INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
ISSN 1841-9836, 10(2):188-199, April, 2015.

Zero-watermarking Algorithm for Medical Volume Data Based on Difference Hashing

B.R. Han, J.B. Li, Y.J. Li

Baoru Han, Jingbing Li*, Yujia Li
College of Information Science and Technology
Hainan University
Haikou, 570228, China
Email:6183191@163.com, Jingbingli2008@hotmail.com, liyujia1219@gmail.com
*Corresponding author: Jingbingli2008@hotmail.com

Abstract: In order to protect the copyright of medical volume data, a new zero-watermarking algorithm for medical volume data is presented based on Legendre chaotic neural network and difference hashing in three-dimensional discrete cosine transform domain. It organically combines the Legendre chaotic neural network, three-dimensional discrete cosine transform and difference hashing, and becomes a kind of robust zero-watermarking algorithm. Firstly, a new kind of Legendre chaotic neural network is used to generate chaotic sequences, which causes the original watermarking image scrambling. Secondly, it uses three-dimensional discrete cosine transform to the original medical volume data, and the perception of the low frequency coefficient invariance in the three-dimensional discrete cosine transform domain is utilized to extract the first 4*5*4 coefficient in order to form characteristic matrix (16*5). Then, the difference hashing algorithm is used to extract a robust perceptual hashing value which is a binary sequence, with the length being 64-bit. Finally, the hashing value serves as the image features to construct the robust zero-watermarking. The results show that the algorithm can resist the attack, with good robustness and high security.

Keywords: zero-watermarking, medical volume data, difference hashing, Legendre chaotic neural network, three-dimensional discrete cosine transform.

1 Introduction

With the extensive application of digital technology, a large number of digital images are used in our daily life and work. Digital images meet the requirements of people's senses, and also provide convenience for people's life and work. People pay more and more attention to the copyright issues in digital image. Digital watermarking, as a new security measure, is widely used in digital image copyright protection [1, 2]. As an important branch of information security research area, digital watermarking also is an effective way to protect the integrity of digital image [3, 4]. It is an effective complement to traditional encryption techniques. Digital watermarking is the meaningful information hidden into the digital works, as a basis for the identification of copyright. At the same time, the watermarking information can be detected and analyzed by detecting algorithm, to determine the copyright holder and to protect the digital products. However, due to the digital watermarking technology research being multidisciplinary, the communication theory, computer science and signal processing, and many other areas involved, for which it is unable to avoid the inherent drawbacks in these fields [5, 6]. This brings certain difficulty and challenge to research work. At present, in the field of digital watermarking, the digital image watermarking has become a branch of the most widely used, the most mature development, and the most fruitful achievements [7].

Along with the construction of hospital informatization, digitalization has become more and more deeply into the medical field [8]. Medical diagnostic equipment will produce a lot of medical image information every day. These medical images as a basis for medical diagnosis have an extremely important position. The establishment of medical digital image transmission standard has promoted the exchange of the digital medical imaging information. However, medical images information during network transmission may also encounter tampering, illegal copying and other information security issues [9,10]. Medical image is not only an important basis for doctors to diagnose the disease, but also involving the patient's privacy. In order to ensure the medical image security, reliability and availability, we must effectively solve the security problem of medical image management. The emergence of medical image digital watermarking can solve this problem [11]. It is the specific meaning digital information or some secret information embedded into the digital medical image, which can realize the information hiding and copyright protection. Medical image especially is strict to the requirement of image quality does not allow the distortion and not allowed to do any changes. In this case, people put forward the concept of zero-watermarking [12]. Zero-watermarking is a novel digital watermarking technique. It is different from general digital watermarking in its use of the characteristics of the original image to construct the watermarking, and not directly embed watermarking in the image, so it does not break the original image [13].

Image hashing is also called the digital fingerprint, it is a summary of multimedia information, which can be widely applied in image authentication, image indexing and retrieval, digital image watermarking, etc [14]. Image hashing represents the image itself with a short digital sequence, which is a kind of expression of image compression based on visual content. Usually, the image hashing should satisfy the requirements of perceptual robustness, uniqueness and security. Image hashing technique can be any image-resolution image data into a binary sequence of hundreds or thousands of bits. For a large database of image retrieval, this means greatly reducing the search time, but also reduces the cost of storage media images. At the same time, its robustness feature ensure that it can resist a variety of different types of attacks. In addition, the characteristics of image hashing technology security make the copyright protection of image become possible. The main image hashing methods now mainly focus on the characteristics of robustness study [15,16]. It is mainly divided into the method based on image statistics, a rough image representation, the relationship and visual feature points extraction. Combined the features of above mentioned extraction methods, in order to better satisfy the perceptual image hashing robustness, security, and uniqueness, the discrete cosine transform to extract the feature is considered to be an ideal method. According to the characteristics of medical volume data, this paper presents a zero-watermarking algorithm for medical volume data based on Legendre chaotic neural networks and differences hashing. The algorithm is based on three-dimensional discrete cosine transforms perception of the low frequency coefficient invariance and image hashing robust feature, which is a robust zero-watermarking method. The algorithm uses the robust hashing sequence in medical volume data transform domain to construct the zero-watermarking, instead of modifying the features of medical volume data. It can adapt to the characteristics of medical volume data, can resist strong attack, and has very strong robustness. And it uses Legendre chaotic neural network scrambling and encryption, which has good security and confidentiality.

