INT. J. BIOAUTOMATION, 2015, **19**(3), 397-408

A Novel Medical Image Watermarking in Three-dimensional Fourier Compressed Domain

Baoru Han, Jingbing Li[*], Mengxing Huang

College of Information Science and Technology
Hainan University
Haikou, Hainan, 570228, China
E-mails: 6183191@163.com, Jingbingli2008@hotmail.com, huangmx09@163.com

[*]*Corresponding author*

Received: March 13, 2015 **Accepted: September 23, 2015**

Published: September 30, 2015

Abstract: *Digital watermarking is a research hotspot in the field of image security, which is protected digital image copyright. In order to ensure medical image information security, a novel medical image digital watermarking algorithm in three-dimensional Fourier compressed domain is proposed. The novel medical image digital watermarking algorithm takes advantage of three-dimensional Fourier compressed domain characteristics, Legendre chaotic neural network encryption features and robust characteristics of differences hashing, which is a robust zero-watermarking algorithm. On one hand, the original watermarking image is encrypted in order to enhance security. It makes use of Legendre chaotic neural network implementation. On the other hand, the construction of zero-watermarking adopts differences hashing in three-dimensional Fourier compressed domain. The novel watermarking algorithm does not need to select a region of interest, can solve the problem of medical image content affected. The specific implementation of the algorithm and the experimental results are given in the paper. The simulation results testify that the novel algorithm possesses a desirable robustness to common attack and geometric attack.*

Keywords: *Medical image, Watermarking, Fourier compressed domain.*

Introduction

With the advent of the era of digital information, the rapid development of computer network and multimedia technology, major hospitals have carried out information construction. At the same time, along with the gradual development of medical information technology, the picture archiving and communication system, the electronic medical record and hospital information system are becoming more common [2, 5, 15]. Medical digital imaging technology have been widely used in medical radiology, cardiovascular imaging, and get more in-depth widely used in the department of ophthalmology, dental and other medical fields. The original film image storage method is gradually being replaced by digital medical image. The rapid progress of medical digital imaging technique and Internet technique brings convenience to remote medical treatment, remote diagnosis and academic exchange, and effectively solves the problem of uneven distribution of medical resources. Medical information can be faster and more efficient transmission over public networks. At the same time, it also faces some security issues [16, 19, 20, 24]. When the patient's medical image transmission through the network, interception and tampering with medical information has become easier. There is a risk of leakage of patient privacy. Therefore, how to ensure the safety of medical images transmitted over the Internet, the problem is also with the popularity of the network becomes increasingly severe [9, 10, 25, 26].

Medical image digital watermarking technology is a very effective way to solve this problem. The medical image digital watermarking technology was initially used for protecting copyright of digital media on the internet [1]. Now using digital watermarking invisibility and robustness characteristics, the patient information as watermarking information is hidden in medical images, in order to ensure transmission security on the Internet, and thus play a role in protecting patient privacy. In remote medical diagnosis and remote operation, the use of medical image watermark can protect the patient's privacy, and avoid the patient's information has been tampered with. Medical image digital watermarking technology as a new security measure is widely used in medical image protection [4, 6, 8]. Conventional digital watermarking algorithms are mainly applied in intellectual property protection of digital works, e-commerce transactions in the security of electronic instruments, as well as covert communications and confrontation [17]. These digital watermarking algorithms often only need to consider the effectiveness of the watermarking embedding, transparency, and in their respective application scenario effective extracting watermark information [22]. The medical image watermarking technology has advantages in addition to conventional watermarking algorithm, but is also required to meet the requirements of the characteristics of medical image strict quality [12]. At present, the research objects of medical image digital watermarking technology are most of the two-dimensional planes of the images, research on medical volume data watermarking algorithm is less [7, 14, 18]. However, most of the existing medical images are three-dimensional volume data, especially the new generation of medical devices generated, such as computed tomography imaging, magnetic resonance imaging, ultrasonic imaging and other imaging equipment. The majority of digital image generation is three-dimensional volume data.

According to the characteristics of medical volume data, a novel medical image digital watermarking algorithm in three-dimensional Fourier compressed domain is proposed. The medical image digital watermarking algorithm takes advantage of three-dimensional Fourier compressed domain characteristics and robust characteristics of differences hashing. Its security is ensured by Legendre chaotic neural network. The construction of zero-watermarking adopts differences hashing in three-dimensional Fourier compressed domain. It has fine robustness resist all sorts of attacks, which and realizes the blind extraction. The remainder of the paper is organized in this way. Legendre chaotic neural network is described in Section 2. Section 3 introduces discrete Fourier transform. Differences hashing is presented in Section 4. Section 5 gives digital watermarking algorithm. Simulations are presented in Section 6. Conclusion is given in the final section.

