The Medical Image Watermarking Algorithm Based on DWT-DFT and Logistic Map

Jingbing Li*
College of Information Science and Technology
Hainan University
Haikou, China
Jingbingli2008@hotmail.com

Yaoli Liu
College of Information Science and Technology
Hainan University
Haikou, China
Ylmy0910@163.com

***Abstract*—Medical image data require strict security, confidentiality and integrity when transmitted and stored in hospitals. However, the transmission of wireless and wired networks has made the medical information vulnerable to attacks like tampering, hacking etc. And the Region of Interest(ROI) of medical image is unable to tolerate significant changes. In order to solve these problems, we have proposed an algorithm which introducing the digital watermarking technology to increase the security of medical images. The scheme obtains the visual feature vectors of the medical image using DWT-DFT. At the same time, the watermarking image is encrypted by Logistic Map to enhance its security. The experiment results showed that the scheme has strong robustness against common attacks.**

Keywords-DWT-DFT; medical image; watermarking; logistic map

I. INTRODUCTION

As digital technology pervades our society, a vast amount of medical images now exist in electronic format for easy storage and transmission. However, medical image and the corresponding patient's information were stored separately now. It is easy to cause information disorder, and increase the storage space. At the same time, when the medical images are transmitted on the Internet [1], the patient's personal information can be easily compromised, tampered [2], and the other problem of information security. It is an urgent need of security measures in medical information system to serve these problems. Digital watermarking has been introduced as an effective complementary measure to traditional encryption in an attempt to solve above problems. We regard patient's information as a digital watermarking hidden in medical images using this kind of technology. Even though the medical images have been attacked, we can still completely extract the watermarking which can protect patient's personal information.

Currently the field of digital watermarking for medical research focused on the spatial domain and transform domain (DCT, DFT and DWT) [3], which can be implemented by changing some pixel gray-scale values in the space domain or by changing the values of coefficients in the transform domain to embed watermark.

Although current traditional watermarking techniques were primarily developed for applications such as multimedia copy right protection [4], they may not be quite suitable for the medical image's information security. Medical image is an important basis for doctors to acquire the physical illness information of patients. Traditionally, it has very strict requirements to medical data, and do not allow any data changes.

This paper presents a watermarking algorithm which acquires the visual feature vectors of the medical image using DWT-DFT, and by combining it with the chaotic encryption technology, it can enhance the security of the watermarking. The experiment results showed that the algorithm has good robustness against common attacks.

II. THE FUNDAMENTAL THEORY

A. The Discrete Wavelet Transform (DWT)

The Wavelet Transform, first proposed by Daubechies and Mallat in 1988, is a new signal analysis theory and is a "time-frequency" method [5]. The basic idea of DWT is to analysis the signal $f(t)$ based on wavelet function, $\psi_{a,b}(t)$.

$$Wf_{a,b} = \int_R f(t)\overline{\psi}_{a,b}(t)\,dt \tag{1}$$

Where, wavelet function $\psi_{a,b}(t)$ is a group of functions obtained from the same base function ψ by translating and stretching.

$$\psi_{a,b}(t) = |a|^{-\frac{1}{2}}\psi\left((t-b)/a\right) \quad a,b \in R, a \neq 0 \tag{2}$$

Where, ψ is the dilated function, a and b are the dilation factor and the translation factor, respectively.

The decomposing equation of the Mallat algorithm is as follows:

$$c_{j+1,k} = \sum_{n\in Z} c_{j,n}\overline{h}_{n-2k} \qquad k \in R \tag{3}$$

$$d_{j+1,k} = \sum_{n\in Z} c_{j,n}\overline{g}_{n-2k} \qquad k \in Z \tag{4}$$

The reconstruction equation of the Mallat algorithm is given by:

$$c_{j,k} = \sum_{n\in Z} c_{j+1,n}h_{k-2n} + \sum_{n\in Z} d_{j+1,n}g_{k-2n}, \quad k \in Z \tag{5}$$

By the one-layer wavelet decomposition of the original image, four subband images can be acquired. Where, LL1 is the approximated subband image with low frequency characteristics that are robust to attacks. The others (LH1, HL1, and HH1) with high frequency characteristics are

easily affected by attacks. Therefore, embedding the watermarking into the low frequency subgraph can provide better robustness.

Since both the JPEG2000 and the MPEG-4 use DWT, a watermarking algorithm that uses DWT is compatible with them.

B. The Discrete Fourier Transform (DFT)

The discrete fourier transform is a signal analysis theory. The $M \times N$ medical image's DFT is defined by:

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cdot e^{-j2\pi xu/M} e^{-j2\pi yv/N} \tag{6}$$

$$x = 0,1,...,M-1 \; ; \; y = 0,1,...,N-1$$

Where $f(x,y)$ is the value of the medical image at the point (x,y) and $F(u,v)$ corresponds to the DFT coefficient at point (u,v) in frequency domain.

