IJCSN International Journal of Computer Science and Network, Volume 5, Issue 5, October 2016
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 1.02

Fragile Watermarking of Medical Image for Content Authentication and Security

[1] Nassiri Boujemaa, [2] El aissaoui Abdelaziz , [3] EL mourabit Yousef , [4] Latif Rachid, [5] Bsiss Mohammed Aziz

[1, 2] International University, Laboratory Innovation and Applied Research Center
Agadir , Morocco

[3,4] Ibn Zohr University, Laboratory of Systems Engineering and Information Technology (LISTI)
Agadir, Morocco

[5] University Cady Ayyad, Faculty of Medicine and Pharmacy, Biophysiqe Laboratory Department of Nuclear Medicine
Marrakech, Morocco

Abstract - Currently in the health environment, medical images are a very crucial and important part of the medical information because of the large amount of information and their disposal two-dimensional. Medical images are stored, transmitted and recovered on the network. The images users await efficient solutions to preserve the quality and protect the integrity of images exchanged. In this context, watermarking medical image has been widely recognized as an appropriate technique to enhance the security, authenticity and content verification. Watermarking image may bring elements of complementary research methods of classical cryptography. The objective of this paper is to develop a method to authenticate medical images to grayscale, detect falsified on these image zones and retrieve the original image using a blind fragile watermarking technique. We propose a method based on the discrete wavelet transform (DWT) for the application of content authentication. In our algorithm, the watermark is embedded into the sub-bands detail coefficient. The sub-bands coefficients are marked by adding a watermark of the same size as three sub-bands and a comparison of embedding a watermark at vertical (LH), horizontal (HL) and diagonal (HH) details. We tested the proposed algorithm after applying some standard types of attacks and more interesting. The results have been analyzed in terms of imperceptibility and fragility. Tests were conducted on the medical images to grayscale and color size 512 × 512.

Keywords - *Watermarking, DWT, Imperceptibility, Authenticity, Fragility, Normalized Hamming Distance, Medical Image.*

1. Introduction

Currently the exchange of medical images between different departments of a hospital and hospitals situated in different geographic regions is a common practice. But unfortunately, this exchange of images through open networks like the Internet is unsecure. These medical images require strict security because the critical judgment is made on the information provided by these images. Therefore, they should not be changed illegitimately; otherwise, undesirable result can cause loss of essential information. The large bases of image data must be processed in the hospitals for both clinical and research purposes. These bases of image data must be protected against malicious attempts. For this purpose, the medical image authentication may be performed through the digital watermarking technique. In the watermarking process, the insertion and extraction steps are more important. A watermark (secret message) is inserted into the original image (insertion phase). The doctor will be able to follow the authentication phase, when the image is retrieved from the database; it will include the extraction watermark. Consequently, if the extraction of the secret message fails, the doctor will know that some manipulations have been performed. However, if the extraction watermark is made successfully, the doctor can proceed securely to the diagnosis.

This work is based on the development of blind fragile watermarking algorithm medical images to grayscale in a wavelet transformed domain. Watermarking is implemented to improve the safety, fidelity, authenticity and content verification images manipulated remotely. The results have been analyzed in terms of imperceptibility and authenticity.

This paper is structured as follows: The first section, deals with literature survey of digital image watermarking,

medical image watermarking and wavelet for image watermarking. The second section explains how a blind, additive and fragile watermarking algorithm is proposed in the transformed wavelet domain. The experimental results and discussion are described in the third section. The conclusion and future works are given in the last section.

2. Watermarking Application on Medical Images

2.1 Digital Watermarking Technique

The powers of computers and public networks have facilitated access and modification of information. Unfortunately, the digital crime has greatly increased piracy. The image watermarking appeared at the beginning of the 1990's, in order to parry piracy of multimedia documents. Watermarking involves inserting into a digital document or object (signal, image, video, audio) a watermark can be of different kinds (a sequence of binary random, a small image, logo, ..) for ensuring service security (protection of copyright, copy protection, authenticity, integrity, etc.) [1-2-3]. The conditions to be fulfilled that mark depends on the problem to be treat and algorithms should take into account the specificities of images such as color, resolution and compression standards [4]. For medical images, it is important that the distortion introduced by mark is imperceptible; that is to say the deformation should be low enough so that the user can not differentiate between the watermarked image and the original image [5].