Legendre chaotic neural network

The watermarking information is pre processed before the watermarking embedding. There are two purposes for the watermark image scrambling. The first purpose is to reduce the degree of attention and reduce the chance of recognition. The second purpose is to increase the robustness of the watermarking image. This is the main purpose for this paper of using scrambling. The common scrambling algorithms have amold transform, transform, chaotic sequence, s magic box, the game of life [3]. The chaotic sequence for scrambling is adopted in this paper. The chaotic sequence for scrambling is produced by a new Legendre chaotic neural network in this paper. Fig. 1 shows its structure.

Definition 1

$$P_0(x)=1,\ P_n(x)=\frac{1}{2^n n!}\frac{d^n}{dx^n}\left(x^2-1\right)^n,\ n=1,\ 2,\ 3,\ ...,\ L \qquad (1)$$

$P_n(x)$ is called Legendre polynomials. Its value range in $[-1, 1]$.

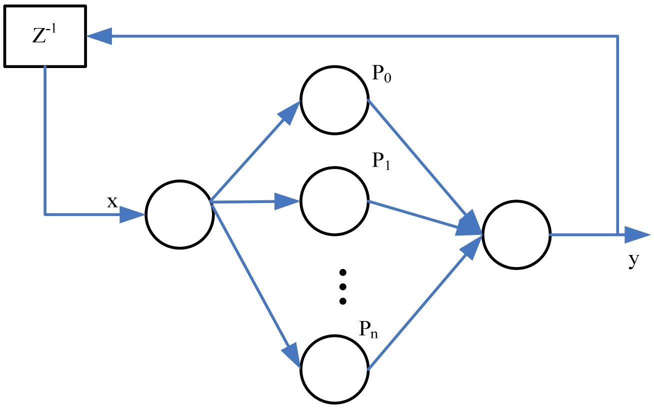


Fig. 1 Network structure

Types of contributions w_j represent the input-layer's weights. The hidden-layer's input is

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

Hidden-layer's output is a batch of Legendre orthogonal polynomial terms $P_j\left(net_j\right),\ j = 0, 1, 2, ..., n-1$. It is attained by Eq. (1) recursive. c_j represents the output-layer's weights. Its network's output is

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

$\left(T_t,\ d_t\right),\ t = 1, 2, ..., l$ represents the training sample, l represents the number of samples. Its input is $T_t = \left(x_{1t},\ x_{2t},\ ...,\ x_{mt}\right)$. Its desired output is d_t. The Network weights adjustment employ BP learning algorithm. Its formulas are given as follows:

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

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

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

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

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

where k denotes the training epochs, $t = 1, 2, ..., l$, $j = 1, 2, ..., n$.

Discrete Fourier transform

Fourier transform is the most basic method of signal analysis, which is also a very important algorithm in the field of digital signal process [11, 21]. Its basic idea is firstly put forward by the French scholar Fourier. Fourier transform is the core of Fourier analysis, through which the signal is transformed from time domain to frequency domain in which the spectrum structure and transformation patterns of signal are studied.

Fourier transform belongs to harmonic analysis. The Fourier inverse transform is easy to calculate. In view of physical effects, the physical meaning of Fourier transform is that the image gray distribution function is converted into frequency distribution function of the image, the physical meaning of Fourier inverse transformation is that frequency distribution function of the image is converted into the image gray distribution function.

One-dimensional discrete Fourier transform

If $f(x)$ satisfies Dirichlet conditions: (1) finite number of discontinuities; (2) finite number of poles; (3) absolutely integrable, where $f(x)$ is a function of x.

Then, the Fourier positive transform formula of $f(x)$ is

$$F(u)=\sum_{x=0}^{N-1} f(x)e^{-j2\pi ux/N},\ u=0,1,\ldots,N-1 \tag{9}$$

Its inverse transform formula is as follows.

$$f(x)=\frac{1}{N}\sum_{u=0}^{N-1} F(u)e^{j2\pi ux/N},\ x=0,1,\ldots,N-1 \tag{10}$$

where x is the time-domain variable; u is the frequency domain variable.

Two-dimensional discrete Fourier transform

Two-dimensional Fourier transform can be obtained from the one-dimensional Fourier transform.