C. Logistic Map

A chaotic system has a noise like behavior while is exactly deterministic so we can reproduce it if we have its parameters and initial values. These signals are extremely sensitive to the initial conditions [8]. One of the most famous chaotic systems is Logistic Map, which is nonlinear return map given by:

$$x_{k+1} = \mu x_k \left(1 - x_k\right) \tag{7}$$

Where, $0 \le \mu \le 4$ is the growth parameter, $x_k \in (0,1)$ is the system variable, and k is the number of iterations. The study of the chaotic dynamical systems shows that Logistic Map works in chaotic state when $3.569945 \le \mu \le 4$. In this paper, we set $\mu = 4$. The Chaotic sequences are generated by different initial values, x_0.

We can generate a chaotic image by using chaotic sequences. This encrypted image has the same size with the watermarking image. Applying the Hash function of Cryptography, the encrypted image is very easy to obtain. Fig. 1 shows the result that a binary watermarking image is scrambled by using chaotic sequences.

Fig. 1. The scrambled watermarking image by using chaotic sequences

In the same way, it is easy to restore the original watermarking image according to the same initial value based on Logistic Map.

III. The Algorithm

We choose a significant binary image as the original watermarking image. It is described as: W= {*w(i,j)* | *w(i,j)*=0 or 1; 1⩽*i*⩽*M1*, 1⩽*j*⩽*M2*}. At the same time, we select the tenth slice of one medical volume data as the original medical image. It is described as: F= {*f(i,j)*, 1⩽*i*⩽*N1*, 1⩽*j* ⩽*N2*}. To facilitate the operation, we assume *M1=M2=M*, *N1=N2= N*.

A. The feature vector designing of medical image

Firstly, DWT is applied to the original medical image to obtain the approximated subband LL1. Then, DFT of the whole LL1 is computed and the DFT coefficient matrix is acquired. We choose 5 low-frequency DWT-DFT coefficients (F(1,1),F(1,2),…F(1,5)) to compose the feature vector, shown in Table Ⅰ. Here, two signs are generated from one complex coefficient. Let "1" represents a positive or zero coefficient, and "0" represents a negative coefficient, and then we can obtain the sign sequence of low-frequency coefficients, as shown in the column "Sequence of coefficient signs" in Table I. After attacks, the sign sequence is unchanged, and the Normalized Cross-correlation (NC) is equal to 1.0.

Therefore, the sequence of DWT-DFT coefficient signs can be used as the feature vector of medical image.

TABLE I. Change of DWT-DFT low-frequency coefficients with respect to different attacks.

Image Processing	F(1,1)	F(1,2)	F(1,3)	F(1,4)	F(1,5)	Sequence of coefficient signs	NC
Original image	2.03	-1.19-0.10i	-0.01-0.00i	0.17+0.04i	0.04+0.03i	1100001111	1.0
Gaussian noise (3%)	2.93	-0.87-0.05i	-0.02-0.02i	0.11+0.01i	0.03+0.05i	1100001111	1.0
JPEG (8%)	2.19	-1.14-0.09i	-0.01-0.01i	0.17+0.04i	0.04+0.03i	1100001111	1.0
Median filter ([3x3])	2.04	-1.20-0.10i	-0.00-0.00i	0.18+0.04i	0.05+0.03i	1100001111	1.0
Rotation (20°)	2.03	-1.10-0.23i	-0.06-0.06i	0.11+0.06i	0.05+0.07i	1100001111	1.0
Scaling (×0.5)	5.08	-2.95-0.39i	-0.03-0.01i	0.40+0.15i	0.09+0.10i	1100001111	1.0
Translation (5%, down)	1.99	-1.16-0.09i	-0.04-0.01i	0.19+0.04i	0.04+0.03i	1100001111	1.0

Cropping (10%, from y axis)	1.91	-1.09-0.09i	-0.06-0.01i	0.17+0.04i	0.05+0.03i	1100001111	1.0

B. Watermarking encryption algorithm

The steps of generating an encrypted watermarking are as follows:

Step1: Generate the chaotic sequences.

The chaotic sequence *X(j)* is generated by the initial value, x_0 . But it is one-dimension sequence. In order to match the two-dimension watermarking image, we need to get a two-dimensional matrix through liter-dimension operation. Finally, the binary encrypted matrix *C(i,j)* can be achieved by symbolic computation of the chaotic sequence *X(j)*. Where, the value of *X(j)* is more than 0.5, we noted as "1"; or we noted as "0.