2 Legendre chaotic neural network

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

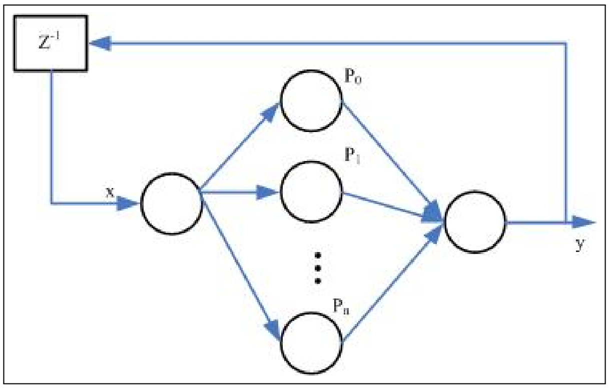


Figure 1: Legendre chaotic neural network

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

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

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

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

Set 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 legendre chaotic neural network input. d_t is Legendre chaotic neural network desired output. The network is trained using BP learning algorithm.

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 $t = 1, 2, \cdots, l$; $j = 0, 1, 2, \cdots, n$.

3 Three-dimensional discrete cosine transform

Three-dimensional discrete cosine transform formula is as follows.

$$F(u,v,w)=c(u)c(v)c(w)\left[\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\sum_{z=0}^{P-1}f(x,y,z)*\cos\frac{(2x+1)u\pi}{2M}\cos\frac{(2y+1)v\pi}{2N}\cos\frac{(2z+1)w\pi}{2P}\right] \quad (9)$$

$u=0,1,\cdots,M-1;v=0,1,\cdots,N-1;w=0,1,\cdots,P-1$

In the formula,

$$c(u)=\begin{cases}\sqrt{1/M} & u=0\\ \sqrt{2/M} & u=1,2,\dots,M-1\end{cases} \quad (10)$$

$$c(u)=\begin{cases}\sqrt{1/N} & v=0\\ \sqrt{2/N} & v=1,2,\dots,N-1\end{cases} \quad (11)$$

$$c(u)=\begin{cases}\sqrt{1/P} & w=0\\ \sqrt{2/P} & w=1,2,\dots,P-1\end{cases} \quad (12)$$

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:

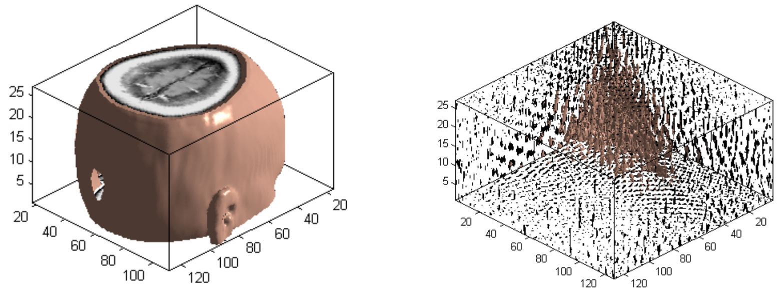
$$f(x,y,z)=\left[\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\sum_{z=0}^{P-1}F(u,v,w)*\cos\frac{(2x+1)u\pi}{2M}\cos\frac{(2y+1)v\pi}{2N}\cos\frac{(2z+1)w\pi}{2P}\right] \quad (13)$$

$u=0,1,\cdots,M-1;\, v=0,1,\cdots,N-1;\, w=0,1,\cdots,P-1$

Three-dimensional discrete cosine transform for medical volume data is shown in figure 2.

4 Difference hashing

Perceptual hashing has become a hot research topic in the field of multimedia signal processing and multimedia security. Perceptual feature extraction is the core part of the perceptual hashing structure. The validity and reliability of perceptual feature extraction will directly affect the robustness and uniqueness of image perception hashing sequence. Image perceptual hashing study is mainly for image authentication and image retrieval. Image features include image color, texture, edge, corner and image transform domain coefficient, etc. Compared with perceptual hashing, difference hashing in speed is much faster. Compared with the average hashing, the effect of the difference hashing is better in the case of almost the same efficiency. It is based on the gradual implementation. Based on the difference hashing algorithm, a difference hashing algorithm in three-dimensional discrete cosine transform domain is presents for medical volume



(a) The original medical volume data

(b) The medical volume data in transform domain

Figure 2: Three-dimensional discrete cosine transform for medical volume data

data feature extraction in this paper. Figure 3 depicts the algorithm flow. In the algorithm flow, medical volume data is represented by a three-dimensional map into a one-dimensional feature vector. The algorithm is used to extract the robust features of medical volume data, which can increase the robustness of watermarking algorithm.