If $f(x,y)$ satisfies Dirichlet conditions

$$F(u,v)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)e^{-j(2\pi/M)xu}e^{-j(2\pi/N)yv},\ u=0,1,\ldots,M-1,\ v=0,1,\ldots,N-1 \tag{11}$$

Its inverse transformation formula is

$$f(x,y)=\frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)e^{j(2\pi/M)xu}e^{j(2\pi/N)yv},\ x=0,1,\ldots,M-1,\ y=0,1,\ldots,N-1 \tag{12}$$

$F(u,v)$ is a two-dimensional discrete Fourier transforming coefficient of $f(x,y)$.

Three-dimensional discrete Fourier transform

Three-dimensional Fourier transform can be obtained from the two-dimensional Fourier transform. Its positive transform and inverse transform are given in Eqs. (13) and (14), respectively.

$$F(u,v,w)=\sum_{x=0}^{L-1}\sum_{y=0}^{M-1}\sum_{z=0}^{N-1} f(x,y,z)e^{-j\frac{2\pi x\mu}{L}}e^{-j\frac{2\pi yv}{M}}e^{-j\frac{2\pi zw}{N}} \quad (13)$$

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

$$f(x,y,z)=\frac{1}{LMN}\sum_{\mu=0}^{L-1}\sum_{\upsilon=0}^{M-1}\sum_{w=0}^{N-1} F(u,v,w)e^{j\frac{2\pi x\mu}{L}}e^{j\frac{2\pi yv}{M}}e^{j\frac{2\pi zw}{N}} \quad (14)$$

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

where $f(x,y,z)$ represents volume data value in the (x,y,z), $F(u,v,w)$ denotes the three-dimensional discrete Fourier transform coefficient.

Differences hashing

Differences hashing research originated in digital image watermarking technology. It refers to the concept and theory of multimedia authentication domain and traditional cryptography hashing. It is applied to the image retrieval and authentication, which provides the possibility for the protection of the copyright of the image. And it gradually becomes a research hotspot of image processing and image security, which has become a hot trend emerging in recent years [13, 23].

Image difference hashing techniques can transform any resolution of the image data into two to a few hundred or a few thousand binary sequences. It is a kind of perception extraction of image. For a large database of image retrieval, this means that the search time is greatly reduced, and also reduces the cost of storage media. Compared with the traditional cryptography hashing, image difference hashing is not only a data compression, and is robust for visual features. Its robustness guarantees that it can resist many kinds of attacks. Therefore, difference hashing study has important significance. Feature extraction is a key step in the difference hashing generation of perception.

Based on the traditional difference hashing algorithm, a new differences hashing algorithm in Fourier compressed domain is presented. The specific steps are as follows:

Step 1: Reduce the size in Fourier compressed domain;

Step 2: Select the transformed coefficients;

Step 3: Take real part of the coefficients;

Step 4: Build feature matrix;

Step 5: Compare value;

Step 6: Obtain hashing value.

Digital watermarking algorithm

Digital watermarking construction

Fig. 2 shows digital watermarking construction process.

