International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.6, No.6 (2013), pp.245-258
http://dx.doi.org/10.14257/ijsip.2013.6.6.23

A New Robust Zero-watermarking Algorithm for Medical Volume Data

Baoru Han , Jingbing Li* and Liang Zong

College of Information Science and Technology, Hainan University
Haikou, 570228, Hainan, China

6183191@163.com

Abstract

Aiming at medical image information security problem, this paper proposes a new robust zero-watermarking algorithm for medical volume data based on three-dimensional discrete wavelet transform, three-dimensional Fourier transform and hermite chaotic neural network . Firstly, it employs a novel hermite chaotic neural network to generate the pseudo-random chaotic sequence for scrambling. Secondly, three dimensional medical image is transformed by three-dimensional discrete wavelet transform and three-dimensional discrete Fourier transform. Then, select the transformed low and intermediate frequency coefficients symbol as medical volume data characteristics to structure zero-watermarking. The algorithm integrates hermite chaotic neural network and zero-watermarking technology, which is not confined to artificially selected region of interest. The watermarking extraction does not need the original image. And its security depends on the chaotic sequence complexity and unpredictability, solving the watermark embedding, extraction safety and efficiency. The simulation results show that the algorithm is simple to implement, with good robustness, security and invisibility.

Keywords: *Zero-watermarking algorithm, Three-dimensional discrete wavelet transform, Three-dimensional Fourier transform, Hermite chaotic neural network*

1. Introduction

The digital medical imaging technology, which plays a more and more important role in medicine, has become a very important clinical diagnostic tool since the 1970s. However, the corresponding information security problems gradually emerge [1, 2], though the storage and transmission of medical images is convenient. The current encryption algorithm and application limitation of access control make it difficult to meet the needs of medical image information security and confidentiality, for which the new information security technology research is imperative. Digital watermarking technology, which has been serving as important means to the digital copyright protection and network information security, has got wide attention and become a hot research topic in the field of multimedia information security in recent years [3]. Medical image digital watermarking technology has specific meaning identification information embedded into the carrier image, which can realize the authenticity and integrity authentication of medical images, electronic medical record hiding and copyright protection. Initially, digital watermarking technology, a new kind of digital products copyright protection technology, makes use of data hiding technology to hide specific information in digital products in order to protect the digital product copyright and copyright purposes, proving that the products are genuine and reliable. Now, the usage of

ISSN: 2005-4254 IJSIP

digital watermarking invisibility and robustness can protect medical images and data information transmission on the network, guarantee the digital medical treatment and the development of telemedicine [4].

For medical images, any form of distortion should not happen. Any one medical image acquisition needs the support of precise instruments and expensive medical costs [5]. More importantly, the distortion may cause potential misdiagnosis. In view of this situation, people put forward the concept of zero watermarking [6]. Zero watermarking algorithm, with no modifying the original image to construct watermark, maintaining the important feature of the protected image to construct watermark information, readily avoiding the contradiction between imperceptibility and robustness, further improving the robustness of the watermark [7]. As chaotic sequence has both controllable low-pass characteristics but also has a good correlation property. Currently the usage of digital watermarking technology of chaos theory has become a research hotspot [8, 9].

Through the orgic combination of the hermite chaotic neural network and zero-watermarking algorithm, this paper presents a highly secure medical volume data zero-watermarking algorithm. First, prior to embedding, use a chaotic sequence produced by the hermite chaotic neural network to pretreat the watermark image. Secondly, medical volume data is made three-dimensional wavelet transform and three-dimensional Fourier transform. Then select the transformed low frequency coefficients symbol as feature vector to construct zero watermark. Experiments show that the algorithm has been invisible well, able to adapt to the characteristics of medical image data, and to resist attack, with strong robustness and good safety.

2. Hermite Chaotic Neural Network

Chaos is an approximately random process in nonlinear systems. Two very similar initial chaos is brought into the same function to iterate[10].After a certain stage of the operation, the numerical sequence becomes irrelevant, which is difficult to predict though it belongs to deterministic system; it can not be decomposed though included in the complex system; it is quite regular in reality though seemed chaotic. Chaotic signals are a periodic, continuous broadband frequency spectrum, noise-like characteristic, making it a natural concealment, highly sensitive to initial conditions, and the chaotic signal featured with long-term unpredictability. The concealment, unpredictability, high complexity and easiness to implement of chaotic signal are in line with the requirements of cryptography [11]. Chaotic system is a kind of natural encryption system [12].