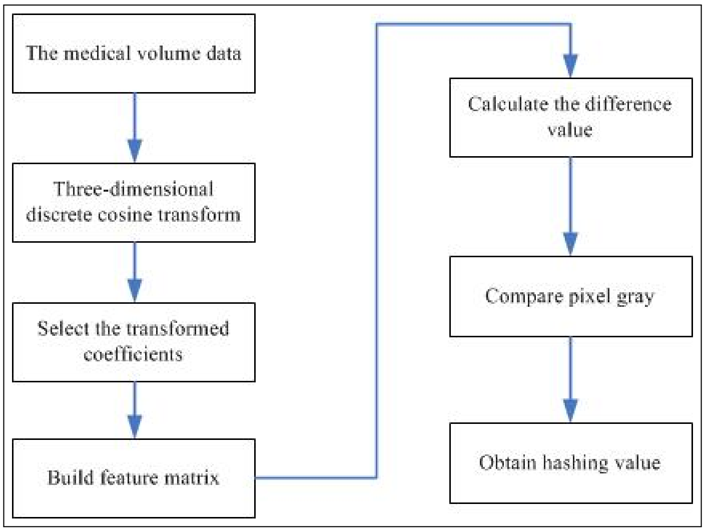

The medical volume data
Three-dimensional discrete cosine transform
Select the transformed coefficients
Build feature matrix
Calculate the difference value
Compare pixel gray
Obtain hashing value

Figure 3: The difference hashing algorithm flow

5 Zero-watermarking algorithm

Zero-watermarking embedding

Figure 4 illustrates zero-watermarking embedding process.

Zero-watermarking extraction

Figure 5 illustrates zero-watermarking extraction process.

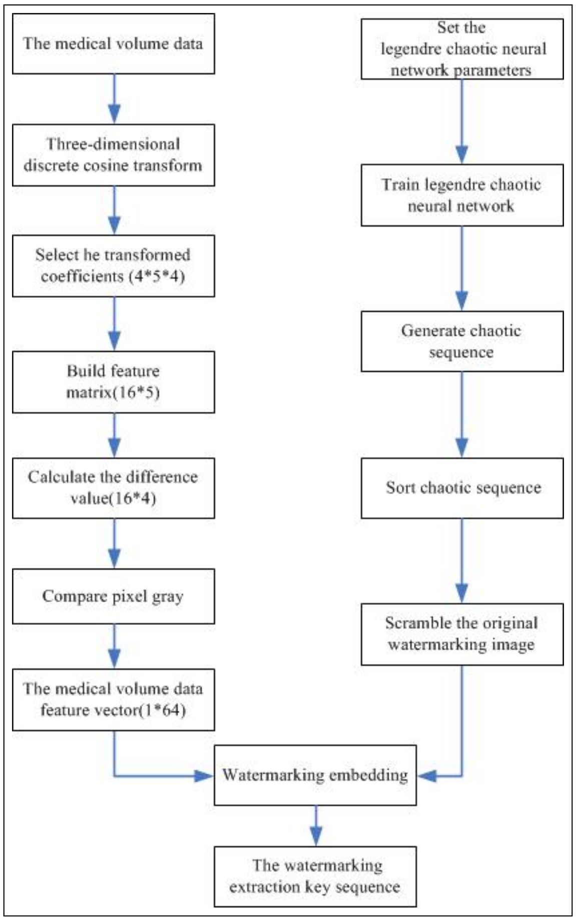

The medical volume data
Three-dimensional discrete cosine transform
Select he transformed coefficients (4*5*4)
Build feature matrix(16*5)
Calculate the difference value(16*4)
Compare pixel gray
The medical volume data feature vector(1*64)
Set the legendre chaotic neural network parameters
Train legendre chaotic neural network
Generate chaotic sequence
Sort chaotic sequence
Scramble the original watermarking image
Watermarking embedding
The watermarking extraction key sequence

Figure 4: Embedding process

6 Simulation and analysis

The legendre chaotic neural network parameters are as follows. The number of hidden neurons is 3,$E = 10^{-4}$,$\eta = 0.1$,$l = 1000$ and the number of training is 1500 epochs. Its training error curve is shown in figure 6, in the 69 epoch it has converged to the expected error. Scrambling initial value is 0.46. The chaotic sequence for scrambling is shown in figure7. The scrambled watermarking image is shown in figure 8.

1. Without attack
   The medical volume data without attack is as shown in figure 9 (a). The slice is shown in the figure.9 (b). The extracted watermarking image is shown in the figure 9(c).