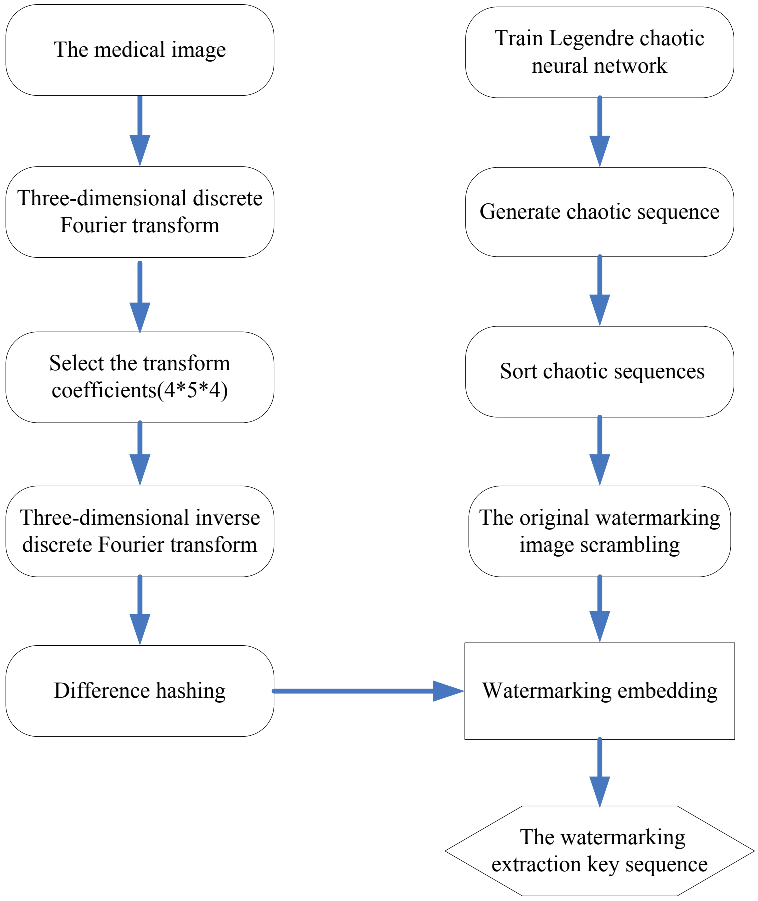


Fig. 2 Digital watermarking construction process

Digital watermarking detection

Fig. 3 shows digital watermarking detection process.

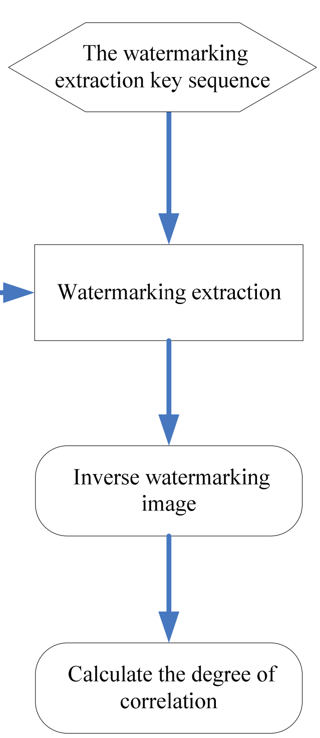


Fig. 3 Digital watermarking detection process

Simulation

The watermarking algorithm is implemented in Matlab2010a platform to test and verify its effectiveness. The Legendre chaotic neural network parameters are as follows. Its network structure adopts the 1*4*1. Its chaotic sample number is 1000. Expected error is 10^{-10}. The maximum training epoch is 2000. Fig. 4 shows the training error curve. Fig. 5 displays the chaotic sequence for scrambling. Fig. 6 gives its autocorrelation. The original watermarking image and scrambled watermarking image are given as Fig. 7 (a) and (b), respectively.

