International Journal of Grid Distribution Computing
Vol.8, No.1 (2015), pp.201-212
http://dx.doi.org/10.14257/ijgdc.2015.8.1.19

Zero-watermarking Algorithm for Medical Volume Data Based on Legendre Chaotic Neural Network and Perceptual Hashing

Baoru Han, Lisha Cai* and Wenfeng Li

Department of Electrical Engineering, Hainan Software Profession Institute
Qionghai, 571400, Hainan, China
6183191@163.com

Abstract

Medical information digitization makes the medical information storage and extraction more convenient. Medical image information security and copyright protection is also gradually being taken seriously, and some medical image watermarking has been applied. According to the characteristics of three-dimensional medical images, this paper proposes a robust zero-watermarking algorithm for medical volume data based on legendre chaotic neural network and perceptual hashing. The algorithm is based on three-dimensional discrete wavelet transform frequency analysis features, which uses perceptual hashing technique to extract medical volume data itself feature vector in order to structure robust zero watermarking. And using legendre chaotic neural network to generate chaotic sequence to enhance the security of the watermarking. The algorithm achieves a combination of legendre chaotic neural network encryption and zero-watermarking technology, which can improve the medical volume data watermarking algorithm security and robustness. The simulation results show the effectiveness of the algorithm.

Keywords: *Zero-watermarking algorithm, Three-dimensional discrete wavelet transform, Three-dimensional discrete cosine transform, Legendre chaotic neural network, Perceptual hashing.*

1. Introduction

In recent years, with the rapid development of computer science and technology and multimedia communication technologies, especially the Internet is widely used all around the world, which all promotes the digitization process of the health care system. A large number of medical information in text, images, audio, video, software and other forms is stored on a computer and transmitted over the Internet. Medical information digitalization makes the storage and retrieval of medical information more convenient, but also greatly promotes the rapid development of telemedicine. But malicious attacks, tampering, illegal possession and other serious security problems attendant [1]. Therefore, to enhance healthcare information system security seems increasingly important.

As an important basis for medical diagnosis, medical image on the image quality is very strict. How to use digital watermarking technology to solve medical image due to tampering, theft and other issues, has become an important question for the future development of the medical system need to be addressed urgently. In the field of medicine, patients with the pathology of medical data is extremely strict quality requirements, are often not allowed to make any changes. Medical image digital watermarking technology can effectively solve this problem [2].

Digital watermarking technology as an information hiding technique is an important branch of research in the field, and also is an effective way to protect the integrity of multimedia information [3]. It is an effective complement to traditional encryption techniques. The patient's personal information as a digital watermark is embedded

ISSN: 2005-4262 IJGDC

medical volume data. This embedding is invisible to the naked eye form. Experienced in medical volume data exchange of information in the data processing, the watermarking was extracted completely and accurately, so as to achieve the purpose of protection of patient information [4, 5]. Watermarking information can be text, images, personal medical history, *etc*. Watermarking is generally not visible or perceived. With the original medical image closely together , it is still be able to be extracted in the case of external attack suffered in a certain algorithm to determine the ownership of medical images and owner. Kutter proposed second generation watermarking concept in the literature [6], which use the image features for watermarking embedding and extraction.

[7] proposed a robust digital watermarking algorithm against geometric attacks, and the use of low-frequency domain wavelet image has better stability. [8] conducted research on robust digital image watermarking, taked still images as research object, the image processing technology is currently the most popular into watermark technology, creatively put forward the solution of digital watermarking based on fractal transform scheme, and finally in the zero-watermarking technology is explored, breaks through the traditional routine solutions to embed the watermarking in the original image, proposed a zero watermarking technology. [9] proposed a robust zero-watermarking against attacks, the chaos and image moment technique are applied to the robust zero-watermarking in order to solve the key technical problems.