In order to improve the security of watermark system and enhance the robustness of watermark against various attacks, the original watermark is usually encrypted before the watermark is embedded host data [13]. In fact, this encryption of watermark sequence method is the watermark image scrambling, which is equivalent to two times the encryption of watermark information, enhancing the ability of the security of the watermark and malicious attack.

This paper uses a new hermite neural network [14]. The hermite neural network model is shown in Figure 1. The hermite neural network selects hermite orthogonal polynomials as the activation function of hidden layer. Performance close to the theoretical values of the chaotic sequence is generated by the neural network weights and the chaos initial value. The chaotic sequence is used for scrambling.

Definition 1 satisfies the following recurrence relations polynomial:

$$\begin{cases} H_0(x)=1, H_1(x)=2x \\ H_{k+1}(x)=2xH_k(x)-2kH_{k-1}(x), k=1,2,\cdots \end{cases} \quad (1)$$

$$x \in (-\infty, \infty)$$

is known as the weight function $\rho(x)=e^{-x^3}$ n hermite orthogonal polynomials.

As shown in Figure 1, the hermite chaotic neural network topology is $m \times n \times 1$. Set the input layer to the hidden layer weight is w_{ij}, hidden layer to the output layer weight is c_j. The activation function of hidden layer neuron is hermite orthogonal polynomials that is defined by formula (1). The hidden layer neuron input is

$$O_j = \sum_{i=1}^{m} w_{ij} x_i, j = 0,1,2,\cdots,n-1 \quad (2)$$

Hidden layer neurons output are as a set of hermite orthogonal polynomial terms $H_j(O_j), j=0,1,2,\cdots n-1$. It can be derived by the formula (1). Hermite chaotic neural network output is

$$y = \sum_{j=0}^{n-1} c_j H_j(O_j) \quad (3)$$

Let chaotic system is

$$y(p) = f[y(p-1), y(p-2), \cdots y(p-m)], p \geq m \quad (4)$$

Where m is the system number of the initial input, $y(0), y(1), \cdots y(m-1)$ is a chaotic initial value, $y(p)$ is the chaotic system output sequence, $f()$ is a chaotic function. Set $x_1 = y(p-1), x_2 = y(p-2), \cdots, x_m = y(p-m)$, the training sample is $(T_t, d_t), t=1,2,\cdots,l$. Where l is the number of samples $T_t = (x_{1t}, x_{2t}, \cdots, x_{mt})$ is hermite chaotic neural network input. d_t is hermite chaotic neural network desired output. The network is trained using BP learning algorithm.

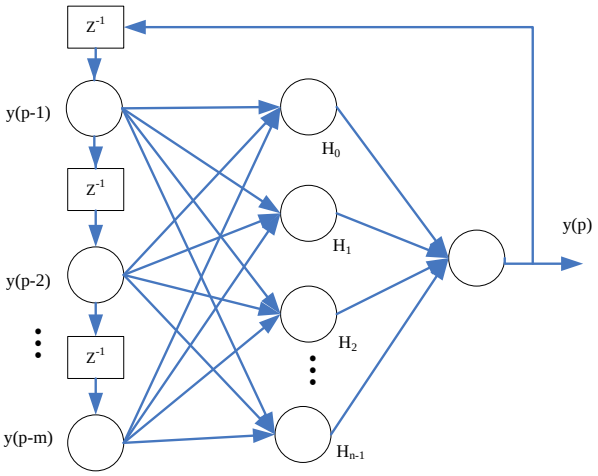


Figure 1. Hermite chaotic neural network

Network weights adjustment formula is as follows.

$$e_t = d_t - y_t \tag{5}$$

$$E = \frac{1}{2}\sum_{t=1}^{l} e_t^{\,2} \tag{6}$$

$$\Delta c_j = -\eta \frac{\partial E}{\partial c_j} \tag{7}$$

$$\Delta w_{ij} = -\eta \frac{\partial E}{\partial w_{ij}} \tag{8}$$

Where $t = 1, 2, \cdots, l$, $i = 1, 2, \cdots, m$, $j = 1, 2, \cdots n$.

This paper adopts the $1 \times 3 \times 1$ network structure. The input layer to the hidden layer all weights is 1. The thresholds of all neurons are 0. The chaotic function takes the Logistic chaotic function.

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

Where $3.5699456 \le u \le 4$, $x \in (0,1)$. The paper use chaotic sequence samples to train hermite neural network. The trained hermite chaotic neural network is used for scrambling.