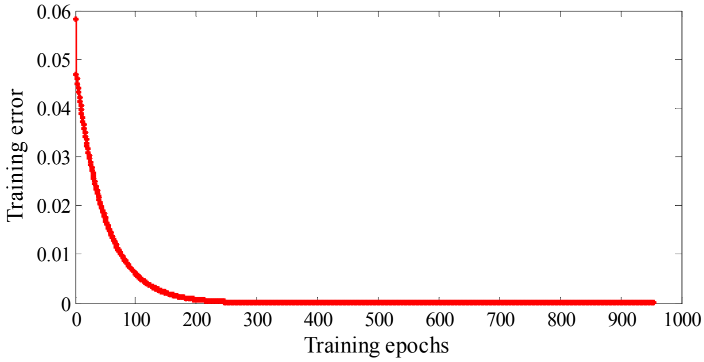


Fig. 4 Training error curve

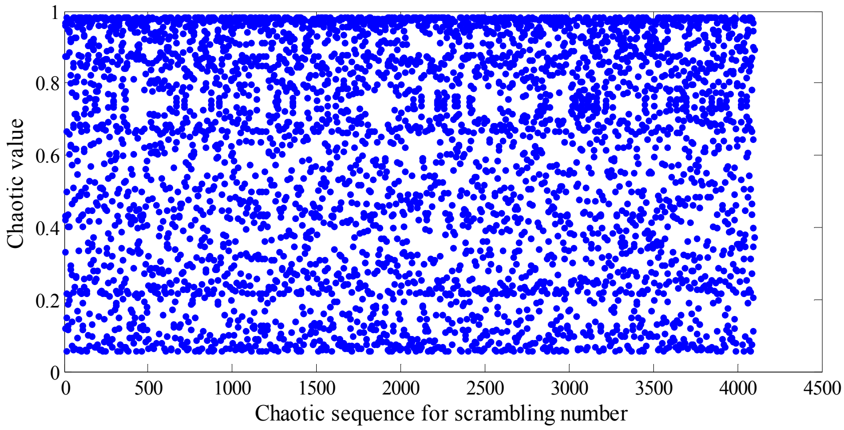


Fig. 5 Chaotic sequence for scrambling

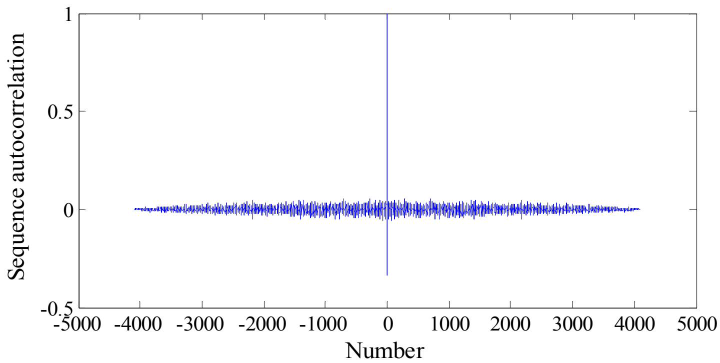


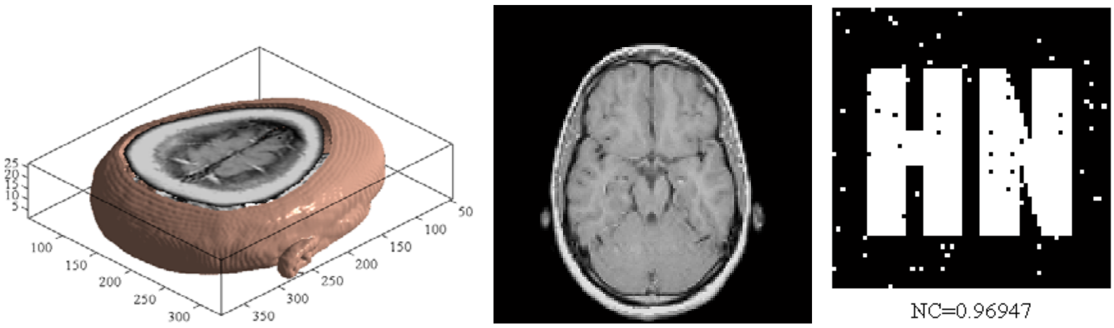
Fig. 6 The chaotic sequence for scrambling autocorrelation

(a) (b)

Fig. 7 The watermarking image

Zooming attack

Medical image is zoomed in 3. The Fig. 8 offers the corresponding simulation results. Fig. 8(a) shows volume data of medical image. Fig. 8(b) gives medical image's slice. As it can be seen from Fig. 8(c), the degree of correlation is 0.96947. This shows that the algorithm is robust against zoom attacks.

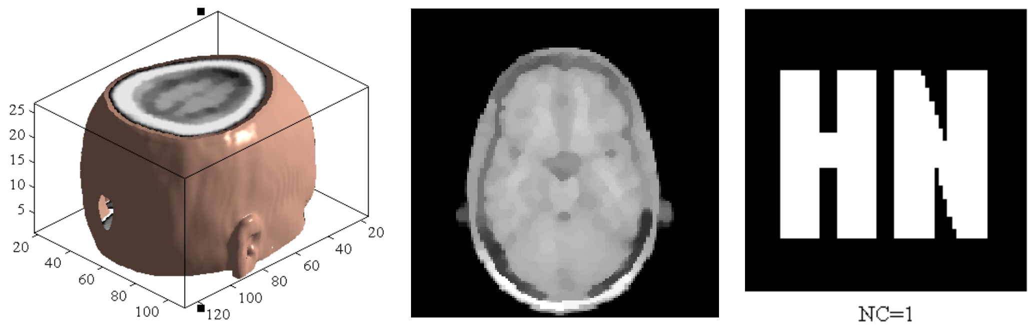


(a) (b) (c)

Fig. 8 Simulation results under zooming attack

Filtering attack

Medical image is filtered attack. Using [3*3] median filter, repeat 25 times, Fig. 9 provides the corresponding simulation results. Then, the degree of correlation is 1. From the Fig. 9, it can be found that the extracted watermarking is still legible. Therefore the watermarking algorithm has favorable robustness resist filtering attack.