For the three-dimensional volume data, [10] proposed a volume data digital watermarking algorithm based on the three-dimensional DCT embedded. The algorithm embedded watermark is invisible, able to resist shear, common assault noise, filtering, rotation, *etc*. resistant to certain noise, filtering attacks, but poor resistance to rotation attack. Based on the existing digital watermarking algorithms [11,12], this paper proposes a robust zero-watermarking algorithm for medical volume data based on legendre chaotic neural network, image feature extraction and perceptual hashing. It can improve robust the zero-watermarking algorithm for medical volume data security and robustness, which can resist both conventional attacks and geometric attacks, but also can be embedded in a large capacity watermark. And it uses legendre chaotic neural network scrambling, which has good security and confidentiality.

2. Legendre Chaotic Neural Network

Chaotic system is a complex nonlinear dynamic system. Chaotic sequence is highly sensitive to initial values, unpredictability, and has ergodic. By changing the parameters of the chaotic system and the initial value may be a huge number of sequences and the sequence length is arbitrary [13]. Chaotic sequence does not cycle, similar to a random process. So it has good security. Chaotic sequence is very easy, just giving a formula for chaos and an initial iteration; we can generate a chaotic sequence.

The watermarking image is scrambled by chaotic neural network, which can convert chaos function dominance relation into the chaotic neural network hidden relationship, and enhance the security.

This paper uses a new legendre chaotic neural network. The legendre chaotic neural network model is shown in figure 1. The legendre chaotic neural network selects legendre polynomials as the activation function of hidden layer. Performance close to the theoretical values of the chaotic sequence is generated by the legendre chaotic neural network weights and the chaos initial value. The chaotic sequence is used for scrambling.

A polynomial defined by the following formula is called the legendre polynomial.

Definition 1

$$P_0(x)=1, P_n(x)=\frac{1}{2^n n!}\frac{d^n}{dx^n}(x^2-1)^n \quad n=1,2,3,\cdots \tag{1}$$

$P_n(x)$ is known as legendre polynomials. It is known as the weight function $\rho(x)=1$ n

orthogonal polynomials in space $[-1,1]$.

Set the input layer to the hidden layer weight is w_j , hidden layer to the output layer weight is c_j .The activation function of hidden layer neuron is legendre orthogonal polynomials. The hidden layer neuron input is

$$net_j = w_j x, j = 0,1,2,\cdots,n \tag{2}$$

Hidden layer neurons output are as a set of legendre orthogonal polynomial terms $P_j\left(net_j\right), j = 0,1,2,\cdots n-1$ which can be obtained by formula (1) recursive. legendre chaotic neural network output is

$$y = \sum_{j=0}^{n} c_j P_j\left(net_j\right) \tag{3}$$

Set the training sample is $\left(T_t, d_t\right), t = 1,2,\cdots,l$. Where l is the number of samples $T_t = \left(x_{1t}, x_{2t},\cdots,x_{mt}\right)$ is legendre chaotic neural network input. d_t is legendre chaotic neural network desired output. The network is trained using BP learning algorithm.

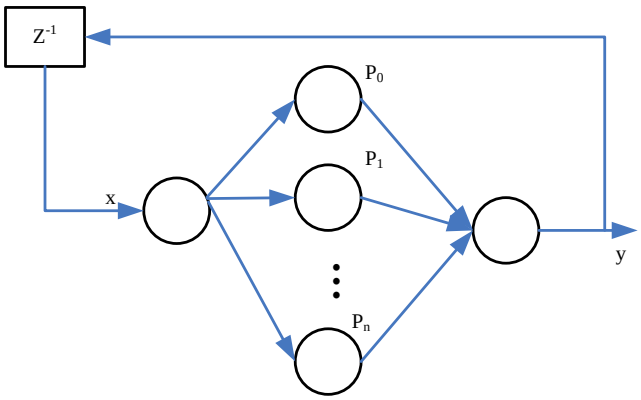


Figure 1. Legendre Chaotic Neural Network

Error formula is as follows.