2. Filtering attack
   Medical volume data is filtered attack. Using $[5 * 5]$ median filter, repeat 10 times, the corresponding medical volume data is shown in the figure 10 (a). The slice is shown in the figure 10 (b). The extracted watermarking image is shown in the figure 10(c). This shows that the algorithm has a better anti-filter ability.

3. 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 medical volume data is shown in the figure 11 (a). The slice is shown

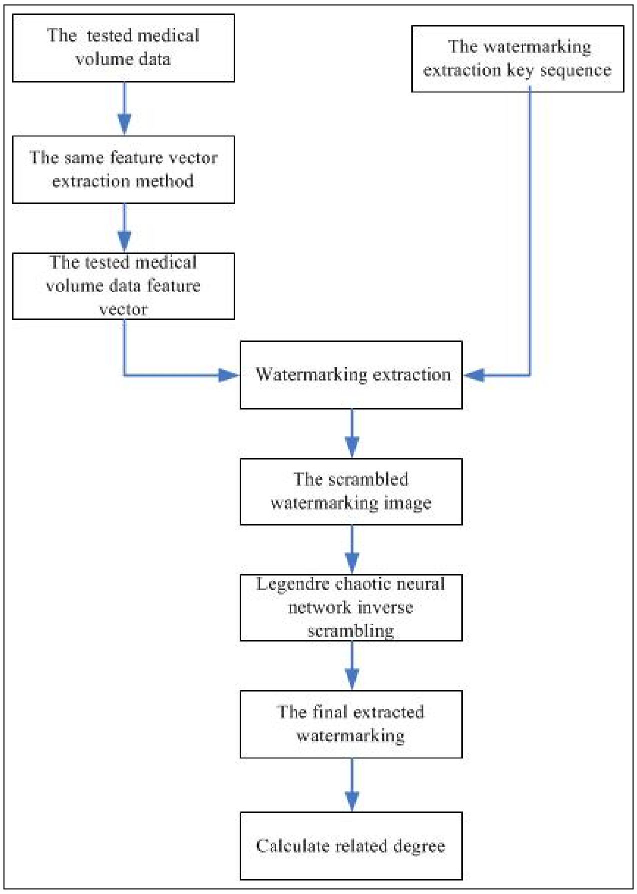

The tested medical volume data
The watermarking extraction key sequence
The same feature vector extraction method
The tested medical volume data feature vector
Watermarking extraction
The scrambled watermarking image
Legendre chaotic neural network inverse scrambling
The final extracted watermarking
Calculate related degree

Figure 5: Extraction process

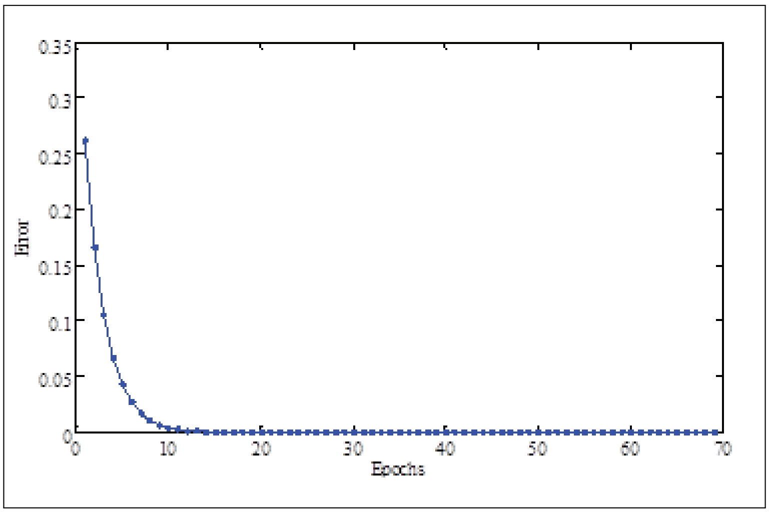


Figure 6: Training error curve

in the figure 11 (b). The extracted watermarking image is shown in the figure 11(c). This shows that the algorithm has better anti-JPEG compression capability.