3. Three-dimensional Discrete Wavelet Transform

Three-dimensional volume data is done multi-resolution decomposition by the wavelet transform, decomposing the image into X, Y, Z of the sub-image in different directions. After the transformation of three-dimensional discrete wavelet, the volume data is decomposed into 8 frequency bands.

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.

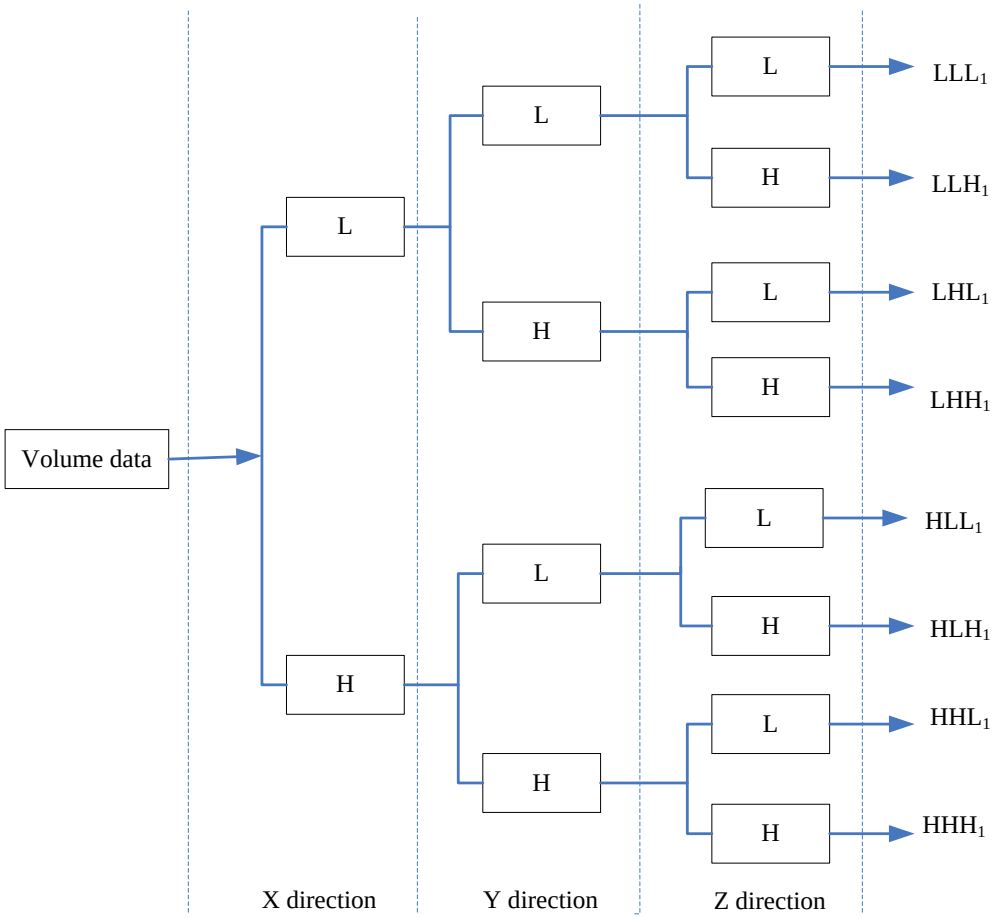


Figure 2. A layer decomposition process for three-dimensional wavelet

4. Three-dimensional Discrete Fourier Transform

Three-dimensional discrete Fourier transform formula is as follows.

$$F(u,v,w)=\sum_{x=0}^{L-1}\sum_{y=0}^{M-1}\sum_{z=0}^{N-1} f(x,y,z)*e^{-j\frac{2\pi x\mu}{L}}e^{-j\frac{2\pi yv}{M}}e^{-j\frac{2\pi zw}{N}} \tag{10}$$

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

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

$$f(x,y,z)=\frac{1}{LMN}\sum_{\mu=0}^{L-1}\sum_{\upsilon=0}^{M-1}\sum_{w=0}^{N-1} F(u,v,w)*e^{j\frac{2\pi x\mu}{L}}e^{j\frac{2\pi yv}{M}}e^{j\frac{2\pi zw}{N}} \tag{11}$$

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

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 Fourier transform coefficients.

