three types of watermarks into the wavelet coefficients of an image: a robust watermark containing the doctor's identification code, a caption watermark conveying patient's information, and a fragile watermark for tamper assessment. The latter is embedded in selected coefficients of all the decomposition levels, thus reflecting the potential image tampering extension. The experimental results indicate the efficiency of the proposed scheme.

ACKNOWLEDGMENT

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

REFERENCES

[1] H. M. Chao, C. M. Hsu, 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, March 2002.

[2] S. G. Miaou, C. M. Hsu, Y. S. Tsai, H. M. Chao, "A secure data hiding technique with heterogeneous data combining capability for electronic patient records," in *Proc. 22nd Annu. Intern. Conf. IEEE Engineering in Medicine and Biology Society, EMBS'00*, Chicago, USA, vol. 1, pp. 280-283.

[3] U. Rajendra Acharya, D. Anand, P. Subbanna Bhat, 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.

[4] X. Kong, R. Feng, "Watermarking medical signals for telemedicine," IEEE Trans. Inf. Technol. Biomed., vol. 5, no. 3, pp. 195-201, Sept. 2001.

[5] A. Wakatani, "Digital watermarking for ROI medical images by using compressed signature image," presented at the 35th Annu. Hawaii Intern. Conf. System Sciences, HICSS'02, Big Island, HI, USA.

[6] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, "Relevance of watermarking in medical imaging," in *Proc. 3rd Conf. Information Technology Applications in Biomedicine, ITAB'00*, Arlington, USA, pp. 250-255.

[7] G. Coatrieux, H. Maitre, B. Sankur, "Strict integrity control of biomedical images," in *Proc. SPIE Security and Watermarking of Multimedia Contents III, SPIE2001,* San Jose, USA, vol. 4314, pp. 229-240, Jan. 2001.

[8] X. S. Hua, J. F. Feng, Q. Y. Shi, "Public multiple watermarking resistant to cropping," presented at the 6th Intern. Conf. Pattern Recognition and Information Processing, PRIP'2001, Minsk, Belarus.

[9] C. S. Lu, H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Proc.*, vol. 10, no. 10, pp. 1579-1592, Oct. 2001.

[10] M. Unser, A. Aldroubi, "A review of wavelets in biomedical applications," in Proc. IEEE, vol. 84, no. 4, pp. 626-638, April 1996.

[11] P. Meerwald, A. Uhl, "A survey of wavelet-domain watermarking algorithms," in *Proc. SPIE Security and Watermarking of Multimedia Contents III, SPIE2001,* San Jose, USA, vol. 4314, pp. 505-516, Jan. 2001.

[12] D. Kundur, D. Hatzinakos, "Digital Watermarking Using Multiresolution Wavelet Decomposition," in Proc. *Intern. Conf. Acoustics, Speech and Signal Processing, ICASSP'98*, Seattle, WA, vol. 5, pp. 2969-2972.

[13] D. Kundur, D. Hatzinakos, "Improved robust watermarking through attack characterization," *Optics Express*, vol. 3 no. 12, pp. 485-490, Dec. 1998.

[14] B. S. Kim, K. K. Kwon, S. G. Kwon, K. N. Park, K. I. Song, K. I. Lee, "A robust wavelet-based digital watermarking using statistical characteristic of image and human visual system," in *Proc. 17th Intern. Conf. Circuits Systems Computers and Communications, ITC-CSCC2002,* Phuket, Thailand, pp. 1019-1022.

[15] J. Tian, "Wavelet based reversible watermarking for authentication," in *Proc. SPIE Security and Watermarking of Multimedia Contents IV, SPIE2002,* San Jose, USA, vol. 4675, pp. 679-690, Jan. 2002.

[16] D. Kundur, D. Xatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication," in *Proc. IEEE,* vol. 87, no. 7, pp. 1167-1180, July 1999.