Proceedings of the Eighth IASTED International Conference
Visualization, Imaging, and Image Processing (VIIP 2008)
September 1-3, 2008 Palma de Mallorca, Spain

MULTIPLE WATERMARK EMBEDDING AND BLIND EXTRACTION SCHEME IN WAVELET-SPATIAL DOMAINS BASED ON ROI

Maha A. Sharkas, Omneya A. Attallah, Ehab F. Badran
Department of Electronics and Communication, College of Engineering
Arab Academy for Science & Technology, 21937 Miami, Alexandria, Egypt
Email: msharkas@aast.edu, omneyaattallah@gmail.com, ebadran@aast.edu

ABSTRACT

Watermarking in medical images is a new area of research. It has the potential of being a value-added tool for medical confidentiality protection, patient-related information hiding, and information retrieval. Medical image watermarking requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality as this may cause misdiagnosis. In this paper we present a scheme that depends on the extraction of the ROI (region of interest) and its use as a watermark to be embedded twice; first as a robust watermark in the RONI (region of non interest) in the wavelet domain and again as a fragile watermark in the ROI in the spatial domain. Moreover multiple watermarks such as the physician’s digital signature and EPR (Electronics Patient Record) are embedded in the RONI in wavelet domain depending on a private key. In our work we use MRI brain images with a brain tumor as the ROI. The experimental results showed that the watermarked image has a PSNR of about 47db and our work is robust to JPEG compression, ROI removal, addition of an additional tumor to the image and some geometrical attacks such as image rotation.

KEY WORDS
Multiple watermarking, ROI, RONI, EPR, DWT, BCH.

1. Introduction

With the rapid development of information, communication, and computer technology, the amount of digital medical images has increased rapidly. The necessity of fast and secure diagnosis is vital in the medical world [1]. Medical images in digital form must be stored in a secured environment to preserve patient privacy. It is also important to prevent unintentional distortion and malicious modifications on the image’s perceptual quality. To achieve these objectives, digital watermarking techniques can be employed [2].

In digital watermarking, an imperceptible signal, referred to as a watermark, is embedded into multimedia data for various purposes [3]. The primary applications of watermarking are to protect copyrights and integrity verification [4]. Nowadays Watermarking in medical images is considered a new area of research. It has the potential of being a value-added tool for medical confidentiality protection, patient-related information hiding, and information retrieval [5]. Works reported in data hiding in medical image are watermarking for authentication, tamper detection of the images, EPR (Electronics Patient Record) hiding, image integrity control and efficient image archiving and retrieval. The medical images of different modalities with EPR attached to them can be sent to the clinicians residing at any corner of the globe for the diagnosis. Embedding of EPR with medical images will save storage space of the Hospital Information System, enhance confidentiality of the patient data and save the bandwidth required for transmission. Obviously this will reduce the cost of diagnosis.

Medical image watermarking requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality as this may cause a misdiagnosis [6].This kind of a system requires a high level of security, which can be ensured by using digital watermarking techniques [7]. Security of medical images, derived from strict ethics and legislative rules, gives rights to the patient and duties to the health professionals. This imposes three mandatory characteristics: confidentiality, reliability and availability: Confidentiality means that only the entitled persons have access to the images; Reliability has two aspects; Integrity: the image has not been modified by non-authorized person, and authentication: a proof that the image belongs indeed to the correct patient and is issued from the correct source; Availability is the ability of an image to be used by the entitled persons in the normal conditions of access and exercise [8].

Van Schyndel et al. [9] used the LSB method to modify the pixels. He added m-sequences simply to the LSB of the pixels in the spatial domain. Cross-correlation is used to test for presence of the watermark. Hyung-Kyo Lee et al. [10] presented a robust watermarking method for medical images that embeds the watermark with ROI information into the RONI .They considered the ROI as the whole brain without the background. Rodriguez Colin Raúl et al. [6] proposed a blind watermarking scheme that uses the metadata attached to an image. This data is compressed and encrypted and then used to generate an image which is considered as a watermark after the original image is centered by the momentum theory.

In this paper we present a multiple watermarking scheme for embedding four types of 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 [11]. The embedding process depends on the region of interest (ROI) which must be extracted first to be used as a watermark. The region of non interest (RONI) is used for embedding these watermarks in the wavelet domain according to a private key. These four watermarks include the digital signature of the doctor for the purpose of source authentication, EPR of the patient, the ROI as a robust watermark as an evidences if someone tried to remove it or to add additional tumor to the original image., and finally a fragile watermark which is embedded in the RONI in the wavelet domain and in the ROI in the spatial domain to provide information on whether or not the image is tampered [11]. We used MRI brain images with brain tumors as a ROI. The watermark extraction is blind i.e. in the extraction process; the host image is not needed to recover the watermark, only the secret key used in embedding is required.

