



Energy Based Wavelet Domain Medical Image Watermarking

K.Anusudha¹, N.Venkateswaren²

Department of Electronics Engineering, Pondicherry University, Pondicherry, India¹

Department of Electronics and Communication Engineering, SSN College of Engineering, Chennai, India²

ABSTRACT: Modern healthcare systems are based on managing diagnostic information of patients in a digital way. To guarantee the security, authenticity and management of medical images and information through storage and distribution, the watermarking techniques are used. This paper aims at developing a watermarking technique in wavelet domain which uses the Electronic Health Record (EHR) as watermark and hospital logo as the reference image. Embedding of the EHR data is based on energy band selection and in reference to the bit location in the reference image. Performance of the proposed method was tested for four modalities of medical images; MRA, MRI, Radiological, and CT. Simulation results show no visible difference between the watermarked and the original image. Moreover, the proposed watermarking method is robust against a wide range of attacks such as JPEG compression, Gaussian noise addition, histogram equalization, contrast adjustment, sharpening and rotation.

KEYWORDS: Medical image watermarking (MIW), Electronic Health Record (EHR), Discrete Wavelet Transform (DWT).

I. INTRODUCTION

Telemedicine combines Medical Information System with information technology that includes use of computers to receive, store and distribute medical information over long distances. Currently, telemedicine applications in teleconsulting, telediagnosis, telesurgery and remote medical education play a vital role in the evolution of the healthcare domain [1]. The transmission, storage and sharing of electronic medical data *via* the networks have many purposes such as diagnosis, finding new drugs and for scientific research. Exchange of medical image between hospitals located in different geographical locations is a common practice. Hence, healthcare industry demands secure, robust and more information hiding techniques promising strict secured authentication and communication through internet or mobile phones.

In general information hiding includes digital watermarking and steganography [3]. A watermarking scheme imperceptibly alters a cover object to embed a message about the cover object (e.g owner's identifier) [4]. Watermarking is used for copyright protection, broadcast monitoring and transaction tracking and thus robustness of digital watermarking schemes becomes critical. In contrast, steganography is used for secret communications. A Steganographic method undetectably alters a cover object to conceal a secret message. Thus, steganographic methods can also hide the very presence of covert communications.

In general, digital watermarking algorithms can be divided into two classes depending on the domain of watermark embedding. The first group belongs to the algorithms which uses spatial domain for data hiding [13,14], while algorithms of the second group take advantage of transform domain like Discrete cosine Transform (DCT) [7], Discrete Fourier Transform (DFT) [15] and Discrete Wavelet Transform (DWT) [16] for watermarking purpose. Previous works reveals that transform domain schemes are typically more robust to noise, common image processing tasks and compression when compared with spatial transform schemes [17]. Digital watermarking can also be categorized into visible and invisible, fragile and robust, blind and non-blind with emphasis on authentication, rightful ownership, availability of the host image etc.



International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

Researchers proposed watermarking techniques and reported findings in the literature survey both integrity and confidentiality requirements (Wang et al.,2000; Zhou et al,2001;Chao et al,2002;Giakoumaki et al,2003;Shieh et al,2004; Piva et al,2005;Xuan et al,2006;

Wang et al[6] proposed to embed secret messages in the moderately significant bit of the cover image. A genetic algorithm is developed to find an optimal substitution matrix for the embedding of the secret messages. They also proposed to use a local pixel adjustment process (LPAP) to improve the image quality of the stego image. As the local pixel adjustment process modifies the LSBs, the technique cannot be applied to data hiding schemes based on simple LSB substitution. Zhou et al [7] presented a method that attaches digital signature and EPR into the medical image. Their method uses LSB replacing technique to embed the signature. Chao et al [8] proposed a secure data hiding technique based on the bipolar multiple base conversion to allow a variety of EPR data to be hidden within the same mark image.Giakoumaki et al [9] presented a wavelet based multiple watermarking approach.Their method addresses confidentiality protection and data authentication problems by using three separate watermarks.

Shieh et al [10] a genetic algorithm (GA) based watermarking scheme is presented.GA is used to locate the optimal frequency bands for watermark embedding. Piva et al [11] a simple and secure self recovery authentication technique is presented which hides an image digest in subbands of Discrete Wavelet Transform. Xuan et al [12] have presented histogram shifting based reversible watermarking techniques .In this work, a part of the histogram of high frequency wavelet co-efficients shifted towards right by one point and then watermark is embedded by using the histogram zero point.