$$e_t = d_t - y_t \tag{4}$$

$$E = \frac{1}{2}\sum_{t=1}^{l} e_t^{\,2} \tag{5}$$

Network weights adjustment formula is as follows.

$$\Delta c_j = -\eta \frac{\partial E}{\partial c_j} = \eta e_t P_j(net_j) \tag{6}$$

$$\Delta w_j = -\eta \frac{\partial E}{\partial w_j} = \eta e_t c_j P_j'(net_j) x_j \tag{7}$$

$$\begin{cases} w_j(k+1) = w_j(k) + \Delta w_j(k) \\ c_j(k+1) = c_j(k) + \Delta c_j(k) \end{cases} \tag{8}$$

Where k is the training epochs, $t = 1,2,\cdots,l$, $j = 1,2,\cdots n$.

The chaotic function takes the Logistic chaotic function.

$$x(n+1) = \mu x(n)(1 - x(n)) \tag{9}$$

Set the input layer to the hidden layer weight w_j all are 1.The logistic chaotic function generate chaotic sample, it use chaotic sequence samples to train legendre chaotic neural network to obtain the weights.

3. Three-dimensional Discrete Wavelet Transforms

A one-dimensional wavelet transform provides a signal in time and frequency characteristics of multi-resolution analysis, the signal is decomposed into different levels of low frequency components and high frequency components. Two dimensional wavelet transform is the extension of one dimensional wavelet transform, which provides the good multi-resolution analysis feature on space for images and other two-dimensional signal . By analogy, three-dimensional wavelet transform is an extension of the two-dimensional wavelet transform, which provides the good multi-resolution analysis feature on space for three-dimensional images.

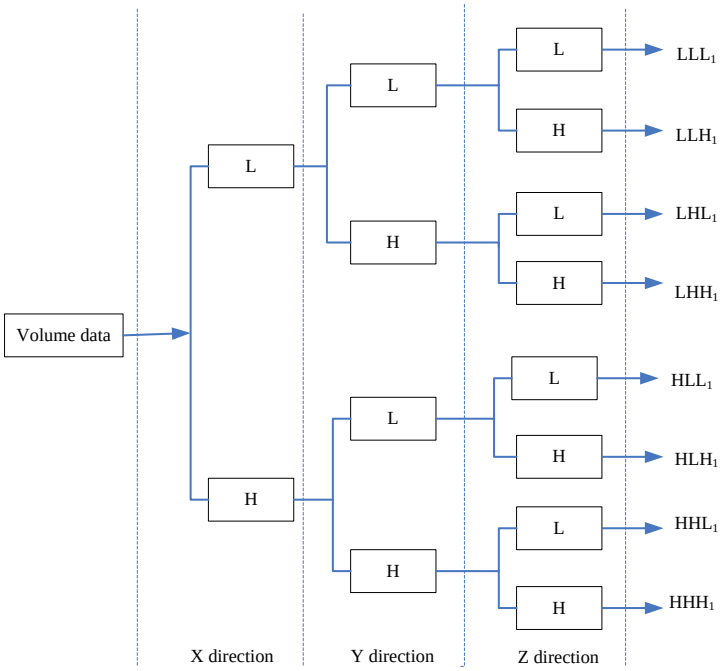


Figure 2. A Layer Decomposition Process for Three-dimensional Wavelet

A layer decomposition process for three-dimensional wavelet is shown in figure 2. L and H respectively denote the low-frequency and high-frequency components of volume data, which are obtained by the filter of low-frequency and high-frequency. Similar to the transformation of two-dimensional image wavelet, three-dimensional volume data is transformed by discrete wavelet transform, which is decomposed into a representative volume data characteristics of low-frequency approximation coefficients LLL1 and seven volume data of high-frequency approximation coefficients. The subscript "1" represents the first layer decomposition of three-dimensional discrete wavelet transform. After the transformation of three-dimensional discrete wavelet, three-dimensional volume data generates wavelet volume data. However, the amount of data remains unchanged. And the generated energy of the wavelet volume data is mainly concentrated in the low frequency part LLL1. In order to improve the robustness of watermark, the watermark is often embedded into the low-frequency part.