5. Feature Extraction

Currently, most watermarking algorithm against geometric attacks is mainly due to poor: people will digital watermark embedded in the voxel or transform coefficients. Volume data slight geometric transformation, often resulting in voxel data values or the transform coefficient suddenly changes, so that the embedded watermark vulnerable. If we are able to extract out of a medical image feature vectors, regardless of what kind of image signal processing, the feature vector has a strong anti-attack capability and the ability to resist geometric transformations, then can use the feature vector for watermark embedding and extraction.

The zero-watermarking information is constructed by an important feature of the image, instead of modifying the original image features. So the zero-watermarking is used in copyright protection of three-dimensional medical image. Medical volume data feature extraction is to construct zero-watermark important foundation. In the paper, the zero-watermarking in transform domain structure has been improved. Three dimensional medical image is three-dimensional discrete wavelet transform and three-dimensional discrete Fourier transform. Select the transformed low and intermediate frequency coefficients symbol as medical volume data characteristics. 1 represents the transformed low and intermediate frequency coefficients positive value and zero. 0 represents t the transformed low and intermediate frequency coefficients negative value. This put the transformed low and intermediate frequency coefficients into a binary sequence, denoted by the characteristic sequence. The feature sequence extracted from the three-dimensional discrete wavelet transform and three-dimensional discrete Fourier transform domain are used as the feature vector of medical volume data.

6. Zero-watermarking algorithm

6.1. Zero-watermarking system

The medical volume data digital watermarking system design is shown in figure 3. The system mainly includes two parts: the watermarking embedding part and the watermarking extraction part. It is essentially a zero-watermarking system.