Based on good time frequency features and discrimination that match well with the Human Visual System (HVS) motivates the use of DWT in image watermarking among several techniques [18].In medical applications, it is very important to maintain the quality of images because of their diagnostic value. The performance of watermarking schemes can be improved by several methods. Dual watermarking technique is one of the methods to increase the level of security on the watermarked data.

In this work a new method for protecting the patient information is introduced in which the information is embedded as a watermark in the discrete wavelet transform (DWT) of the medical image using the hospital logo as a reference image. The scheme is blind so that the EHR can be extracted from the medical image without the need of the original image. Therefore, this proposed technique is useful in telemedicine applications.

The paper is organised as follows: Section 2 explains the EHR generation and the proposed algorithm is introduced in section 3. Simulation results for the proposed technique on different types of images are presented in section 4, Performance metrics and analysis is discussed in section 5 and conclusion is given in section 6.

II. ELECTRONIC HEALTH RECORD

In many areas of health care, particularly in emergency care, health professionals rely on the information provided by the patients about their medical history. However, reliability of the information may be difficult that has acquired from patients who are unwell, confused or having communication difficulties. It is thereby suggested that a personal electronic health record device might empower patients to be aware and have more control of their health status.

A number of different versions of patient record systems exist and it referred by a number of varying terms and acronyms, a common one being Electronic Health Record (EHR).

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014




Fig 1. Electronic Health Record (EHR)

As shown in Fig.1, the patient's information can be inserted in the Electronic Health Record (EHR) which includes personal information (name, gender, age,... etc.), clinical information (doctor's name, diagnosis, blood group.. etc.) and some management information (record number, date.. etc.)

III. PROPOSED METHOD

The proposed system consists of: embedding mode and extraction mode.

A. Embedding Phase

Band selection in Discrete Wavelet Transform is used for the embedding the Electronic Health record onto the cover medical image with the hospital logo as the reference image. Fig 3 shows the proposed embedding block. The algorithm for the proposed phase is as follows.

Step1

For a given $N \times N$ host medical image 'I', m -level DWT is applied which produces 4^m sub-bands of wavelet coefficients. Each sub-band is a matrix of coefficients at a specific resolution with size $n \times n$ where $n = N/4^{m/2}$.

Step 2

Compute the energy of each sub-band using the following equation:

$$E = \frac{1}{n \times n} \sum_{i=0}^n \sum_{j=0}^n c^2(i, j) \quad (1)$$

Where E denotes the energy, $n \times n$ is the size of sub-band, and ' C ' is the DWT coefficient. To ensure trade-off between robustness and imperceptibility out of four bands two sub-bands with middle energy are selected for watermark embedding $b_{r,k}$ where b is sub-band number 1 or 2 and $k = 1, \dots, \frac{n}{4}$ is the block number.

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

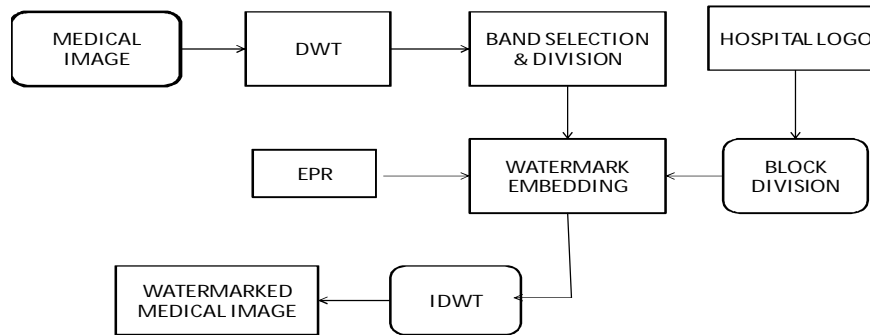


Fig 2: Proposed Embedding phase

Step 3

A grayscale reference image R_k (Hospital logo) whose size is equal to $n \times n$ (64×64 , size of sub-band) is taken , where $k=1, \dots, n/4$.

Step 4

One bit of the watermark (Electronic Health Record) is embedded per pixel. Based on the EHR, the pixels of the reference image R_k is added to the corresponding sub-band block $b_{r,k}$ according to the following rule:

$$b'_{r,k} = \begin{cases} b_{r,k} + \alpha \cdot R_k & \text{if } w = 0 \\ b_{r,k} - \alpha \cdot R_k & \text{if } w = 1 \end{cases} \quad (2)$$

where ' α ' is the weighing factor and ' w ' is the watermark bit.