4. Three-dimensional Discrete Cosine Transform

Discrete cosine transform is essentially a transform analysis method. It uses the properties of Fourier transform, which is an ideal mathematical tool in signal processing. It belongs to the orthogonal transformation coding way, is used to remove the spatial redundancy of the image data. Image after the discrete cosine transform, The correlation

of discrete cosine transform coefficients will be smaller. And most of the energy is concentrated in just a few coefficients. Therefore, discrete cosine transform in image compression is very useful, which is the core of international standard JPEG loss image compression.

Three-dimensional discrete cosine transform formula is as follows.

$$F(u,v,w)=c(u)c(v)c(\omega)\left[\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\sum_{z=0}^{P-1} f(x,y,z)*\cos\frac{(2x+1)u\pi}{2M}\cos\frac{(2y+1)v\pi}{2N}\cos\frac{(2z+1)\omega\pi}{2P}\right] \tag{10}$$

$\mu=0,1,\cdots,M-1;\upsilon=0,1,\cdots,N-1;\omega=0,1,\cdots,P-1$

In the formula,

$$c(\mu)=\begin{cases}\sqrt{1/M} & \mu=0\\ \sqrt{2/M} & \mu=1,2,\cdots M-1\end{cases} \tag{11}$$

$$c(\upsilon)=\begin{cases}\sqrt{1/N} & \upsilon=0\\ \sqrt{2/N} & \upsilon=1,2,\cdots N-1\end{cases} \tag{12}$$

$$c(\omega)=\begin{cases}\sqrt{1/P} & \omega=0\\ \sqrt{2/P} & \omega=1,2,\cdots P-1\end{cases} \tag{13}$$

Where $f(x,y,z)$ is volume data of the data values in the (x,y,z). $F(u,v,w)$ is the data corresponding to the three-dimensional discrete cosine transform coefficients.

Three-dimensional inverse discrete cosine inverse transform formula is as follows.

$$f(x,y,z)=\left[\sum_{\mu=0}^{M-1}\sum_{\upsilon=0}^{N-1}\sum_{\omega=0}^{P-1} c(u)c(v)c(\omega)F(u,v,w)*\cos\frac{(2x+1)u\pi}{2M}\cos\frac{(2y+1)v\pi}{2N}\cos\frac{(2z+1)\omega\pi}{2P}\right] \tag{14}$$

$x=0,1,\cdots,M-1;y=0,1,\cdots,N-1;z=0,1,\cdots,P-1$

5. Perceptual Hashing

Perceptual hashing has become hot research topic in the field of multimedia signal processing and multimedia security. Perception of hash function is based on the information processing theory of the cognitive psychology, which is a one-way mapping from the multimedia data set to the multimedia perception. Image perception hashing is a hotspot of research on the last two years perception hashing. Image perception hashing study mainly for image authentication. Perceptual feature extraction used a variety of signal processing method that is consistent with the model of human perception. It can remove the perceptual redundancies, which choose the most has the characteristics of perceptual significance. Perceptual hashing value is perceived good robustness. The premise is the extraction of accurate of perceptual features.

The following is one of the simplest implementation.

Setp1: reduce the size

Pictures would be reduced to the size of the 8*8. It has a total of 64 pixels. The function of this step is to remove the details of the image, only keep the basic information such as structure, light and shade, and abandon the different size, proportion of image difference.

Setp2: simplify the color

Setp3: calculate the average value.

Setp4: compare pixel gray

The gray level of each pixel and the average value are compared. If greater than or equal to the average value, denoted by 1; if less than the average values, denoted as 0.