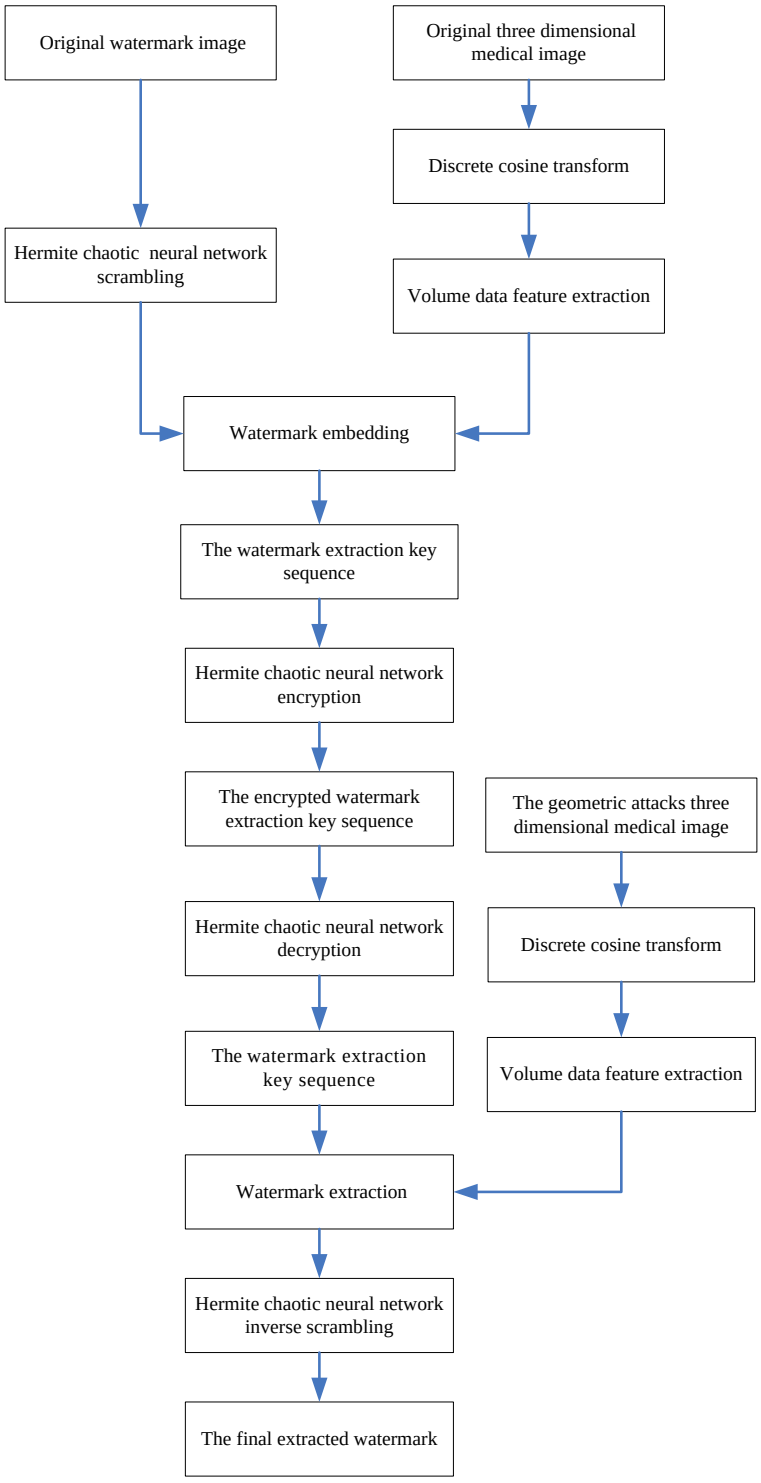


Figure 3. Zero-watermarking system for medical volume data

6.2. Embedding algorithm

Setp1: three dimensional medical image is three-dimensional discrete wavelet transform

and three-dimensional discrete Fourier transform, selecting the transformed low and intermediate frequency coefficients symbol as medical volume data feature vector, denoted by the characteristic sequence.

Setp2: hermite chaotic neural network generates appropriate length of the chaotic sequence. Sort chaotic sequences and get position vector. Based on the position vector, we scramble the original watermarking image.

Setp3: use the HASH function to generate the watermarking extraction key sequence through the XOR operation.

6.3. Extraction algorithm

Setp1: in accordance with the same method, the attacked three dimensional medical image is three dimensional medical image is three-dimensional discrete wavelet transform and three-dimensional discrete Fourier transform, to get the tested medical volume data feature vector.

Setp2: the tested medical image volume data feature vector and the watermarking extraction key sequences are XORed. This can get the scrambled image watermarking image.

Setp3: hermite chaotic neural network generates appropriate length of the chaotic sequence. Sort the chaotic sequences and get the position vector. Based on the position vector, inverse scrambling the scrambled watermarking image, which can get the tested medical volume data watermarking image.

Setp4: on the basis of the original watermarking image and the tested medical volume data watermarking image of correlation degree to judge whether a watermarking embedding. Correlation degree is calculated according to the below formula.

$$NC = \frac{\sum_i \sum_j W(i,j) W'(i,j)}{\sum_i \sum_j W^2(i,j)} \tag{12}$$

Where $W(i,j)$ is the original watermarking image, $W'(i,j)$ is tested medical volume data watermarking image.

7. Simulations

In order to verify the algorithm, we carry out the simulation in Matlab2010a platform. Two groups of logistic chaotic function initial values are set as follows. μ=4, $x(0) = 0.2$. The hermite neural network parameters are as follows. The number of hidden neurons is 3, expected error is 10^{-10}, and the number of training is 5000 epochs. The best individual fitness value change process is shown in Figure 4, in the 115 step it has converged to the expected error 10^{-10}.

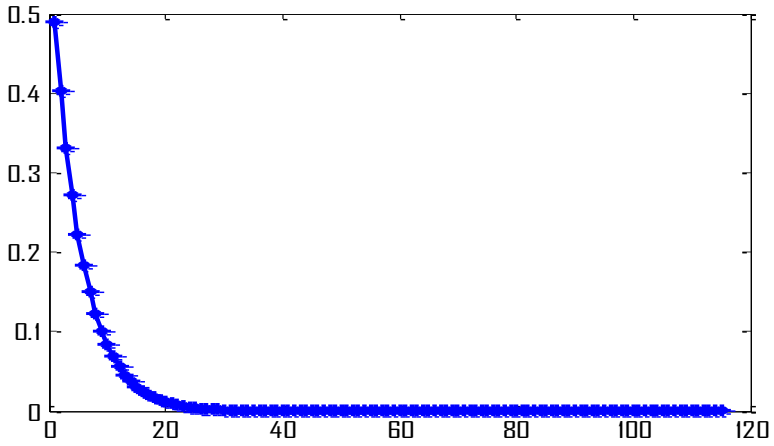


Figure 4. Training error curve

The scrambling initial value is 0.9. The chaotic sequence for scrambling is shown in Figure 5.