Step 5

The process in step 4 is repeated up to the length of the watermark bit stream.

Step 6

Apply the inverse Discrete Wavelet Transform to the modified wavelet coefficients to obtain the watermarked image I' .

B. Extraction Phase

The extraction of Electronic Health Record from the watermarked medical image is blind The procedure is described in the following steps:

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

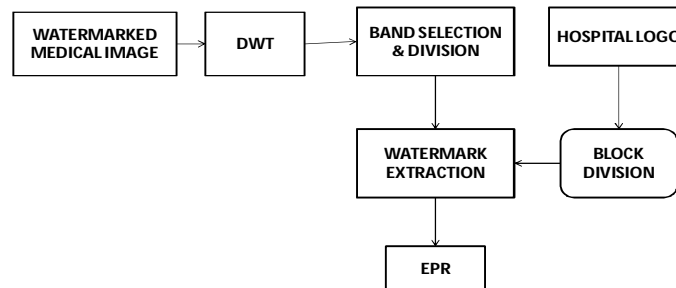


Fig.3 Proposed watermark extraction phase

Step 1

For a given $N \times N$ watermarked (and may be attacked) medical image I , m -level DWT which produces 4^m sub-bands of wavelet coefficients.

Step 2

Choose the same two sub-bands with middle energy used in the watermark embedding $b_{r,k}$.

Step 3

Use the grayscale reference image R_k with size $n \times n$. Where $k = 1, \dots, n/4$.

Step 4

For each block, compute the correlation coefficient value '**corr**' between the reference image block and the corresponding block of watermarked sub-bands as given by

$$corr = R_k * b_{r,k} \quad (3)$$

The recovered watermark bit is selected as follow:

$$w = \begin{cases} \text{If } corr \geq 0 & w = 0 \\ \text{If } corr < 0 & w = 1 \end{cases} \quad (4)$$

Step 5

The watermark is reconstructed with the obtained binary stream.

IV.SIMULATION RESULTS

The performance of the proposed algorithm is tested on 8 grayscale medical images [2] as shown in Fig.4. Four types of medical images CT, MRI, and MRA and radiological of size 256×256 pixels have been considered as sample medical images.

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

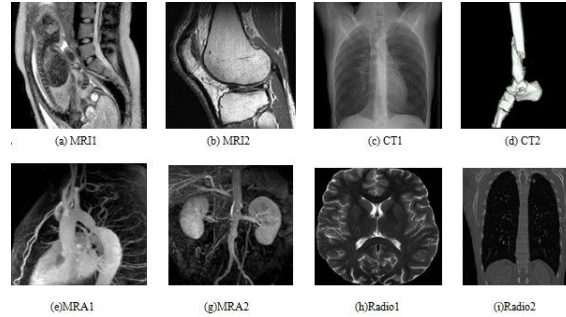


Fig.4. Sample medical images

Among the samples shown in Fig 5, MRI2 image is shown for the illustration of the proposed work. As per the watermarking procedures, the sample medical image is watermarked with the Electronic health record with hospital logo as reference image. The step by step output of the images are as shown in Fig 5-6.

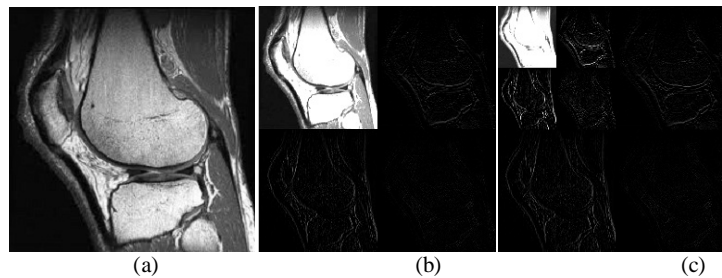


Fig 5. (a) MRI 2 image (Cover medical image) (b) First Level Wavelet Transform (c) Second Level Wavelet Transform

The sub bands with mid energy levels are selected for the watermarking process.