2. Scheme Presented

Discrete Wavelet Transform (DWT), in particular, has recently received considerable attention due to its ability to provide both spatial and frequency resolution. It exhibits a strong similarity to the way-the Human Visual System (HVS) processes images. It can be used as a computationally efficient version of the frequency models for the HVS .The dyadic frequency decomposition of the DWT resembles the signal processing of the HVS and thus allows adapting the distortion introduced by either quantization or watermark embedding to the masking properties of the human eye. DWT decomposes an image into a set of band limited components which can be reassembled to reconstruct the original image without error [11], [12] and [13].

The host image and its watermarked version are shown in Fig. 2 (a) and (b). In our work the ROI is first separated from the RONI using the threshold algorithm proposed in [14] as shown in Fig. 3 (a) and (b) respectively. In medical images ROI is an area which contains important information and must be stored without any distortion [10]. We considered the ROI as the brain tumor and RONI as the rest of the image, The RONI is decomposed into four decomposition levels using Haar DWT as shown in Fig. 4 where we embed all the watermark types. The ROI is used as a watermark. In the next section we will explain how it is generated. It is embedded twice; first into horizontal and vertical detail coefficients of the third decomposition level, then in LSB of the ROI spatial domain. The physician's digital signature is embedded into horizontal detail coefficients of the fourth decomposition level. The EPR of the patient is embedded into the horizontal detail coefficients of the second level after applying the BCH error correction code to it. Finally a fragile watermark is embedded into the vertical detail coefficient of the first decomposition level. Embedding of all previously mentioned watermarks depends on a key which will be explained in the following section.

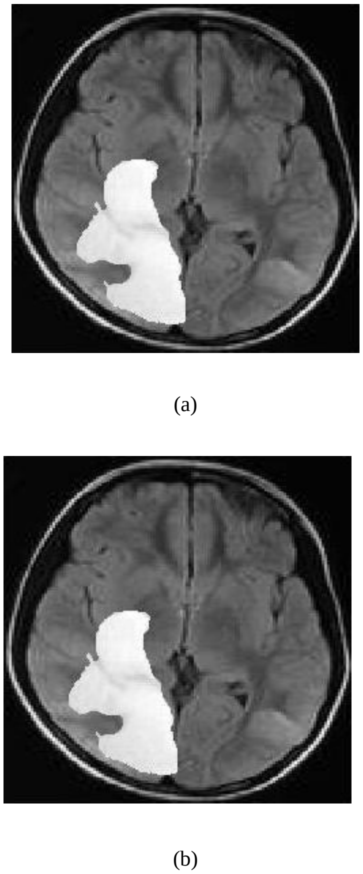
3. Algorithm used

Our algorithm is divided into four main steps; key generation, watermark generation, quantization and embedding. key generation depends on a secret threshold which is used to embed and extract the watermark and provides an addition level of security [15].The key at each decomposition level is generated by first centering each wavelet sub-band, then scanning it in a spiral way using the center of the sub-band as the origin of this scan [6]. This procedure selects the possible coefficients where the watermark could be embedded using a certain secret threshold. The coefficients which are chosen for embedding are given the binary bit one and vice versa. This key avoids embedding in the ROI locations in all sub-bands of the decomposition levels. The key of the fragile watermark embedded in the ROI is also generated as the previously mentioned method; the only difference is that it is generated from the ROI spatial domain. The embedding process is also done in the same spiral manner.

The ROI which is in our case the brain tumor after its extraction from the image is decomposed into three wavelet decomposition levels. The approximation sub-band is converted into a binary image as shown in Fig .1. The binary image is then divided into even and odd bits and embedded as a robust watermark into the horizontal and vertical detail coefficients of the 3^{rd} decomposition level respectively. This binary image is embedded again as a fragile watermark in the LSB of the pixel values of ROI in the spatial domain. The LSB method is used as it has a lower affect on the ROI degradation.