4. Gaussian noise attack
   Gauss noise intensity coefficient is measured the added noise interference size in medical

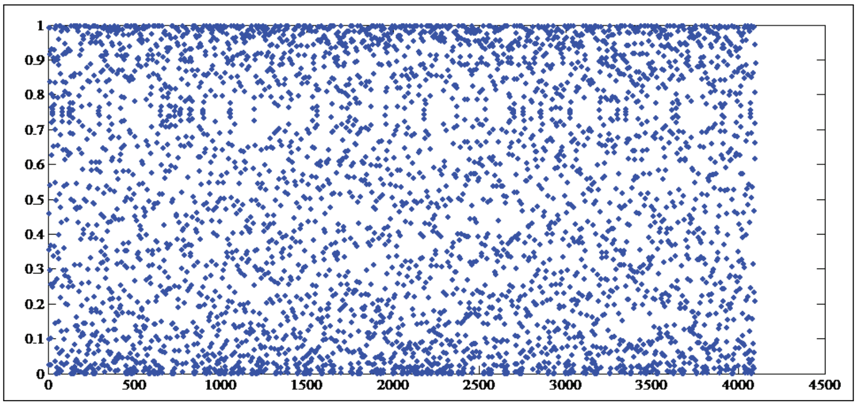


Figure 7: Chaotic sequence for scrambling

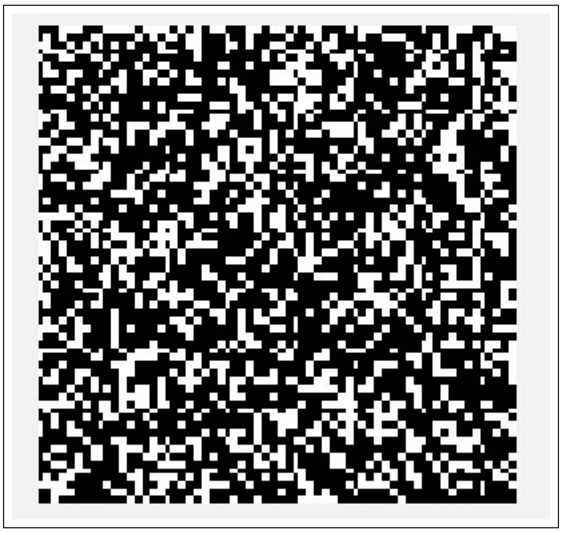
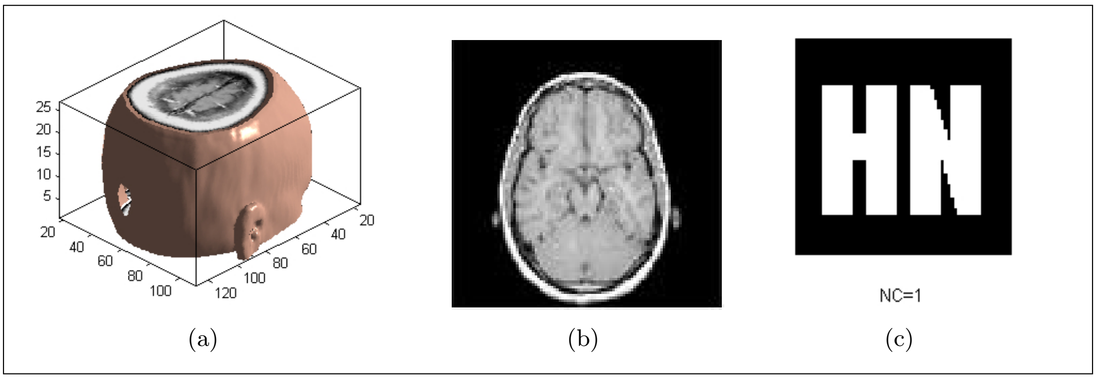


Figure 8: The scrambled watermarking image



(a) (b) (c)

Figure 9: Simulations without attack

image. When the noise intensity is 20%, the corresponding medical volume data is shown in the figure 12 (a). The slice is shown in the figure 12 (b). The extracted watermarking is shown in the figure 12(c). This shows that the algorithm has strong robustness against noise attack.