2.2 Watermarking Application on Medical Images

Regard to medical images, several scenarios using the watermarking has been identified since the year 2000's [6-7-8]:

- Image authentication with the insertion of information certifying the origin and an image the attachment to a specific patient.
- Integrity control by placing in the image control information such as a digital signature.
- Adding data-hiding for enriching the content of images by associating a semantic description of its content.

Another most complete scenario combines authentication and integrity control images and seeks to establish a link between these images and the associated account review report. Watermarking associated information protection and to protect the image into a single entity: marked image.

2.3 Wavelet for Image Watermarking

To obtain better imperceptibility, watermarking is done in frequency domain [9-10]. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) is most popular transforms operating in the frequency domain. Wavelet techniques provide excellent space and frequency energy compaction, in which energy tends to a cluster spatially in each sub-band. The wavelet decomposition is generally used for the fusion of images. As watermarking includes merger a watermark to a host signal, it follows that wavelets are attractive for image watermarking. Wavelet theory appeared in early 1990's [11]. It affects many areas of mathematics, particularly signal processing and image. Wavelet transform divides the information of an image into approximation (low frequencies) and detail (high frequencies) sub-signals [12]. The approximation (LL) sub-signal shows the general trend of pixel values and other three detail sub-signals show the vertical (LH), horizontal (HL) and diagonal (HH) details or changes in the images. The hierarchical structure shown in Fig.1.

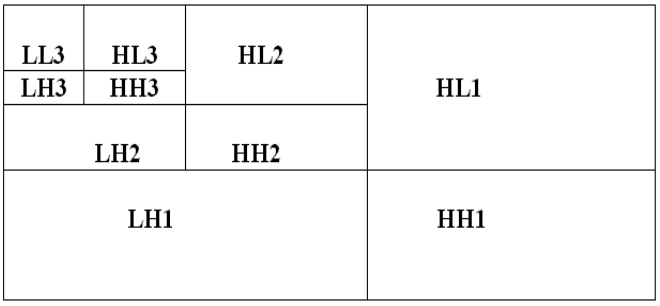

Fig.1 Structure of wavelet decomposition (Tree-level)

3. Method Fragile Watermarking Proposed

Authentication and integrity systems of image can be grouped in several ways depending on the mode of storage of authentication data that is based techniques on electronic signature based or the fragile watermarking or even depending on the nature of the information they burrow into the document to protect. The main difference between these two categories of techniques is that in the digital signature techniques, the authentication data is transmitted in a separate of the raw data stored in the same folder. While in watermarking techniques, the authentication data are embedded in the raw data. In the remainder of this paper, we present a technique developed based on the fragile watermarking.

3.1 Process for Watermarking

We can divide the process of watermarking in four main blocks (Fig.2): Watermark Generation, Watermark Embedding, Watermark Extraction and finally the detection block (Tamper Detection). Among them, the insertion and extraction blocks decide the characteristics of the other blocks, and therefore they are the most important.

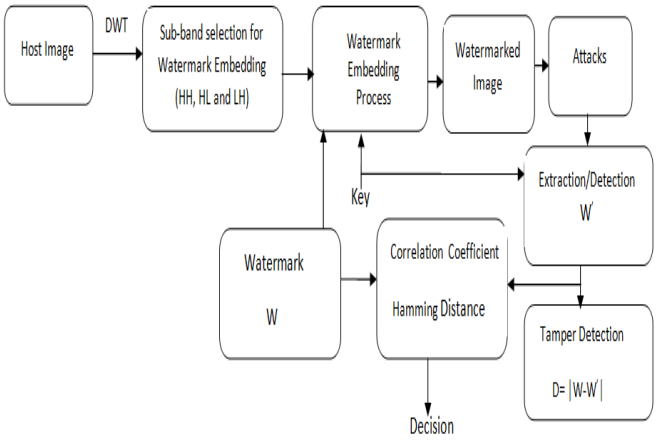

Fig.2 General Model of a proposed authentication system based on a fragile watermarking.