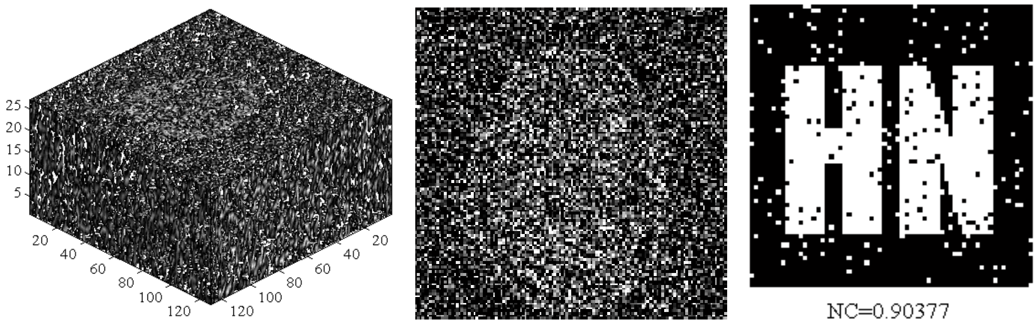


(a) (b) (c)

Fig. 9 Simulation results under filtering attack

Gaussian noise attack

Gauss noise intensity coefficient is measured the added noise interference size in medical image. When the noise intensity is 25%, the corresponding simulation results are as shown in the Fig. 10. This shows that the algorithm has strong robustness against Gauss noise attacks.

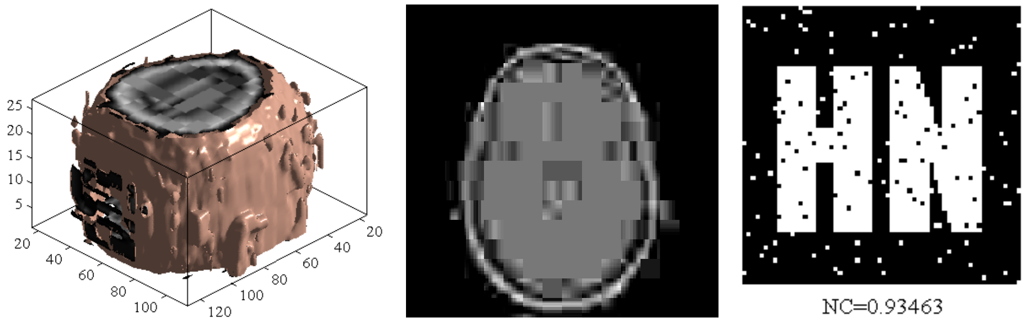


(a) (b) (c)

Fig. 10 Simulation results under Gaussian noise attack

JPEG compression attack

At present, most of the images are full JPEG format. So anti-JPEG compression attack is an important standard to measure the stability of a kind of image information. When the compression quality percentage is 6%, Fig. 11 shows the corresponding simulation results. The extracted watermarking image is very clear. So the algorithm can effectively resist JPEG compression attack.



(a) (b) (c)

Fig. 11 Simulation results under JPEG compression attack

Right shift attack

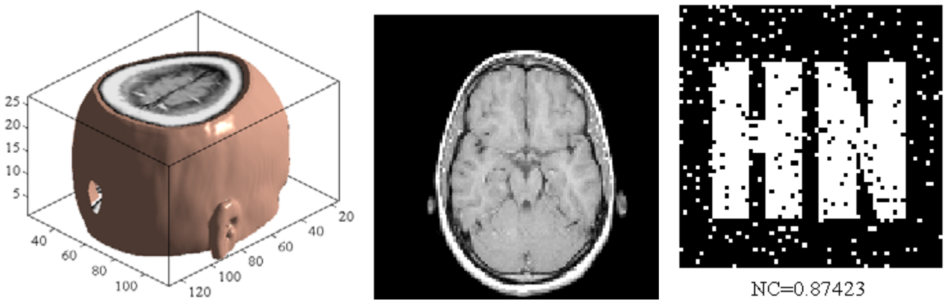
Medical image is attacked with right shifted 4%. Fig. 12 gives the corresponding simulation results. This illustrates that the watermarking algorithm is provided with good robustness against upward shift attack capability.

Anti-clockwise rotation attack

Medical image is attacked by anti-clockwise rotation. The anti-clockwise degree is 20. In the Fig. 13, the degree of correlation is 0.96781. Simulation results show that the algorithm has fine ability against anti-clockwise rotation attack.