5. Zoom attack

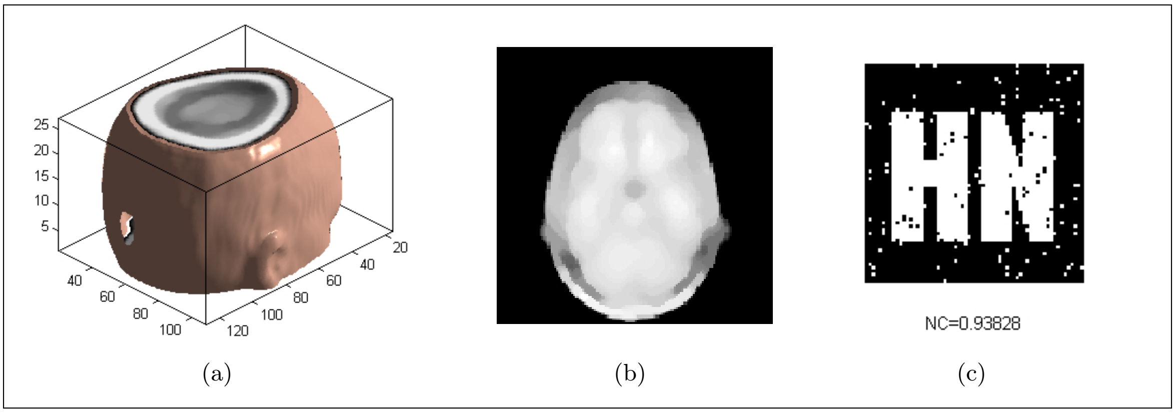


Figure 10: Simulations under filtering attack

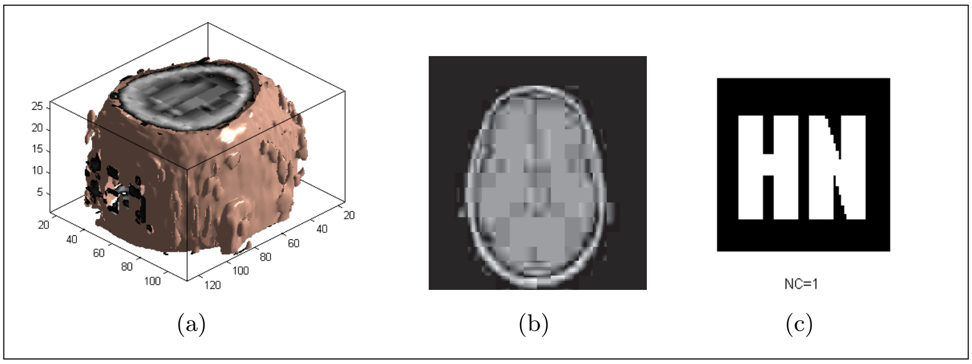


Figure 11: Simulations under JPEG compression attack

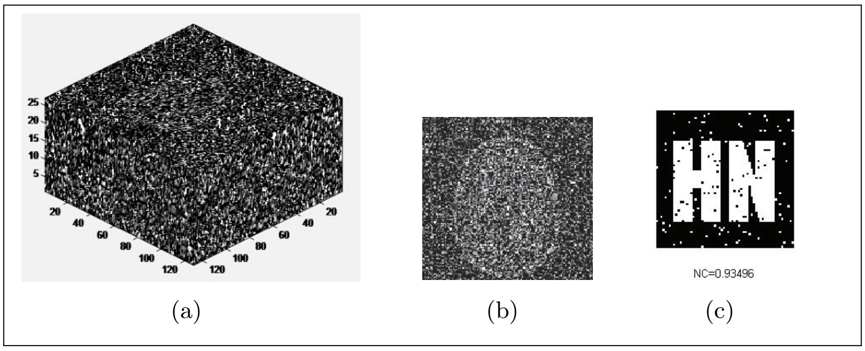
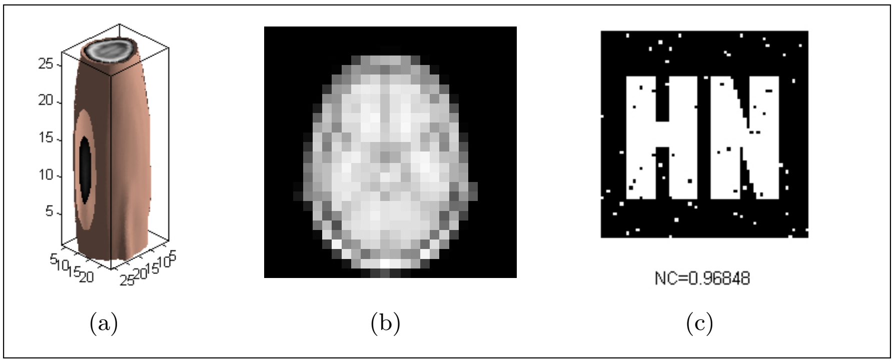


Figure 12: Simulations under filtering attack

Medical image is zoomed attack. When the zoom factor is 0.2, the corresponding medical volume data is shown in the figure 13 (a). The slice is shown in the figure 13 (b). The extracted watermarking image is shown in the figure.13(c). This shows that the algorithm has strong robustness against zoom attack.

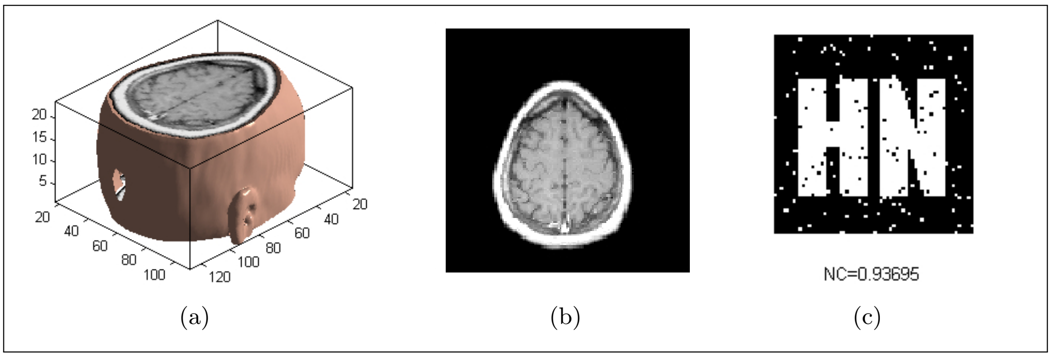
6. Shear attack
   When the medical volume data is shear 10% from the Z-axis direction. The corresponding medical volume data is shown in the figure.14 (a). The slice is shown in the figure 14 (b). The extracted watermarking image is shown in the figure 14(c). This shows that the algorithm has a better anti-shear capability.