Step2: Achieve the encryption watermarking image.

We can generate the encryption watermarking image as follows:

$$BW(i,j) = W(i,j) \oplus C(i,j) \tag{8}$$

Where, *BW(i,j)* denotes the encryption watermarking image, *W(i,j)* denotes the binary watermarking image, *C(i,j)* denotes the binary encrypted matrix.

The initial value, x_0 , is regard as the private key. Even if the algorithm is public, the original watermarking image cannot be recovered without the private key.

C. The embedding and extracting algorithms of watermarking

1) Embedding watermarking

Step3: Acquire a robust feature vector of the original medical image using DWT-DFT.

Firstly, DWT is used to decompose the original medical image, *F(i,j)*, to get approximated subgraph coefficient matrix *FA(i,j)*. Then, DFT of the whole approximated subband, we can get the DWT-DFT coefficients matrix, *FF(i,j)*. Then, after arranging the DWT-DFT coefficients from low to high frequency, the low-frequency sequence *Y(j)* can be acquired. Finally, the feature vector *V(j)* can be obtained as a sign sequence of the top L values in the low-frequency sequence by symbolic computation. In this paper, we set L=32bits.

The process can be described as follows:

$$FA(i,j) = DWT2(F(i,j))$$
$$FF(i,j) = DFT2(FA(i,j))$$
$$Y(j) = Zig-Zag(FF(i,j))$$
$$V(j) = Sign(Y(j))$$

Step4: Acquire the key sequence.

By utilizing the encrypted watermarking *BW(i,j)*and the feature vector *V(j)*, we can generate the public key sequence as follows:

$$Key(i,j) = BW(i,j) \oplus V(j) \tag{9}$$

The public key sequence, *Key(i,j)* ,can be computed by the HASH function of cryptography. It should be stored for extracting the embedded watermarking later. Furthermore, *Key(i,j)* can also be regarded as a key and registered to the third part to preserve the ownership of the original image.

2) Extract the watermarking from the tested image

Step5: Acquire the feature vector of the tested image.

This process of acquiring the feature vector of the tested image is same to step3 of the watermarking embedding process.

$$FA'(i,j) = DWT2(F'(i,j))$$
$$FF'(i,j) = DFT2(FA'(i,j))$$
$$Y'(j) = Zig-Zag(FF'(i,j))$$
$$V'(j) = Sign(Y'(j))$$

Where *F'(i,j)* denotes the tested image, *FF'(i,j)* denotes the DWT-DFT coefficient matrix. *V'(j)* denotes the feature vector of the tested image.

Step6: Extract watermarking

The watermarking image, *BW'(i,j)*, can be extracted as follows:

$$BW'(i,j) = Key(i,j) \oplus V'(j) \tag{10}$$

D. Watermarking decryption algorithm

This process of acquiring the binary encrypted matrix *C(i,j)* is same to step1 of the watermarking encryption algorithm. By the Hash function, we can restore the original watermarking image, *W'(i,j)*, through *C(i,j)* and *BW'(i,j)*.

E. Watermarking evaluating algorithm

The Normalized Cross-correlation (NC) is used for measuring the quantitative similarity between the extracted and embedded watermarking, which is defined as:

$$NC = \frac{\sum_i \sum_j W(i,j) W'(i,j)}{\sum_i \sum_j W^2(i,j)} \tag{11}$$

Where *W* denotes the embedded original watermarking and *W'* denotes the extracted original watermarking.

The higher the NC value, the more similarity there is between the embedded and extracted original watermarking.

The Peak Signal to Noise Ratio (PSNR) is used for measuring the distortion of the watermarked image, which is defined as:

$$PSNR = 10\lg\left[\frac{MN \max_{i,j}\left(\mathrm{I}(i,j)\right)^2}{\sum_i \sum_j \left(\mathrm{I}(i,j) - \mathrm{I}'(i,j)\right)^2}\right] \tag{12}$$

Where *I(i,j)*, *I'(i,j)* denote the pixel gray values of the coordinates *(i,j)* in the original image and the watermarked image, respectively; *M*, *N* represent the image row and column numbers of pixels, respectively.

IV. EXPERIMENTS

To verify the effectiveness of our proposed algorithm, we carried out the simulation in Matlab2010a platform. We choose a significant binary image as the original watermarking image and select the tenth slice of one medical volume data as the original medical image. Fig. 2(b) shows

the original binary image W={ $w(i,j)$=0 or 1; 1⩽i⩽32, 1⩽j⩽32}. Fig. 2(a) shows the original medical image F={ $f(i,j)$; 1⩽i⩽128, 1⩽j⩽128}.