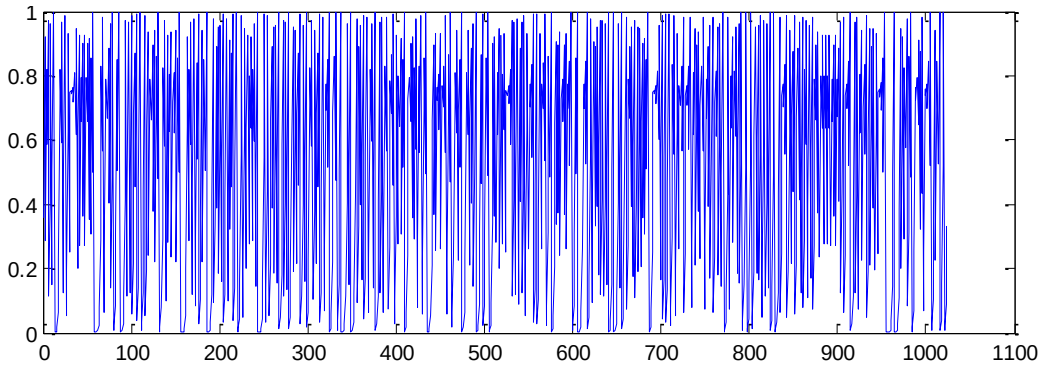
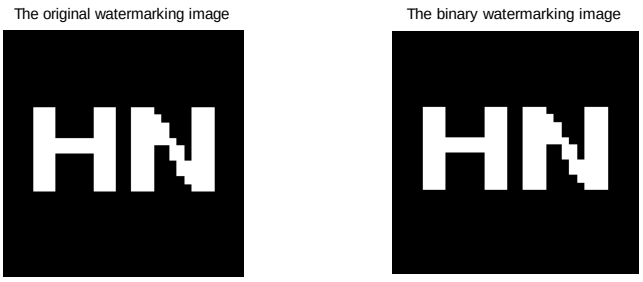


Figure 5. Chaotic sequence for scrambling

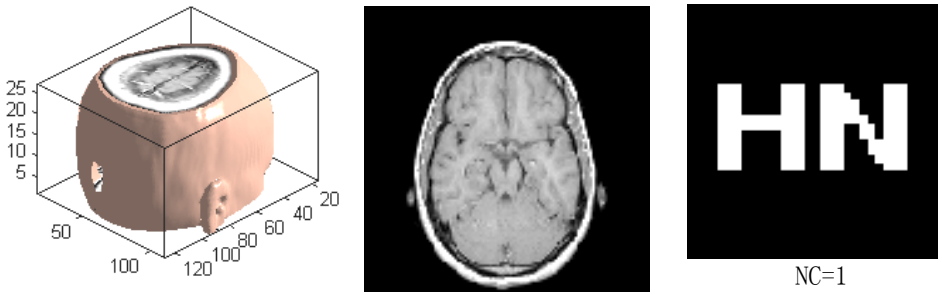
We use 32*32 significant image as the watermarking image. Figure 6(a) shows the original watermarking image. Figure 6(b) shows the binary watermarking image.



(a) (b)

Figure 6. The watermarking image

The three dimensional image of medical volume data without attack is as shown in Figure 7(a).The slice is shown in the Figure 7(b). The extracted watermarking image is shown in the Figure 7(c).



(a) (b) (c)

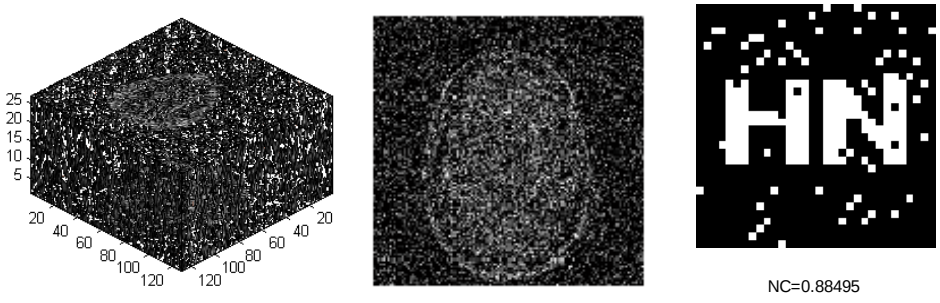
Figure 7. Simulations without attack

7.1 Robustness

In order to test the robust performance of medical volume data digital watermarking algorithm, we have chosen the following spects to authentication.

(1) Gaussian noise attack

Gauss noise intensity coefficient is measured the added noise interference size in medical volume data. When the noise intensity is 8%, the corresponding three dimensional image of medical volume data is as shown in the Figure 8(a). The slice is as shown in the Figure 8(b). The extracted watermarking is as shown in the Figure 8(c). This indicates that the presence of the watermarking can be detected. This shows that the algorithm has better anti-gaussian noise immunity.