7. Translate attack



(a) (b) (c)

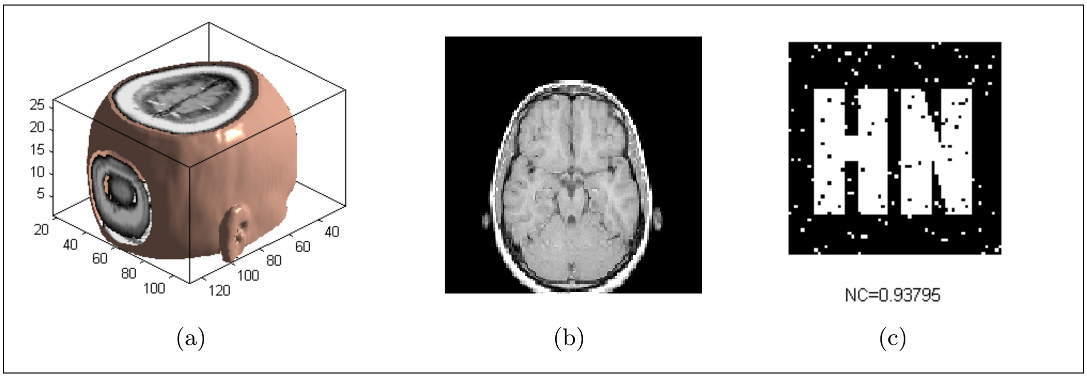
Figure 13: Simulations under filtering attack



(a) (b) (c)

Figure 14: Simulations under filtering attack

Medical volume data is translated attack. When the vertical downward is 5%, the corresponding medical volume data is shown in the figure 15 (a). The slice is shown in the figure 15 (b). The extracted watermarking image is shown in the figure 15(c). This shows that the algorithm has a better anti-translate capability.

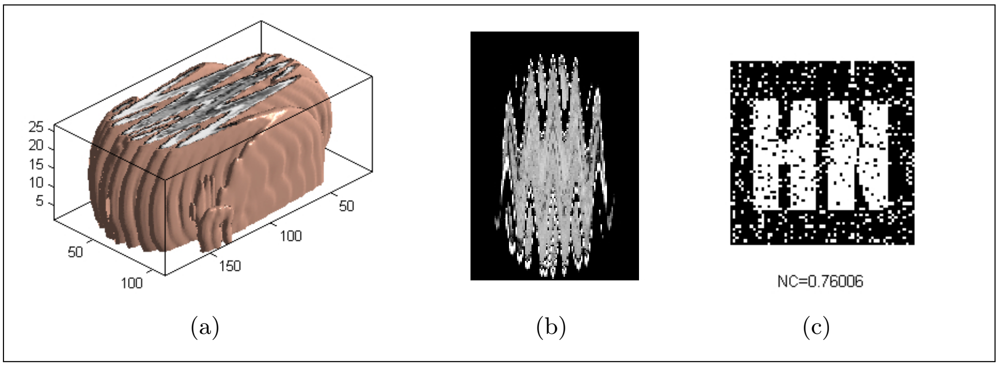


(a) (b) (c)

Figure 15: Simulations under filtering attack

8. Distort attack
   Medical volume data is distorted attack. When the distorting factor is 15, the corresponding medical volume data is shown in the figure 16 (a). The slice is as shown in the figure 16 (b). The extracted watermarking is shown in the figure 16(c). This shows that the algorithm has a better anti-distort capability.

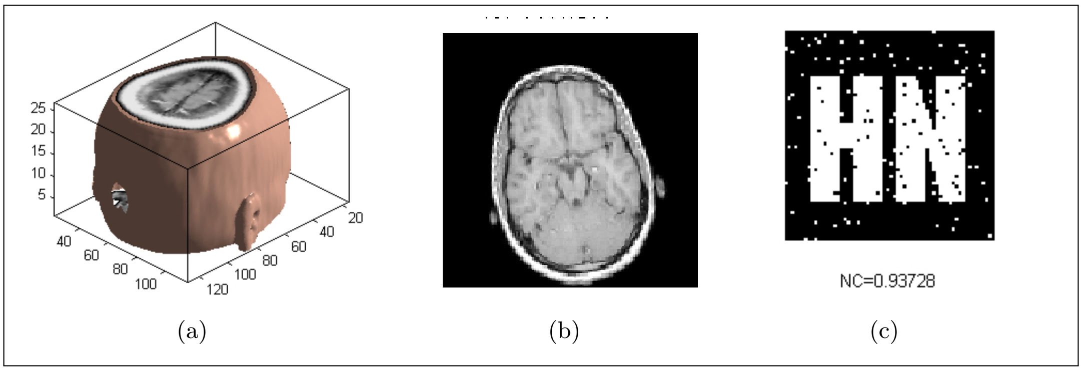
9. Rotation attack.