Fig. 1. ROI as a binary image

Physician's digital signature and the fragile watermark are binary PN sequences generated by a different private seed and generator; each with different length. They are embedded into the horizontal and vertical detail coefficients of the fourth and first decomposition levels respectively. The reason for using PN sequences is that they are reliable; as when the receiver receives the watermarked image and extracts this type of watermark, it



(a)

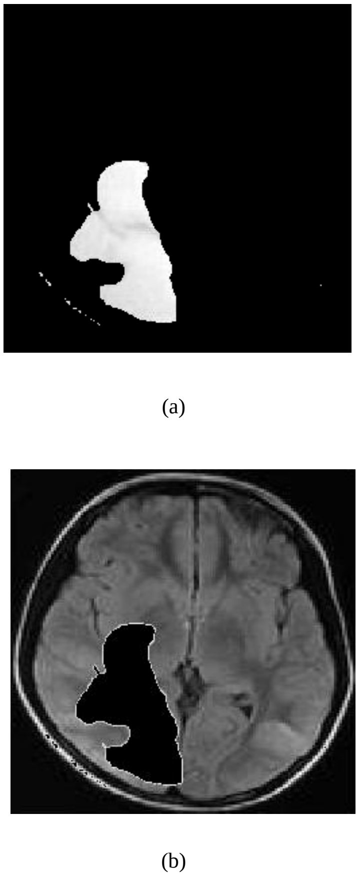
(b)

Fig. 2. (a) the original image,(b) watermarked image

compares it with many PN sequences generated from the same generator. A similarity measure is used to detect the similarity between them. The one which has the closest similarity is the embedded one. Finally the EPR as a watermark is formed by the binary representation of ASCII codes of the EPR file. Each ASCII character is represented by 7 binary bits. In order to lower the percentage of bits that are received in error we encode the watermark with a BCH error correction code.

Multiple watermarks embedding steps are made in a spiral manner. It is based on proper quantization of selected coefficients, which prevent 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; either addition to or subtraction from them of a multiple of 2, guarantees that the inverse discrete wavelet transform produces an image with integer pixel values [16]. The concept of the quantization step is as follows.

Every detail coefficient is assigned a binary number through the quantization function:



(a)

(b)

Fig. 3. (a) ROI image which represents the brain tumor, (b) RONI image

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

Specifically, the quantization parameter Δ is equal to 2^L; where L, is the decomposition level, s is defined by the user for increasing the level of security.

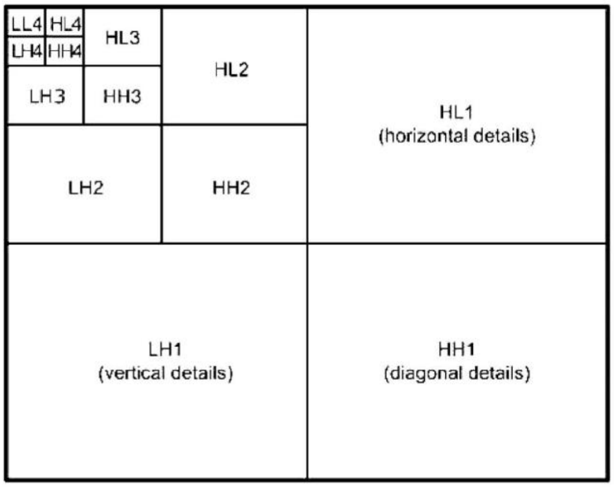


Fig. 4. Four level wavelet decomposition

The embedding procedure is made in 4 steps similar to the one in [16], but the ROI is watermarked by a different method which is described later. At each decomposition level, if the key bit is one, the quantized binary bit *Q(f)* is compared with the watermark bit *wi.* If they are similar the coefficient is not modified otherwise it will be modified so that *Q(f)= wi* as follows :

$$f = \begin{cases} f+\Delta, & if \quad f \le 0 \\ f-\Delta, & if \quad f > 0 \end{cases} \tag{2}$$

Applying the inverse DWT produces the watermarked image without watermarking the ROI locations. The ROI which is the brain tumor is then watermarked by a fragile watermark for the purpose of tamper detection. By using the LSB method in the spatial domain the ROI binary image is used as a watermark to be embedded directly in pixels of the ROI locations by interchanging the lower order bits of the pixels with that of the watermark The main advantage of the spatial domain techniques of watermark embedding is the relatively low calculation when compared to any technique requiring domain transforms [17], and has a minor effect on the tumor image quality. Finally the final watermarked image is formed as shown in Fig. 2(b).