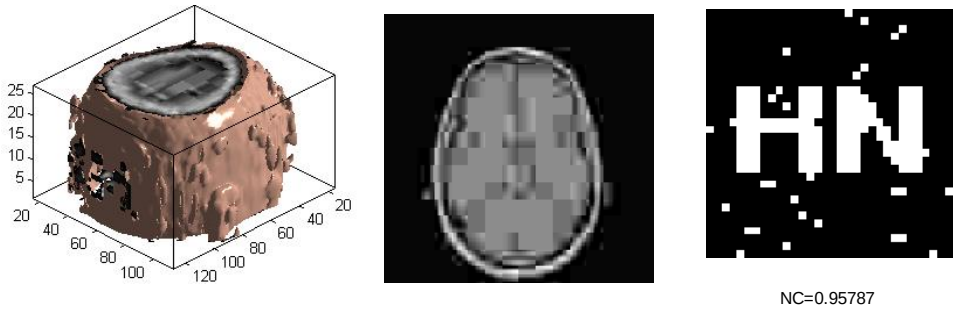


(a) (b) (c)

Figure 8. Simulations under gaussian noise 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 8%, 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.

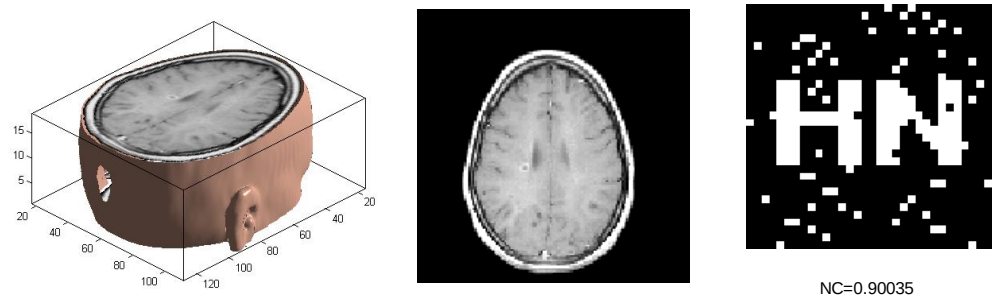


(a) (b) (c)

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 30% 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.

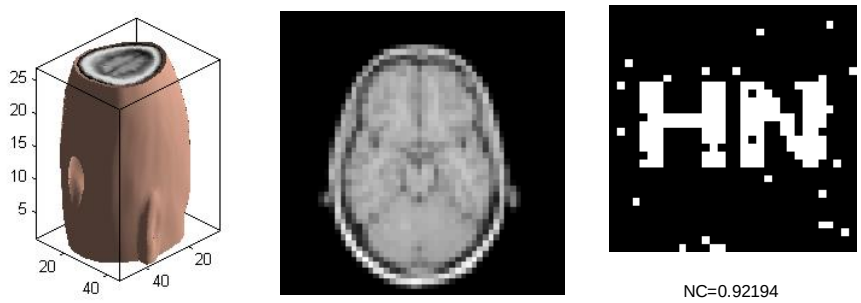


(a) (b) (c)

Figure 10. Simulations under shear attack

(4) Zoom attack

Medical volume data is zoomed attack. When the zoom factor is 0.4, 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)

Figure 11. Simulations under zoom attack

7.2 Security

In order to study the safety of medical volume data watermarking algorithm, it verifies whether the sequence of hermite chaotic neural network has the chaotic behavior. The autocorrelation is shown in Figure 12. The scrambled watermarking image is shown in Figure 13. The watermarking extraction key sequence image is shown in Figure 14.