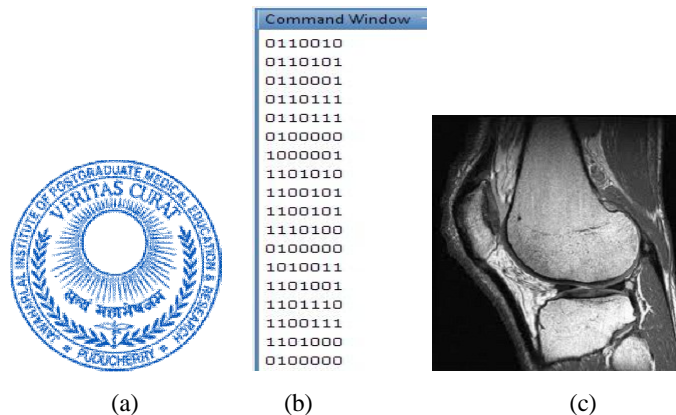


Fig 6. (a) Hospital logo (Reference image) (b) Binary form of EHR data (c) Watermarked Image

V. PERFORMANCE METRICS

The performance evolution of the watermarking approach is analysed against various attacks [19]. The Peak-Signal-To-Noise is defined as:

$$PSNR = \frac{10 \log_{10} (255)^2}{MSE} \quad (5)$$



International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

Where ‘MSE’ is the mean squared error between the original and distorted image and is defined as follows:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (6)$$

Where m, n gives the size of the image and $I(i, j), k(i, j)$ are the pixel values at location (i, j) of the original and distorted image respectively. However, robustness is measured by the normalized correlation coefficient (NC) whose peak value is one and calculated by formula:

$$NC = \frac{\sum_i \sum_j W(i,j) * W'(i,j)}{\sqrt{\sum_i \sum_j W(i,j)^2} \sqrt{\sum_i \sum_j W'(i,j)^2}} \quad (7)$$

Where $W(i, j)$ is the reference image and $W'(i, j)$ is the watermarked image. Results are shown below.

Table 1 shows the PSNR, Mean NC for all tested images in no attack case and with various attacks. The result shows that the watermark is retrieved successfully. The NC is 1.00 for all images.

The four types of medical images are subject to different attacks to measure the robustness of the watermarking algorithm. The MSE, PSNR and NC for the case of attacked images. Analysis of the results shows that our proposed scheme has high degree of robustness to sharpen and automatic equalization attacks.

The similarity between recovered and original information is equal to 1 for the four types of images as shown in Table 1. For Gaussian noise attack, the patient information is recovered with NC=1 when the variance is .001. However, with variance of 0.005 the MRI1 and CT1 images are recovered by NC .9919 and .9963. For median filter attack as indicated, the radiological image type resulted in the best robustness NC=1 while the other three types have NC less than 1.

The results of image attack at different values of the Gamma correction parameter (Par). Satisfactory results are found in the case of contrast attack by factor 10. But, when this factor is increased to 30 the patient information failed to be extracted from the image except for the case of the MRI1 and Radio2 images. The medical image is rotated by 5°. Before extracting the watermark, the image is re-rotated to its original position. The results indicate that the patient information can be extracted with NC=1 except for the MRI1, CT1 and CT2 images where NC=0.9977, 0.9957, and 0.9988 consequently.



International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

Table .1 Images subjected to various attacks

Types of Medical Images	Speckle Noise		Gaussian Noise (0.005)		Median Filter		Salt & Pepper		Sharpening (0.6)		Rotation (50 ^o)		Automatic equalization		JPEG compression (80%)	
	PSNR (dB)	NC	PSNR (dB)	NC	PSNR (dB)	NC	PSNR (dB)	NC	PSNR (dB)	NC	PSNR (dB)	NC	PSNR (dB)	NC	PSNR (dB)	NC
MRI1	32.7487	1	31.9237	.9919	35.8077	1	31.8445	1	26.0128	1	31.8776	.9777	24.0788	1	38.2	1
MRI2	29.9239	1	28.8147	1	36.8173	1	32.5596	1	28.1520	1	26.3739	1	27.5290	1	38.7	1
CT1	55.7479	1	37.4823	.9963	38.9786	.9439	32.5182	.9799	25.7030	1	28.0750	.9951	23.1070	1	38.8	1
CT2	28.3121	1	31.5679	1	40.1122	.9842	38.4112	1	26.9339	1	23.5120	.9988	20.2060	1	37.9	1
MRA1	36.6872	1	30.9541	1	41.5114	.9902	32.9982	1	28.8567	1	35.2934	1	23.1832	1	39.5	1
MRA2	56.0524	1	30.0825	1	41.3610	.9915	32.5291	1	26.5724	1	32.5850	1	22.8456	1	38.0	1
Radio1	37.6368	1	33.8295	1	41.1479	1	32.5307	1	26.1200	1	31.2127	1	29.4570	1	39.3	1
Radio2	46.2817	1	27.8080	1	39.6364	1	33.4630	1	26.4708	1	34.0939	1	30.2097	1	41.0	1