Setp5: calculate hashing value

The previous step of the comparison results together make up a 64 - bit integer, which is the image feature vector.

6. Zero-watermarking

6.1. Zero-watermarking Embedding

Zero-watermarking embedding process is shown in figure 3.

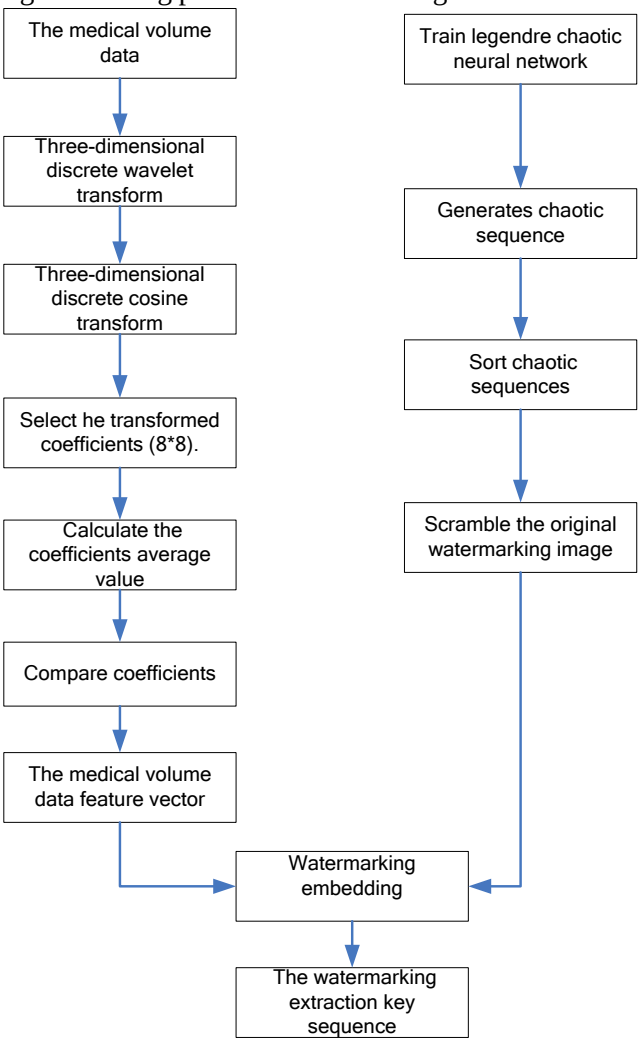


Figure 3. Embedding Process

6.2. Zero-watermarking Extraction

Zero-watermarking extraction process is shown in figure 4.