3.2 Proposed Algorithms

The proposed watermarking algorithms are classified according different criteria, namely: the symmetrical key is implemented; information necessary for the extraction is blind; insertion technique is additive and the insertion transformed domain is used (DWT).

3.2.1 Watermark Generation

In order to generate the watermarks, following steps are implemented:
1. Read the watermark.
2. Convert this gray intensity image into a binary image.

We have used the following procedure to perform the above task:
2.1. First resize the image to 25 x 25 pixels.
2.2. Find mean value of gray scale image and call it threshold T.
2.3. Based on this threshold value T, convert the grayscale image into binary by using the following formula:

If logo (m; n) > T, make the pixel white

Else make the pixel black. Now convert this binary image into vector and call it W such that.

3. A pseudo random binary vector P of the size same as W is generated by a secret key K. The following formula is used to get the ultimate watermark $W^* = W \oplus P$.

3.2.2 Embedding Process

The main steps of the embedding procedure developed are presented here:

1. Read the original image.
2. Resize the image.
3. Apply a wavelet decomposition on the image to the original scale L (L=4) to obtain the transformed image. In our decomposition, we have used 4 levels. This number was chosen to allow for good frequency resolution and to yield enough bands for embedding.

4. Add a mask psycho visual; to better ensure the invisibility of the watermark; psycho visual criteria are used to adjust the insertion force locally to the image. This allows us to maximize the mark embedding weights while minimizing the distortion introduced.

5. Specify the value of parameter robustness alpha; this value determines the force of the watermark that will be inserted.

6. Embedded W* in the host image.

7. Apply an inverse wavelet decomposition of the image transformed to the scale L (L = 4) to obtain the watermarked image.

3.2.3. Algorithm to Extract the Watermark

The extraction process has the following steps:

1. Perform wavelet transform on the possibly distorted watermarked image, using the same wavelet function.
2. Extract the watermark by the reverse process of embedding.
3. Decrypt the extracted watermark W* using the same secret key as was used for embedding.
4. Compare the extracted watermark W' with W. If both are same, received image is authentic, otherwise declare it as unauthentic.

3.2.4 Decision

The last step algorithms watermarking process is to decide whether the extracted watermark effectively matches the signature inserted. For this, measurement of Normalized Correlation (NCC) is given in Eq. (1) [13].

$$NCC(W,W^{'}) = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} W(i,j) * W^{'}(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(W(i,j)\right)^2} * \sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(W^{'}(i,j)^2}} \quad (1)$$

4. Image Quality Measurements and Authentication

4.1 Image Quality Measurements

In watermarking techniques the quality measurement brought on the host document at the insertion of the watermark is large. To determine the distortion in the watermarked image by referring to the original image, some of quality metrics may be applied. Here are the measures most widely used [14].

4.1.1 Mean Square Error: MSE

The MSE signify the mean square error between the luminance of an image and the marked image. The MSE evaluates degradation due to watermarking. It is defined by (Eq. (2), [15-16] :

$$MSE(I, I^{'}) = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(I_{ij} - I^{'}_{ij})^2}{m\,n} \quad (2)$$

I and I' are respectively the original image and watermarked image sizes m*n where Iij and I'ij are their components. This error is mainly due to the addition of the watermark.

4.1.1 Peak Signal to Noise Ratio: PSNR

The PSNR determines the imperceptibility of the signature. In other words, it evaluates the original image distortion caused by the watermarking and possibly other attacks. The PSNR after insertion of the watermark is given in decibels as (Eq. (2), [15-16-17].

$$PSNR_{[dB]}(I, I^{'}) = 10\log_{10}\left(\frac{N^2_{\max}}{MSE(I, I^{'})}\right) \quad (3)$$

For example for an image coded on 8 bits, Nmax= 255. Le PSNR measures the fidelity between two images while the MSE measures the difference between two images [18].