VI.CONCLUSION

In this paper, a new dual watermarking scheme has been introduced for security and privacy of patient information. The robustness of the proposed technique is checked by applying some common attacks on the images and examining the visual quality of medical images by the PSNR and NC (normalized correlation coefficient) parameters. Simulation results shows that the proposed scheme is robust against common attacks such as Speckle noise, Gaussian noise, Median filter, salt &pepper noise, Gamma correction, Rotation, Automatic Equalisation and JPEG compression. From the simulation results, it is observed that the proposed technique is more suitable for radiological images as the robustness of this image to various attacks is better than the other input images.

REFERENCES

- [1] K. Youngberry, "Telemedicine Research", Journal of Telemedicine and Telecare, Vol. 10, No. 2, pp. 121-123, 2004.
- [2] <http://www.osirix-viewer.com/datasets> – DICOM sample image sets.
- [3] S. Tachakra, X. H. Wang, R. S. Istepanian, Y. H. Song, "Mobile e-health: The Unwired Evaluation of Telemedicine", Telemedicine Journal of e-health, Vol. 9, No. 3, pp. 247-257, 2003.
- [4] D. Osborne, D. Rogers, J. Mazumdar, R. Coutts, D. Abbott, "An Overview of Wavelets for Image Processing for Wireless Applications", Proceedings of SPIE: Smart Structures, Devices and Systems, University of Melbourne, Australia, Vol. 4935, pp.427-435, 2002.
- [5] C.-S Woo, "Digital Image Watermarking Methods for Copyright Protection and Authentication", PhD Thesis, Queensland University of Technology, Australia, March2007.
- [6] Wang, R. Z., Lin, C. F., & Lin, J. C. , " Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recognition, 34(3), 671–683, 2001.
- [7] Zkou, X.Q., Huang, H.K. and Lou, S.L., "Authenticity and integrity of digital mammography images". IEEE Transactions on Medical Imaging, 20(8), pp. 784-791, 2001.
- [8] Chao, H.M., Hsu, C.M. and Miaou, S.G., "A data-hiding technique with authentication, integration, and confidentiality for electronic patients records", IEEE Transactions Information Technology in Biomedicine, 6, pp. 46-53, 2002.
- [9] Giakoumaki, D. Rogers, J. Mazumdar, R. Coutts, D. Abbott, "An Overview of Wavelets for Image Processing for Wireless Applications", Proceedings of SPIE: Smart Structures, Devices and Systems, University of Melbourne, Australia, Vol. 4935, pp.427-435, 2003.
- [10] C. Shieh, H. Huang, F. Wang, J. Pan, Genetic watermarking based on transform domain techniques, Pattern Recogn. 37, 555–565,2004.
- [11] Piva, A. Bouridane, M. Ibrahim, S. Boussakta, Digital image watermarking using balanced multiwavelets, IEEE Trans. Signal Process. 54 (4), 1519–1536, 2006.
- [12]Xuan, Lee, Y. K. & Chen, L. H. , " High capacity image steganographic model". In IEEE proceedings of vision, image, and signal processing Vol. 147, pp. 288–294, 2004.
- [13] N. A. Memon, S.A.M. Gilani, "Watermarking of CT Scan Medical Images for Content Authentication", Journal of Computer Mathematics, 2010.
- [14] C. Wu, R. Cathey, "Digital Watermarking: A Comparative Overview of Several Digital WatermarkingSchemes",available at:<http://www.csam.iit.edu/cs549/cs549/project/presentation/report.pdf>.



ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

- [15] F. Sebe, T. Domingo Ferrer, J. Herrera, "Spatial Domain Image Watermarking Robust against Compression, Filtering, Cropping and Scaling", Springer Image computing, vol 2, pp. 44-53, 2000.
- [16] N. Nikolaidis, I. Pitas, "Robust Image Watermarking in Spatial Domain", IEEE SignalProcessing Transaction Vol. 66, No. 3, pp.385-403, 1998.
- [17] Cao, F., Huang, H.K. and Zhou, X.Q., "Medical image security in a HIPAA mandated PACS environment. Computerized Medical Imaging and Graphics", IEEE transaction on Image Processing 27(2-3), pp. 185-196, 2003.
- [18] Zkou, X.Q., Huang, H.K. and Lou, S.L., "Authenticity and integrity of digital mammography images". IEEE Transactions on Medical Imaging, 20(8), pp. 784-791, 2001.