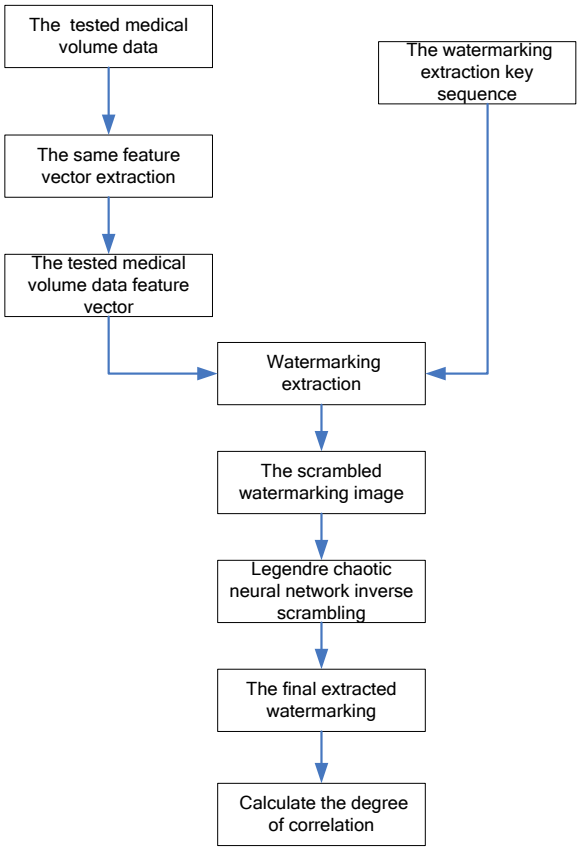


Figure 4. Extraction Process

7. Simulations

In order to verify the algorithm, we carry out the simulation in Matlab2010a platform. The legendre neural network is trained. The number of hidden neurons is 3.The expected error is 10^{-13}, and the number of training is 2000 epochs. Its training error curve is shown in figure 5, in the 130 step it has converged to the expected error 10^{-13}. Scrambling initial value is 0.76. The chaotic sequence for scrambling is shown in figure 6. The scrambled watermarking image is shown in figure 7.

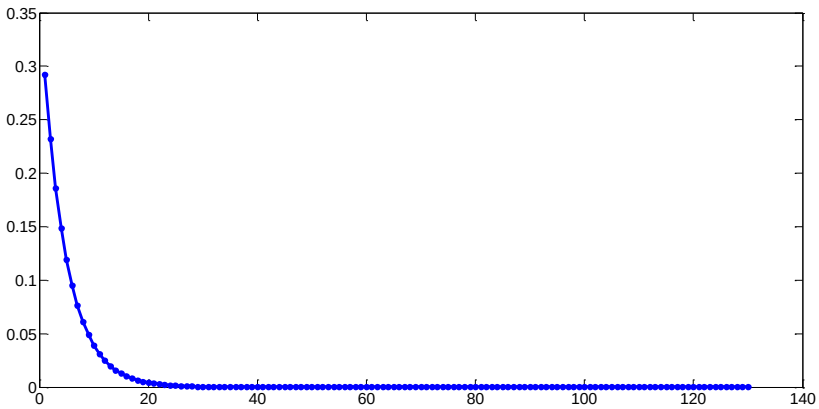


Figure 5. Training Error Curve

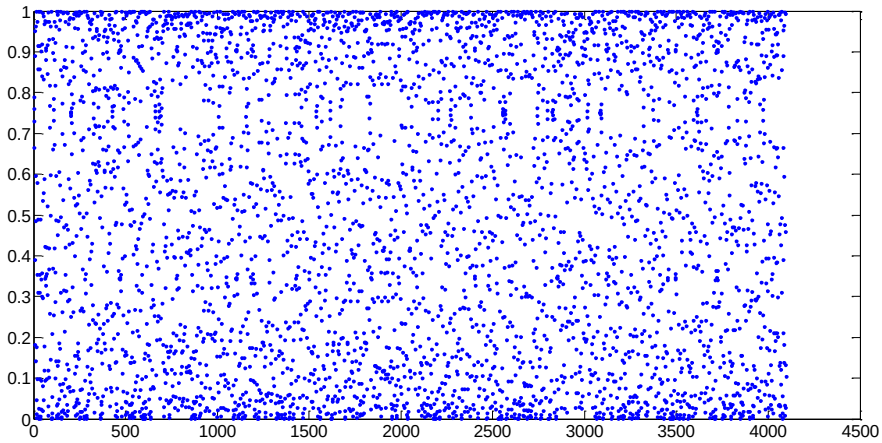


Figure 6. Chaotic Sequence for Scrambling

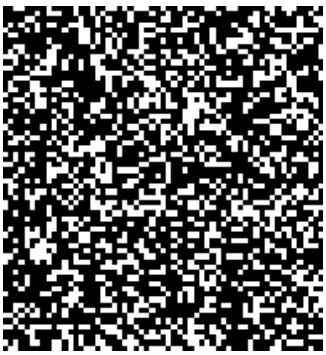
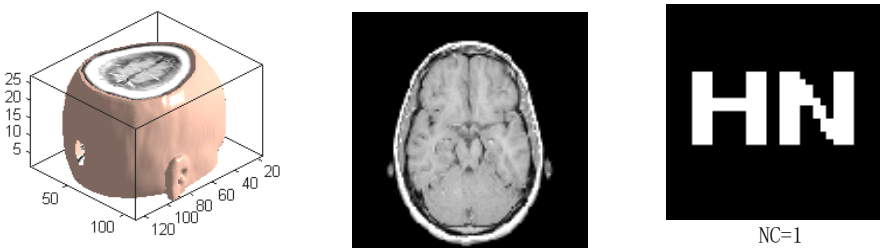