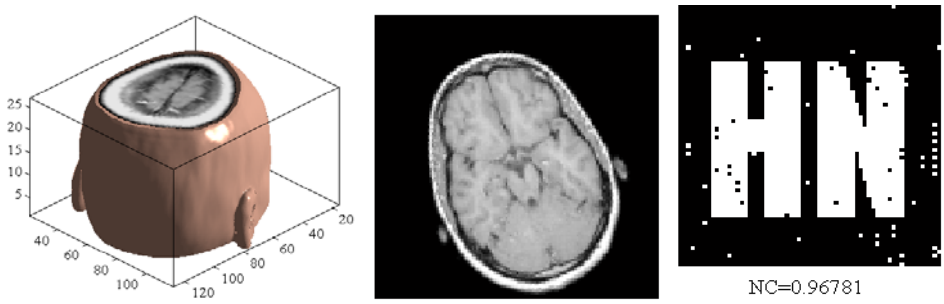
Shear attack

Medical image is sheared about 14% in the *z*-axis direction. The sheared medical image is given in Fig. 14 (a) and (b). The watermarking detection is shown in the Fig. 14 (c), the degree of correlation is 0.96649. Simulation results certificate that the algorithm has strong robustness against shear attack in the *z*-axis direction.



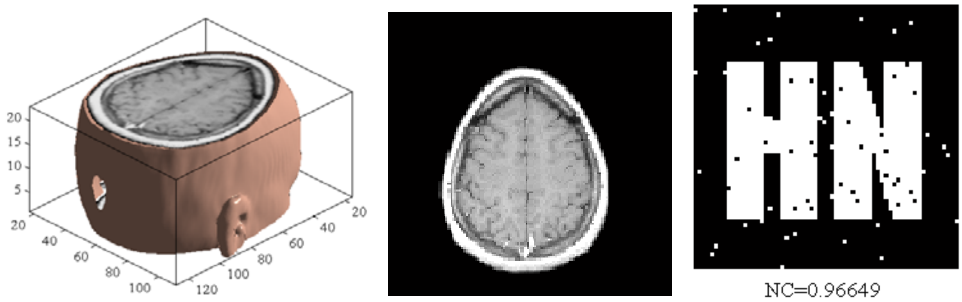
(a) (b) (c)

Fig. 12 Simulation results under right shift attack



(a) (b) (c)

Fig. 13 Simulation results under anti-clockwise rotation attack



(a) (b) (c)

Fig. 14 Simulation results under anti-shear attack

Conclusion

Due to the special nature of medical image, taking into account the patient's privacy issues, a new medical image digital watermarking algorithm is proposed, which adopts differences hashing in Fourier compressed domain to construct zero-watermarking. Without changing the original premise of medical image, the medical image watermarking algorithm has invisibility. Legendre chaotic neural network can protects the watermarking image containing patient information, which enhances the watermarking algorithm security. Simulation results confirm that the algorithm was better robustness and security, which can protect the medical image.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 61263033), the International Science and Technology Cooperation Project of Hainan (No. KJHZ2015-4), the Higher School Outstanding Young Backbone Teachers Funded Project of Hainan Province (No. 2014-129), the International Science and Technology Cooperation Project of Hainan Province (No. KJHZ2014-16) and the Higher School Scientific Research Project of Hainan Province (No. Hnky2015-80).