It is important to know the key of each sub-band used in the embedding step when extracting the multiple watermarks. It is a blind procedure; we don't need the unwatermarked version of the image to extract the watermarks embedded. The extraction procedure is similar to the embedding one. We extract the fragile watermark from the ROI then we apply the same decomposition and quantization procedures.

4. Experimental Results

In our experiments we used 256 x 256 MRI brain images with brain tumor. The physician's digital signature is a binary PN sequence of length 127 bits. The EPR is the binary representation produced by the ASCII codes of the EPR file and its length is 1050 bits. The BCH encoding scheme was applied to EPR binary representation. It was split into parts of equal length, and incorporated into suitably selected BCH codes [16]. Here we used (127, 50, 13) BCH encoding scheme. ROI binary image which is used as a watermark is of length 1024 bits and was split into even and odd bits of length 512 bits each. When the ROI binary image embedded in the wavelet domain is extracted we filtered it with a median filter for better results. The fragile watermark embedded into the wavelet domain is a PN sequence of length 4095 bits. The embedded watermarks must not affect the image quality. This condition is very important in the medical field since the medical information is very important for the diagnosis of the patient's condition. Artifacts in a patient's diagnostic image may cause errors in diagnosis and treatment with possible life threatening consequences. As an objective quantity, the peak signal to noise ratio (PSNR) which is calculated from (3) is used to present the distortion caused by watermarking [17]. We applied several attacks to demonstrate the efficiency of our presented scheme, examples for such attacks are; JPEG compression, tumor removal, external tumor addition, image rotation and changes in the image contrast. It is necessary for watermark extraction under image rotation attack that the watermarked image returns to its original position after applying this attack. In our results the watermark extracted is under this attack is exactly similar to the embedded. Fig. 5-7 demonstrate some of the suggested attacks. Tables I-V show our results.

$$PSNR = 10 * \log_{10} \frac{255^{2}}{MSE} \tag{3}$$

$$MSE = \frac{1}{MN} \sum_{m=1}^{M} \sum_{n=1}^{N} e(m,n) \tag{4}$$

Where *MSE* is the mean square error and it is calculated from (4), *e(m,n)* is the difference between the watermarked and original un-watermarked images, and *M by N* is the image size.

Finally we used the normalized hamming distance (NHD) as a similarity measure to determine the degree of similarity between the embedded and extracted watermarks.

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

Where w and $\tilde{w}$ are the embedded and extracted watermarks respectively. *Nw* is the length of the watermark. The distance ranges between (0,l) 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 [11].

5. Conclusion

In the medical field, the number of digital images used for diagnostics and therapy are produced in great quantities and are increasing rapidly. At the same time medical image protection and authentication are becoming increasingly important in an e-Health environment. Watermarking medical images is considered as an additional tool that offers medical confidentiality protection, patient-related information hiding, and information retrieval. In this paper we presented a multiple watermarks embedding scheme for embedding four types of watermarks in order to addresses the above issues, provide medical information systems with an additional level of security and physicians with an added value tool for accurate diagnosis and efficient treatment planning and . Our experimental results showed the efficiency of the presented scheme. As for future work we may work on increasing the robustness against more attacks.

Fig. 5. Fragile watermark extracted under; ROI removal (left); JPEG compression (right)

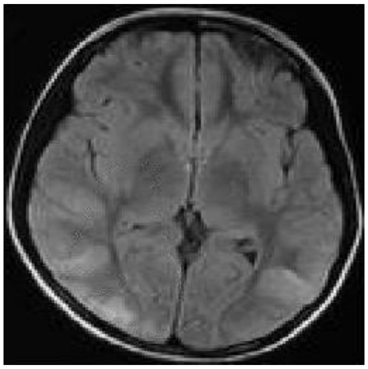


Fig. 6. Brain after the ROI removal attack

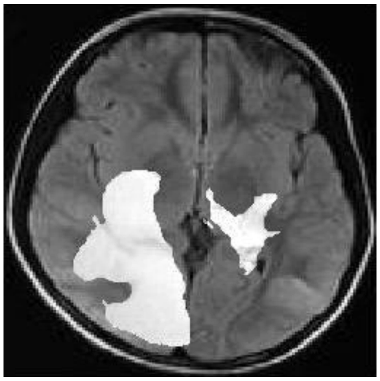


Fig. 7. Brain after the addition of a tumor

Table I
NHD under JPEG compression

JPEG Compressed watermarked Image (Q-factor)	NHD of the Digital Signature	NHD of the EPR
75	0.0709	0.3990
80	0.1102	0.3371
85	0.0551	0.2914
90	0.1024	0.2276
95	0.0866	0.1381

Table II
PSNR of the JPEG compressed original image

Watermarked Image	PSNR (dB) = 47.3489
JPEG Compressed Original Image (Q-factor)	PSNR (dB)
70	40.7829
75	41.8812
80	44.3966
85	47.0271
90	48.9997
95	50.3947

It is clear in Table II that the PSNR of the watermarked image is greater than that of the original image subjected to JPEG compression up to a quality factor of 85.