Figure 7. The Scrambled Watermarking Image

(1)Without attack.

The medical volume data without attack is as shown in figure.8 (a).The slice is shown in the figure.8 (b). The extracted watermarking image is shown in the figure.8(c).



(a) (b) (c)

Figure 8. Simulations without Attack

(2)JPEG compression attack

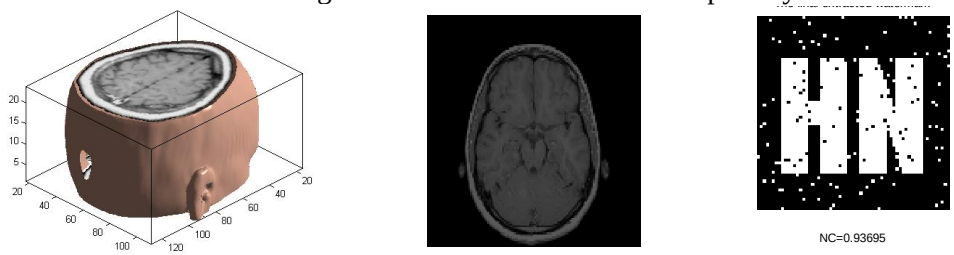
The percentage of compression quality is examined medical volume data after JPEG compression for the impact of watermarking. When the compression quality percentage is 20%, the corresponding three dimensional image of medical volume data is as shown in the figure.9 (a). The slice is as shown in the figure.9 (b). The extracted watermarking is as shown in the figure.9(c). This indicates that the presence of the watermarking can be detected. This shows that the algorithm has better anti-JPEG compression capability.

(a) (b) (c)

Figure 9. Simulations under JPEG Compression Attack

(3)Shear attack

The shear area percentage is examined medical volume data after shear for the impact of watermarking. When the medical volume data is shear 10% from the Z-axis direction. The corresponding three dimensional image of medical volume data is as shown in the figure.10 (a). The slice is as shown in the figure.10 (b).The extracted watermarking is as shown in the figure.10(c). This indicates that the presence of the watermarking can be detected. This shows that the algorithm has a better anti-shear capability.

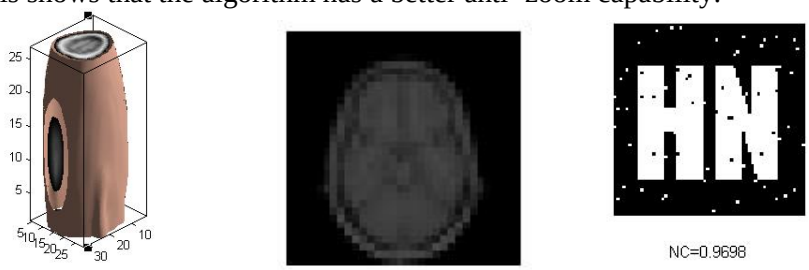


(a) (b) (c)

Figure10. Simulations under Shear Attack

(4) Zoom attack

Medical volume data is zoomed attack. When the zoom factor is 0.25, the corresponding three-dimensional image of medical volume data is as shown in the figure.11 (a). The slice is as shown in the figure.11 (b).The extracted watermarking is as shown in the figure.11(c). This indicates that the presence of the watermarking can be detected. This shows that the algorithm has a better anti- zoom capability.