In multimedia applications, any image with more than 30 dB is acceptable. In medical images, however, the quality of data is paramount, and a PSNR around 50dB is a definite indication of quality image and that no significant degradation in the image with respect to the original host exists [14].

4.2 Authentication

For the objective analysis Normalized Hamming Distance measure given in (Eq.4) is used for authentication.

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

Where N_w is the length of the watermark, and $\oplus$ is the exclusive-OR (XOR) operator. The value of NHD ranges between (0, 1) and application dependent decision can be made concerning the integrity of the content of medical image. The values closer to zero give better results.

5. Simulation and Experimental Results

In this section, we evaluate the performance of our method in terms of two important requirements of medical image watermarking: imperceptibility and authenticity. The experimental results are separated into two parts: the first is devoted to the tested of the imperceptibility property while the second is devoted to the analysis fragility property after applying some standard types of attacks and most interesting.

5.1 Imperceptibility

To test the property of imperceptibility of our watermarking method, multiple medical images to grayscale of size 512 × 512 are marked with the Image doctor logo of size 25 × 25 (fig.3). To assert the visual quality of our method, we apply the embedding algorithm described above. The watermark is embedded into the

sub-bands detail coefficients that are diagonal (HH), vertical (LH) and horizontal (HL).

Fig.3: Watermark: Image doctor logo

Figure 4 shows host images and their watermarked images.

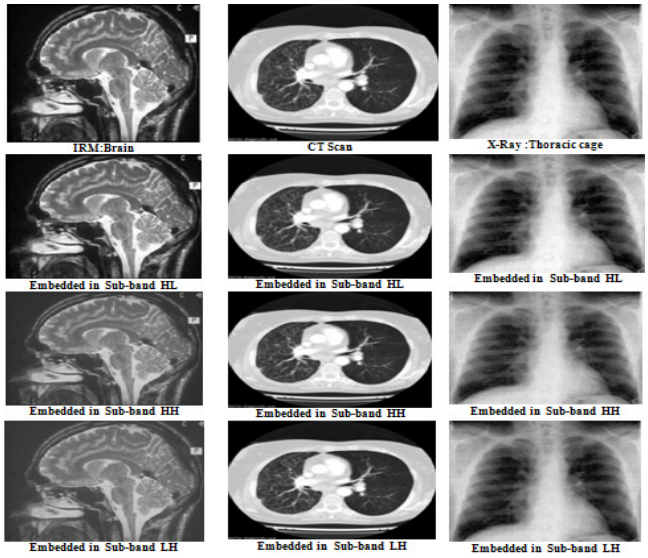

Fig.4 Visual quality of watermarked image based on three sub-band details (coefficients diagonal, vertical and horizontal). Row No. 1: Original images. Row No. 2, No. 3 and No. 4: Watermarked Images

From this figure and for the diagonal coefficients (HL), we can see that it is difficult to differentiate between the original image and watermarked image.

To determine the actual quality of our method, PSNR and MSE are used to estimate the distortion of the watermarked images. The values of PSNR and MSE are presented in Table 1.

The degree of distortion calculated by the PSNR and MSE (Table 2) depends on the type of medical images used that is to say, the acquisition hardware used (anatomical imaging and functional imaging) and also according to the different acquisition technique (X-Ray, CT scan, Magnetic Resonance Imaging (MRI), ultrasound,…etc.).

Table 1: Quality of watermarked images

Image Type	Host image	Format	Sub-band	PSNR (dB)	MSE
Gray scale	Brain (IRM)	. BMP	LH	25.8080	170.7190
			HH	29.1449	79.1757
			HL	75.8034	0.0017
		. PNG	LH	25.8080	170.7190
			HH	29.1449	79.1757
			HL	75.8034	0.0017
	Thoracic cage (X-Ray)	. BMP	LH	32.3873	37.5278
			HH	34.8006	21.5288
			HL	75.8034	0.0017
		. PNG	LH	32.3873	37.5278
			HH	34.8006	21.5288
			HL	75.8034	0.0017
	CT Scan	. BMP	LH	27.6525	111.6438
			HH	29.8470	67.3572
			HL	75.8034	0.0017
		. PNG	LH	27.6525	111.6438
			HH	29.8470	67.3572
			HL	75.8034	0.0017
Color	Breast (TEP)	. BMP	LH	29.9786	65.3462
			HH	31.9715	41.2978
			HL	75.8034	0.0017
		.PNG	LH	29.9786	65.3462
			HH	31.9715	41.2978
			HL	75.8034	0.0017