References

1. Barnett R. (1999). Digital Watermarking: Applications, Techniques and Challenges, Electronics & Communication Engineering Journal, 11(4), 173-183.
2. Chao H.-M., C.-M. Hsu, S.-G. Miaou (2002). A Data-hiding Technique with Authentication, Integration, and Confidentiality for Electronic Patient Records, IEEE Transactions on Information Technology in Biomedicine, 6(1), 46-53.
3. Cheng N. (2012). Algorithm for Image Encryption Based on Chaotic Maps, J Converg Inf Technol, 7, 493-500.
4. Deng X. H., Z. G. Chen, X. H. Deng (2011). A Novel Dual-layer Reversible Watermarking for Medical Image Authentication and Electronic Patient Record Hiding, Advanced Science Letters, 4(11-12), 3678-3684(7).
5. Giakoumaki A., S. Pavlopoulos, D. Koutsouris (2006). Multiple Image Watermarking Applied to Health Information Management, IEEE Transactions on Information Technology in Biomedicine A, 10(4), 722-732.
6. Gunjal B. L., R. R. Manthalkar (2010). An Overview Transform Domain Robust Digital Image Watermarking Algorithms, Journal of Emerging Trends in Computing and Information Sciences, 2(1), 37-42.
7. Han B., J. Li (2013). A Robust Watermarking Algorithm for Medical Volume Data Based on Hermite Chaotic Neural Network, International Journal of Applied Mathematics and Statistics, 48(18), 128-135.
8. Han B., J. Li, L. Zong (2013). A New Robust Zero-watermarking Algorithm for Medical Volume Data, International Journal of Signal Processing, Image Processing and Pattern Recognition, 6(6), 245-358.
9. Hsu C.-T., J. L. Wu (1999). Hidden Digital Watermarks in Images, IEEE Trans on Image Processing, 8(1), 58-68.
10. Kim J., N. Kim, D. Lee, S. Park, S. Lee (2010). Watermarking Two Dimensional Data Object Identifier for Authenticated Distribution of Digital Multimedia Contents, Signal Processing: Image Communication, 25(8), 559-576.
11. Kitamura I., S. Kanai, T. Kishinami (2001). Copyright Protection of Vector Map Using Digital Watermarking Method Based on Discrete Fourier Transform, IEEE International Geoscience and Remote Sensing Symposium, 3, 1191-1193.
12. Lavanya A., V. Natarajan (2012). Watermarking Patient Data in Encrypted Medical Images, Sadhana − Academy Proceedings in Engineering Sciences, 37(6), 723-729.
13. Lei Y., Y. Wang, J. Huang (2011). Robust Image Hash in Radon Transform Domain for Authentication, Signal Processing: Image Communication, 26(6), 280-288.
14. Liu C., M. Wang (2014). A Zero-watermarking Algorithm Resisting JPEG Compression on Images, Microcomputer & Its Applications, 33(14), 32-35.
15. Lu C.-S., H.-Y. M. Liao (2001).Multipurpose Watermarking for Image Authentication and Protection, IEEE Transactions on Image Processing, 10(10), 1579-1592.
16. Panduranga H. T., N. Kumar, S. K. Kiran (2014). Image Encryption Based on Permutation-Substitution Using Chaotic Map and Latin Square Image Cipher, The European Physical Journal Special Topics, 223(8), 1663-1677.
17. Podilchuk C. I., E. J. Delp (2001). Digital Watermarking: Algorithm and Application, IEEE Signal Processing Magazine, 18(4), 33-46.
18. Qu C., D. Wang (2014). Robust Zero Watermarking Algorithm Based on Bit Plane Theory and Singular Value Decomposition, Journal of Computer Applications, 33(14), 3462-3465.
19. Tan C. K., J. C. Ng, X. T. Xu (2011). Security Protection of DICOM Medical Images Using Dual-layer Reversible Watermarking with Tamper Detection Capability, Journal of Digital Imaging, 24(3), 528-540.

20. Tu J.-H. (2014). A Novel Building Boundary Extraction Method for High Resolution Aerial Image, Review of Computer Engineer Studies, 1(2), 19-22.
21. Wang Q., Q. Guo, L. Lei (2013). Double Image Encryption Based on Phase-amplitude Hybrid Encoding and Iterative Phase Encoding in Fractional Fourier Transform Domains, Optik – Int J for Light Electron Optics, 124(22), 5496-5502.
22. Weng S., S. C. Chu, N. Cai, R. Zhan (2013). Invariability of Mean Value Based Reversible Watermarking, Journal of Information Hiding and Multimedia Signal Processing, 4(2), 90-98.
23. Winter C., M. Steinebach, Y. Yanniko (2014). Fast Indexing Strategies for Robust Image Hashes, Digital Investigation, 11(1), S27-S35.
24. Zhang S., T. Gao, L. Gao (2014). A Novel Encryption Frame for Medical Image with Watermark Based on Hyper Chaotic System, Mathematical Problems in Engineering, 2014, http://dx.doi.org/10.1155/2014/240749.
25. Zhang X. (2011). Reversible Data Hiding in Encrypted Image, IEEE Signal Processing Letters, 18(4), 255-258.
26. Zhang X. (2012). Separable Reversible Data Hiding in Encrypted Image, IEEE Transactions on Information Forensics and Security, 7(2), 826-832.

Baoru Han, Ph.D. Student
E-mail: 6183191@163.com

Baoru Han received his M.Sc. in Circuits and Systems from Yanshan University of China in 2007. He is currently a Ph.D. Student in Information and Communication Engineering at Hainan University of China. His major research interests include digital watermarking, neural network and image processing.

Prof. Jingbing Li, Ph.D.
E-mail: Jingbingli2008@hotmail.com

Jingbing Li received his M.Sc. in Automation from Beijing Institute of Technology of China in 1996. He received the Ph.D. degree in Control Theory and Engineering from Chongqing University of China in 2007. His main fields of scientific interest are digital watermarking and image processing.

Prof. Mengxing Huang, Ph.D.
E-mail: huangmx09@163.com

Mengxing Huang received the Ph.D. degree in Systems Engineering from Northwestern Polytechnical University of China in 2007. His main fields of scientific interest are wisdom health, wisdom travel and intelligent information processing.