Table III
NHD and PSNR under JPEG attack

JPEG Compressed watermarked Image(Q-factor)	PSNR (dB)	NHD Tumor Hidden
70	41.9908	0.0400
80	42.7302	0.0234
85	43.3668	0.0234
90	44.5576	0.0098
95	46.7063	0.0107

Table IV
NHD under ROI removal attack

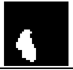
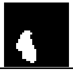
	NHD
Hidden Tumor	0.0088 
Digital Signature	0.0079
EPR	0

Table V
NHD after adding a new tumor

	NHD
Hidden Tumor	0.0088 
Digital Signature	0.0472
EPR	0.0048

References

[1] W.Puech, and J.M.Rodrigues, A new crypto-watermarking method for medical image safe transfer, *Proc. 12th European Signal Processing Conference (*EUSIPCO'04*)*, Vienna, Austria, September 2004, 1481-1484.

[2] C.Woo, J.Du, and B.P. Chen, Multiple watermark method for privacy control and tamper detection in medical images, *Proc. APRS Workshop on Digital Image Computing (WDIC)*, Brisbane, South bank, 2005,59-64.

[3] S. Lee, C.D. Yoo, and T. Kalker, Reversible image watermarking based on integer to integer wavelet transform, *IEEE Trans.Information forensics and security.;v*ol. 2,no. 3,September 2007,.321-330.

[4] M. Kallel, J. Lapayre, and M.S. Bouhlel, A multiple watermarking scheme for medical image in the spatial domain, *GVIP Journal, Volume 7,* Issue 1, 2007.

[5] G. Sun, et al., Combination independent content feature with watermarking annotation for medical image retrieval, *Proc. Second Conference on Innovative Computing, Information and Control, ICICI* **,** 2007, 607-607.

[6] R. Raúl et al., Hiding scheme for medical images , *Proc .17th International Conference on Electronics, Communications and Computers,* 2007, 32-32.

[7] K. A. Navas , M. Saesikumar, and S. Sreevidya, A benchmark for medical image watermarking, *Proc. 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services,* June, 2007, 237-240.

[8] M. Zain, and R. M Fauzi, Medical image watermarking with tamper detection and recovery, *Proc. 28th IEEE EMBS Annual International Conference,* New York, USA, 2006*, 3270-3273.*

[9] R. van Schyndel, A. Tirkel, and C. Osborne, A digital watermark, *Procs.. of the IEEE International Conference on Image Processing*, vol. 2, Austin, Texas, 1994, 86-90.

[10] H.K. Lee et al., ROI medical image watermarking using DWT and bit-plane, *Proc. Asia-Pacific Conference on Communications*, 2005, 512 – 515.

[11] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, A medical image watermarking scheme based on wavelet transform, *Proc. 25th Annual International Conference of the IEEE EMBS* Cancun, Mexico, 2003, 17-21.

[12] K. Nallaperumal et al., A wavelet transform based digital image watermarking and authentication**,** *Proc. Annual India Conference***,** New Delhi, 2006, 1-6.

[13] R. Mehul, P. Rege , Discrete wavelet transform based multiple watermarking scheme, *Proc. Conference on Convergent Technologies for Asia-Pacific Region***,** *Vol.3*, 2003, 935- 938.

[14] O.A. Alim, N. Hamdy, W.G. El-Din, Determination of the Region of Interest in the Compression of biomedical Images, *Proc. Radio Science Conference (NRSC 2007),* Cairo,Egypt, 2007, 1 – 6.

[15] K Pushpala, R Nigudkar, A novel watermarking technique for medical image authentication**,** *Proc. Computers in Cardiology*, 2005, 683- 686.

[16] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, Multiple image watermarking applied to health information management, *IEEE Trans. Information Technology in Biomedicine, vol. 10,* no. 4, 2006, 722-732.

[17] I.F Kallel et al., Fragile watermarking for medical image authentication, *Proc. The 2nd International Conference on Distributed Frameworks for Multimedia Applications*, 2006, 1-6.