In the experiment, the parameter values: The initial value is 0.2, another parameter of Logistic map is 4, and the number of chaotic system is 32, i.e. x_0=0.2, u=4, k=32.

It is can be seen visually from Fig. 2 that the quality of the medical image embedded has hardly any change. The quality of extracted watermarking is of high-quality with no difference with the original in normal case (no attacking on watermarking).

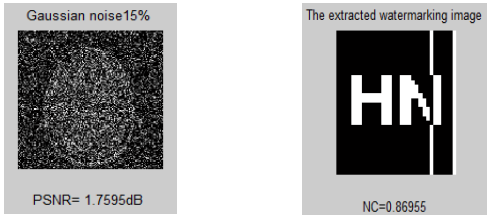
(a) (b)

Fig. 2. The watermarked medical image without attacks: (a) the original medical image; (b) the binary watermarking image.

The following are several types of common attacks to test the robustness of the algorithm.

1) Adding Gaussian noise

Fig. 3(a) shows the watermarked image with Gaussian noise (15%), PSNR is 1.76dB. The watermarking image can be extracted with NC=0.87, as shown in Fig. 3(b). The result shows that our proposed algorithm has strong robustness against noise attacks.

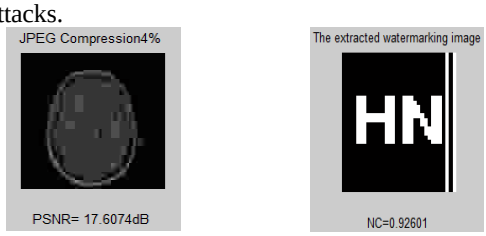


(a) (b)

Fig. 3. Under noise attacks (3%): (a) an image under noise attack; (b) the exacted watermarking image.

2) JPEG attacks

Fig. 4(a) shows the watermarked image with JPEG attacks (4%), PSNR is 17.61dB. The watermarking image can be extracted with NC=0.93, as shown in Fig. 4(b). The result shows that the watermarking algorithm is robust to JPEG attacks.

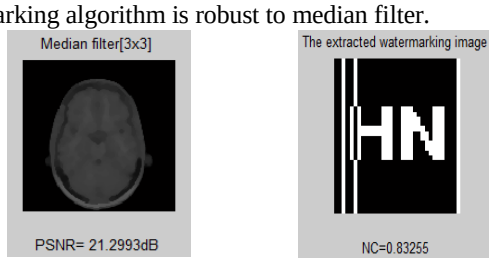


(a) (b)

Fig. 4. JPEG compression (4%): (a) The watermarked image after JPEG compression; (b) The extracted watermarking image.

3) Filter Processing

The medical image under median filter attack [3×3], whose repeat time is 20, is shown in Fig. 5(a). PSNR is 21.30dB. As shown in Fig. 5(b), the watermarking image can be extracted with NC=0.83. The result shows that the watermarking algorithm is robust to median filter.



(a) (b)

Fig. 5. Median filter [3×3, repeat times=20]: (a) Image after median filter; (b) The extracted watermarking image.

V. CONCLUSION

This paper proposed a watermarking algorithm based on DWT-DFT. It combines feature vector, Hash function, Logistic Map and the third part authentication. The watermarking can be extracted without the original medical image. Experiment results proved that the algorithm is robust to common attacks. Moreover, we use Logistic Map to encrypt the watermarking image. Therefore, it is very practical to be used in health care system.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (No:61263033) and the NSF of Hainan Province of China(60894).

REFERENCES

[1] S. Kaur, O. Farooq, R. Singhal, B. S. Ahuja, “Digital watermarking of ECG data for secure wireless communication,” In Proceedings of the 2010 IEEE International Conference on Recent Trends in Information, Telecommunication and Computing, March 2010, pp. 140-144.

[2] K. A Navas and M. Sasikumar, “Survey of Medical Image Watermarking Algorithms,” In Proceedings of the 4th Sciences of Electronic, Technologies of Information and Telecommunications International Conference, Tunisia, March 2007, pp. 25-29.

[3] Y. X. Zhou, W. Jin, “A novel image zero-watermarking scheme based on DWT-SVD,” In Proceedings of the 2010 IEEE International Conference on Multimedia Technology, Dec. 2009, pp. 2873-2876.

[4] M. Unoki, R. Miyauchi, “Reversible Watermarking for Digital Audio Based on Cochlear Delay Characteristics,” In Proceedings of the 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Oct. 2011, pp. 314-317.

[5] Koch E, Zhao J. Towards robust and hidden image copyright labeling. Proceeding of 1995 IEEE Workshop on Nonlinear signal and image processing. Neos Marmaras, Halkidiki, Greece, 1995.