(a) (b) (c)

Figure 16: Simulations under filtering attack

Medical volume data is rotated attack. When the medical volume data rotated anticlockwise 10 degrees, the corresponding medical volume data is shown in the figure 17 (a). The slice is shown in the figure 17 (b). The extracted watermarking image is shown in the figure 17(c). This shows that the algorithm has a better resistance to rotation attack ability.



(a) (b) (c)

Figure 17: Simulations under filtering attack

7 Conclusion

According to the transform domains perception of the low frequency coefficient invariance and the robustness of image hashing, a new robust watermarking algorithm for medical volume data is presented in this paper. It shows that the algorithm has the following characteristics.

1. The medical volume data has the good transparency without making any changes to the original medical data.

2. It uses the discrete cosine transform coefficients of low frequency stability characteristics and difference hashing algorithm robustness, thereby increasing the robustness of the algorithm.

3. The relationship between the initial values and chaotic sequences is contained in the chaotic neural network, which is inherently unpredictable. Therefore, the algorithm is theoretically absolutely security.

4. The watermarking can be extracted without original medical volume data, and it realizes the blind detection. The results show that this algorithm has better robustness and security.

8 Acknowledgements

This work was supported by the National Natural Science Foundation of China (No: 61263033) and the Natural Science Foundation of Hainan Province (No: 614241).

Bibliography

[1] R.Barnett (1999); Digital Watermarking: applications. Techniques and Challenges, *Electronics & Communications of Engineering Journal*, 11(4):173-183.

[2] Cox I J, Kilianj, Leighton F T. (2003); Secure spread specture watermarking for multimedia . *IEEE Trans on Image Processing*, 6 (12):1673-1687.

[3] Xueming Li, Guangjun He.(2012); Efficient audio zero-watermarking algorithm for copyright protection based on BIC and DWCM matrix, *Int. J. of Advancements in Computing Technology*, 4 (6): 109-117.

[4] Bami M, Bartolinit F, Rosa A D. (2000); Capacity of full frame DCT image watermarks, *IEEE Trans. on Image Processing*, 9 (8):1450-1455.

[5] Guanghui Cao, Hu Kai (2013); Image scrambling algorithm based on chaotic weighted sampling theory and sorting transformation, *Journal of Beijing University of Aeronautics and Astronautics*, 39(1):67-72.

[6] Yaoli Liu, Jingbing Li (2013); A medical image robust multi watermarking method based on DCT and Logistic Map, *Application Research of Computers*, 30(11):3430-3433.

[7] J-L Dugelay, S. Roche, C. Rey, G. Doerr (2006); Still image watermarking robust to local geometric distortions. *IEEE Trans. on Image Processing*, 15(9):2831-2842.

[8] Giakoumaki A., Pavlopoulos S., Koutsouris D. (2006) Multiple image watermarking applied to health information management. *Information Technology in Biomedicine, IEEE Transactions on*, 10(4): 722-732.

[9] Wu J H K, Chang R F, Chen C J, et al.(2008); Tamper detection and recovery for medical images using near-lossless information hiding technique, *Journal of Digital Imaging*, 21(1): 59-76.

[10] Tan C.K., Ng J.C., Xu X.T. Security protection of DICOM medical images using dual-Layer reversible watermarking with tamper detection capability. *Journal of Digital Imaging.* 2011, 24(3):528-540.

[11] Deng X.H., Chen Z.G., Deng X.H., et al. (2001); A Novel Dual-Layer Reversible Watermarking for Medical Image Authentication and EPR Hiding, *Advanced Science Letters*, 4(11):3678-3684.

[12] Baoru Han, Jingbing Li (2013); A robust watermarking algorithm for medical volume data based on hermite chaotic neural network, *Int. J. of Applied Mathematics and Statistics*, 48(18):128-135.

[13] Baoru Han, Jingbing Li and Liang Zong (2013); A new robust zero-watermarking algorithm for medical volume data, *Int. J. of Signal Processing, Image Processing and Pattern Recognition*, 6(6):245-258.

[14] H. C. Yang, S. B. Zhang, and Y. B. Wang (2012); Robust and precise registration of oblique images based on scale-invariant feature transformation algorithm, *IEEE Geosci. Remote Sens. Lett.*, 9(4): 783-787.

[15] Q. L. Li, G. Y. Wang, J. G. Liu, and S. B. Chen (2012); Robust scale-invariant feature matching for remote sensing image registration, *IEEE Geosci. Remote Sens. Lett.*, 6(2): 287-291.

[16] Y. Lei, Y. Wang, and J. Huang (2011); Robust Image Hash in Radon Transform Domain for Authentication. *Signal Processing: Image Comm.*, 26(6): 280-288.