5.2 Authenticity

The Normalized Hamming Distance is used for objective authentication. Numbers of image manipulations were performed on the watermarked images. The attacks are given as follow:

- Noise addition (Gaussian noise, Multiplicative Uniform and Salt and pepper)
- Filtering (median filtering, Filter Gaussian and Adaptive filtering)
- Rotation
- Compression JPEG

Table 2 illustrates the results after applying these various attacks on the images given in Fig.4, Row No.1.

Table 2: Authentication measurement against the various attacks performed on the images

Attacked performed	Normalized Hamming Distance (NHD)							
	Noise addition			Filtering			Rotation	Compression JPEG
	Salt and Pepper	Multiplicative uniform	Gaussian noise	Median filtering	Filter Gaussian	Adaptive filtering		
Thoracic cage (X-Ray)	0,0608	0,0384	0,0352	0,2336	0,0608	0,0432	0,0192	0.2320
Brain (IRM	0,0704	0,0496	0,352	0,2048	0,2304	0,0352	0,0672	0.0352
CT Scan	0.0432	0.0432	0.0432	0.1920	0.0880	0.0448	0.0432	0.0432
TEP	0.0752	0.0432	0.0432	0.2032	0.1104	0.0448	0.0432	0,0432

It can be observed that almost all the attacks were recognized by the proposed scheme.

6. Conclusion

The proposed scheme is very sensitive. It can detect even one bit of distortion in the image. The image doctor logo used as watermark can easily detect the authenticity of the image. One shortcoming of the proposed technique is that it cannot distinguish between the intentional and un-intentional attacks. During transmission from one hospital to the other, medical images are generally compressed in order to save the bandwidth memory. In this case compression can be considered as un-intentional attack and the authentication system should deem the image authentic. However the proposed scheme declares the image as unauthentic in this scenario as shown in (table2). The future work will deal with the semi-fragile watermarking technique for medical images that can survive against the legitimate attacks like common signal and image processing operation where as declare the image unauthentic if an instance of illegitimate attack occurs.

References

[1] J.L. Dugelay and S. Roche, 1999 , “Introduction au tatouage d’image,” in Ann. Télécommunication, vol. 54, pp. 427–437.

[2] P. Bas, 2000, ‘‘Méthodes de tatouages d’images fondées sur le contenu’’. Thèse de Doctorat, Institut National Polytechnique de Grenoble.

[3] S. Katzenbeisser and F. A. Petitcolas, 2000, ‘‘Information Hiding, Techniques for Steganography and Digital Watermarking’’, Artech House.

[4] Nikolaidis and I. Pitas, 1999, “Digital Image Watermarking : An Overview’’. In ICMCS, volume 1, pages 1_6.

[5] B. Mathon, 2011, ‘‘Développement de méthodes de tatouage sûres pour le traçage de contenus multimédia’’, thèse en cotutelle internationale, université de Grenoble et catholique de Louvain.

[6] G .Coatrieux, , H. Maitre, B .Sankur, Y .Rolland, and Collorec, R., 2000 “Relevance of watermarking in medical imaging’’. Proceedings of International Conference on Information , Technology Applications in Biomedicine, IEEE-EMBS, pp. 250–255.

[7] I. J .Cox, M. L .Miller and J. A. Bloom, 2002 ,‘‘ Digital watermarking’’.San Francisco, CA: Morgan Kauffman.

[8] G. Coatrieux, L. Lecornu, and B .Sankur, 2006, ‘‘A review of image watermarking applications in healthcare’’, Proceedings of the 28th IEEE.