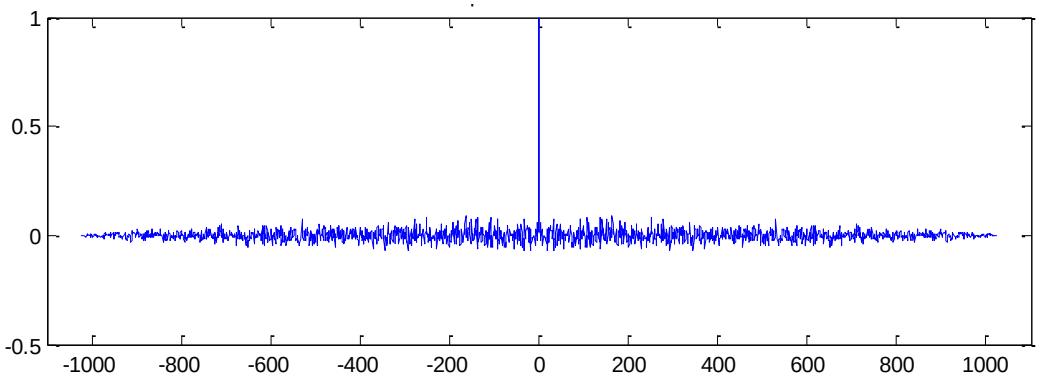


Figure 12. The chaotic sequence for scrambling and its autocorrelation

Figure 13. The scrambled watermarking image

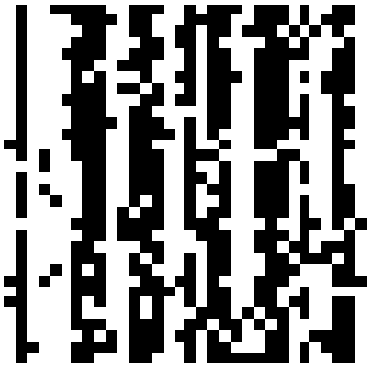


Figure 14. The watermarking extraction key sequence image

8. Conclusions

This paper proposed a new zero-watermarking algorithm for medical volume data. The algorithm, with the chaotic neural network for scrambling, which maked the watermarking extraction key sequence very sensitive to the key, with good pseudo randomness, complexity, difficult to analyze, unpredictability, has reached the one-time encryption goal with a higher safety performance. Meanwhile, the algorithm need not require artificial selection for the region of interest, with no embedding capacity limit. The watermarking can be extracted without the original image, thus avoiding the original medical image tampering. The algorithm had good resistance to conventional attack capability and resistance to geometric attacks capability. Thus this algorithm had very high practical value and a broad application prospect.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (No: 61263033) and the Natural Science Foundation of Hainan Province (No: 613166). Jingbing Li is corresponding author.

References

[1] M. Barni and F. Bartolini, "Data hiding for fighting piracy", IEEE Signal Processing Magazine, vol. 2, no. 21, **(2004)**.
[2] R. Acharya U., 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)**.
[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] M. M. Soliman, A. E. Hassanien, N. I. Ghali and H. M. Onsi, "An adaptive watermarking approach for medical imaging using swarm intelligent", International Journal of Smart Home, vol. 1, **(2012)**, pp. 6.
[6] G. Coatrieux, C. Le Guillou, J. M. Cauvin and C. Roux, "Reversible watermarking for knowledge digest embedding and reliability control in medical images", IEEE Transactions on Information Technology in Biomedicine, vol. 2, **(2009)**, pp. 13.
[7] S. Sun and Z. Lu, "Digital watermarking techniques", Acta Electronica Sinica, vol. 8, no. 18, **(2000)**.
[8] X. Zhang, "Reversible data hiding in encrypted image", IEEE Signal Processing Letter, vol. 4, no. 18, **(2011)**.
[9] C. R. Mirasso, "Chaos shift keying encryption in chaotic external cavity semiconductor lasers using a single receiver scheme", IEEE Photonics Technology Letters, vol. 4, no. 14, **(2002)**.

[10] G. Cao, K. Hu and T. Wei, "Logistic uniform distribution based image scrambling", Acta Physical Sinica, vol. 11, no. 60, **(2011)**.
[11] 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).**
[12] S. Lian, J. Sun and Z. Wang, "Security analysis of a chaos based image encryption algorithm", Physics letters A, vol. 2, **(2005)**, pp. 351.
[13] D. Bouslimi, G. Coatrieux, M. Cozic and C. Roux, "A Joint Encryption watermarking system for verifying the reliability of medical images", IEEE Transactions on Information Technology in Biomedicine, vol. 5, no. 16, **(2012)**.
[14] A. Zou and Y. Zhang, "An asynchronous encryption algorithm based on hermite chaotic neural networks", CAAI Transactions on Intelligent Systems, vol. 5, no. 4, **(2009).**

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. His major research interests include digital watermarking, neural network and image processing.

Jingbing Li. He received his M.Sc. in automation from Beijing Institute of Technology of China in 1996. He received the PhD. degree in Control Theory and Engineering from Chongqing University of China in 2007. Currently, he is a Professor at Hainan University, China. His major research interests include digital watermarking and image processing. He is corresponding author of this paper.

Liang Zong. He received his M.Sc. in Computer Application Technology from Ningbo University of China in 2010. Now he is studying for PhD. degree in Information and Communication Engineering at Hainan University of China. His major research interests include communication networks.