(a) (b) (c)

Figure11. Simulations under Zoom Attack

8. Conclusions

Along with the construction of hospital informationization, digitalization has more and more deeply permeated in the medical field. Digital watermarking technology as an important branch in the field of information hiding technology research is an effective method to realize the digital medical image protection. Without breaking the original image, this paper proposes a new robust zero-watermarking algorithm for medical volume data. This algorithm solves the contradiction between the watermark can not be perceived

and robust, can achieve blind watermark detection, and has strong robustness to various common attacks. Relationship with the initial value and chaotic sequence is contained in the legendre chaotic neural network, is inherently unpredictable, which achieved the "one-time pad" encryption, and enhanced security of the algorithm.

Acknowledgement

This work was supported the Natural Science Foundation of Hainan Province (No: 614241). Lisha Cai is corresponding author.

References

[1] A. U Rajendra, P. S. Bhat, S. Kumar and L. C. Min, "Transmission and storage of medical images with patient information", Journal of Computers in Biology and Medicine, vol. 33, **(2003)**.
[2] K. A Navas and M. Sasikumar, "Survey of Medical Image Watermarking Algorithms 4th International Conference: Sciences of Electronic", Technologies of Information and Telecommunications, **(2007)**; Tunisia.
[3] M. Alghoniemy and A. H. Tewk, "Geometric invariance in image watermarking", IEEE Transactions on Image Processing, vol. 2, no. 13, **(2004)**.
[4] J. Li, C. Dong, M. Huang, H. Zhang and Y. W. Chen, "A novel robust watermarking for medical image", International Journal of Advances in Information Sciences and Service Sciences, vol. 4, **(2012)**.
[5] Y. Liu and J. Li., "A medical image robust multi watermarking method based on DCT and Logistic Map", Application Research of Computers, vol. 11, **(2013)**.
[6] M. Kutter, S. K. Bhattacharjee and T. Ebrhimi, "Towards second generation watermarking schemes ICIP", **(1999)**.
[7] W. Xia, "Robust digital image watermarking algorithm against geometric attacks", Ph.D. Dissertation of huazhong university of science and technology, **(2010)**.
[8] S. Yang, "The robust image watermarking research", Ph.D. Dissertation of Harbin engineering university, **(2003)**.
[9] G. Gao, "Robust zero watermarking technology research based on chaos and moments", Ph.D. Dissertation of Nanjing university of posts and telecommunications, **(2012)**.
[10] W. Liu, S. Jiang and S. Sun, "Volume data robust watermarking embedding algorithm based on 3D DCT transform", Journal of electronics, vol. 12, no. 33, **(2005)**.
[11] T. Ye, "Anti-JPEG compression and geometric attacks robust zero-watermarking algorithm", Acta Photonica Sinica, vol. 2, no. 41, **(2012)**.
[12] B. Han, J. Li and L. Zong, "A new robust zero-watermarking algorithm for medical volume data", International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 6, no. 6, **(2013)**.
[13] G. Cao and H. Kai, "Image scrambling algorithm based on chaotic weighted sampling theory and sorting transformation", Journal of Beijing University of Aeronautics and Astronautics, vol. 1, no. 39, **(2013)**.

Authors

Baoru Han. He received his M.Sc. in Circuits and Systems from Yanshan University of China in 2007 .Now he is studying for PhD. degree in Information and Communication Engineering at Hainan University of China. Currently, he is a associate professor at Hainan Software Profession Institute, China. His major research interests include digital watermarking, neural network and image processing.

Lisha Cai. She received her M.Sc. in Software Engineering from Zhongshan University of China in 2014. Currently, she is a lecturer at Hainan Software Profession Institute, China. Her major research interests include intelligent diagnosis and intelligent planning.

Wenfeng Li. He received his M.Sc. in Communication and Information Systems from Hainan University of China in 2013. Currently, he is a lecturer at Hainan Software Profession Institute, China. His research direction is computer application.