[9] H. Yuan, X.-P. Zhang, 2004, "A Multiscale Fragile Watermark Based on the Guassian Mix-ture Model in Wavelet Domain", Proceedings of IEEE ICASSP Confernce, Vol. 3, pp.17-21, May.

[10] N.F. Johnson, Z. Duric, S. Jajodia, 2000, "Information Hiding: Stegnography and Watermarking Attacks and Counterattacks", Kluwer Academic Publishers, Dordrechet.

[11] S.Mallat, 1989, “Multiresolution Approximation and Wavelet Orthonormal Bases of L2 (R)”, Trans. Amer. Math. Soc, pp. 69-87.

[12] Z. Dezhong, C. Fayi, 2008, “Face Recognition based on Wavelet Transform and Image Comparison”,International Symposium on Computational Intelligence and Design.

[13] S.Chikhi, 2008 ,‘‘Contribution to the supple authentication by digital techniques watermarkings digital image: application to medical image", PhD thesis, Univesity of Constantine Algeria .

[14] N. V. Rao & V. Meena Kumari, 2011, “Watermarking in Medical Imaging for Security and Authentication’’,

Information Security Journal: A Global Perspective, 20:3, 148-155.

[15] C.Shien Lu, 2005, "Multimedia security : steganography and digital watermarking techniques for protection of intellectual property" ,Institue of Information Science Academie Sinica,Taiwan.

[16] C.R. Rodriguez, F. Uribe Claudia, T. Blas Gershom, 2007, "Data Hiding Scheme for Medical Images", Proceedings of IEEE 17thInternational Conference on Electronics, Communications and Computers (CONIELECOMP).

[17] F. Autrusseau, 2002, ''Watermarking based on modeling the human visual system and the transformation Mojette'', Doctoral thesis, University of Nantes.

[18] H.Y. Leung, L.M. Cheng, and L.L. Cheng, 2009, "Digital Watermarking Schemes Using Multi-resolution Curvelet and HVS Model" Proceedings of Springer , 8th International Workshop, IWDW, Guildford, UK, , August 24-26.

Boujemaa Nassiri was born in El Jadida, Morocco on January 1, 1974. He received the Master's degree in electronic systems from Ibn Zohr University, Agadir, Morocco, in 2009. He received the PhD degree in data processing in 2015, Currently, he is a teacher researcher in the international university of Agadir. His research interests include Real time Acquisition and protected transmission of medical data.

Abdelaziz El Aissaoui was born in Agadir in Morocco on June 3, 1967. He holds a Master in Business Intelligence from the University of Lorraine in France in 2010. Currently he is a preparatory course coordinator in the international university of Agadir . His research interests relate to the processing of medical image.

Yousef EL Mourabit was born in Agadir, Morocco in 1986.
He is graduate as a computer engineer in 2011 from National school of applied sciences (ENSA) of Agadir in IBN ZOHR University. He joined the Laboratory of Systems Engineering ans Information Technology (LISTI) in the ENSA of Agadir in IBN ZOHR University as a PhD Student in 2012. His current research interests include information technology, security of sensor networks and biomedical image.

Rachid Latif was born in Agadir, Morocco, on December 8, 1968. He received the PhD degree in signal processing in 2000 and the Habilitation degree in 2005, from Ibn Zohr University, Morocco. Currently, he is a Professor with the Department of Industrial Engineering, Ibn Zohr University, Agadir, Morocco. His research interests include biomedical signal processing, fuzzy logic, time-frequency signal processing and he is working on the modeling, filtering, and analysis of fetal cardiac signals. Prof. Latif is the head of the Laboratory of Systems Engineering ans Information Technology (LISTI) in the ENSA of Agadir in IBN ZOHR University and is a member of the Marocain Acoustical Society (SMA).

Bsiss Mohammed Aziz Doctor in Medicine,Assistant Professor of Biophysics and Nuclear Medicine University Cady Ayyad Marrakech CHU Mohammed VI Marrakech, Faculty of Medicine and Pharmacy Marrakech, Biophysiqe Laboratory Department of Nuclear Medicine.
.