BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **16**, No 2
Sofia • 2016 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.1515/cait-2016-0026

A New Zero-Watermarking Algorithm Resisting Attacks Based on Differences Hashing

Baoru Han[1,2], *Jingbing Li*[1]

[1] *College of Information Science and Technology, Hainan University, Haikou, 570228 China*
[2] *Hainan Software Profession Institute, Qionghai, 571400 China*
Emails: 6183191@163.com Jingbingli2008@hotmail.com

Abstract: *Medical volume data containing patient information is often faced with various attacks in the transmission process. In order to enhance the medical information system security, and effectively solve the problem of medical volume data protection, a new zero-watermarking algorithm is proposed in the paper. The new zero-watermarking algorithm takes advantage of three-dimensional discrete wavelet transform multi-resolution analysis characteristics of space and time, three-dimensional discrete cosine transform properties, and differences hashing robust characteristic. In order to enhance watermarking algorithm security, Legendre chaotic neural network is used for scrambling original watermark image. The medical volume data is made by three-dimensional discrete wavelet transform, three-dimensional discrete cosine transform and three-dimensional discrete inverse cosine transform r to obtain the medical volume data feature matrix* ($4\times5\times4$)*, which is converted to 64-bit binary feature sequence through difference hashing algorithm. The 64-bit binary feature sequence is used to construct the zero-watermarking. The experimental results prove that the new zero-watermarking has favorable security and robustness resisting various attacks. Therefore, the new zero-watermarking algorithm is more applicable to protect medical volume data.*

Keywords: *Zero-watermarking algorithm, scrambling, medical volume data, three-dimensional discrete inverse cosine transform, difference hashing.*

1. Introduction

The multimedia communication has become the important means of information exchange between people. People communicate all kinds of information through the network [1, 2]. The digital information and network have become an important part of people's life. With the development of network technologies, especially the widely used of the Internet, as well as the establishment and implementation of personal communications, information exchange has become increasingly convenient.

Unfortunately, more and more serious security problem are exposed [3]. Although the security problem of image information covers a lot more in a broad sense, it is extremely critical to ensure the integrity and confidentiality of the image information [4, 5].

Nowadays, with the development of information technology, image has become one of human beings' most important information carriers. In the field of medical, with the increasing maturity of medical imaging technology, great deals of medical images are provided by a variety of medical equipments [6]. The transmission of digital medical image information is promoted with the development of medical digital imaging communication standards. However, in an open network environment, medical images and data information through network transmission will also be confronted with more security issues [7, 8]. The patient's private information can easily be intercepted and leaked. Digital medical image information can easily be altered or forged, for which Security of medical image and data information must be protected. A good solution to the security problem is provided by digital watermarking technology.

Digital technology and the protection of copyright are growing fast in recent years. Digital watermarking has become an important means of copyright protection and integrity testing, which is widely used in protection of digital image, intellectual property protection of digital work and other applications [9-11]. Digital watermarking algorithm has many classification methods. According to the most important features of the current digital watermarking algorithm, digital watermarking algorithm is divided into watermarking algorithm in space/time domain, watermarking algorithm in frequency domain, compressed domain watermarking algorithm in compressed domain, watermarking algorithm based on statistics and watermarking algorithm based on physiological models. According to watermarking embedding digital media of different space, digital watermarking algorithms are classified into watermarking algorithm in spatial domain and watermarking algorithm in transform domain. Under the premise of the image quality assurance, watermarking algorithm in transform domain can enhance the robustness of data hiding. Therefore the watermarking algorithm in transform domain is better than that the watermarking algorithm in spatial domain. The watermarking algorithm in transform domain has become a research focus in current watermarking algorithms. Invisible robust watermark is mainly used for image copyright protection. The spatial information or transform domain information of the image is usually made with certain changes to embed into watermarking [12, 13]. The watermarking imperceptibility and robustness is always a pair of conflicting constraints. In view of this problem, [14] is of great value to put forward the concept of zero-watermarking. The zero-watermarking is the use of the important features of image itself to construct watermarking information. But the image did not make any change. Its theoretical basis is that each image has a different feature. Thus, each image with watermark information is different from the other image. After the concept of the zero-watermarking is put forward, all relevant scholars pay close attention to it, and are committed to zero-watermarking to do a lot of research work [15, 16]. At the same time, many of the new algorithms are proposed [17, 18].

The emergence of zero-watermarking is an effective complement to traditional medical image encryption technology. After being attacked, zero-watermarking can still be complete and reliable to extract the watermarking. Its unique robustness and security can better protect medical image information. Based on the zero-watermarking, a new zero-watermarking algorithm resisting attacks is proposed. The new zero-watermarking algorithm is based on three-dimensional discrete wavelet transform, three-dimensional discrete cosine transform, three-dimensional discrete inverse cosine transform and differences hashing, which use the Legendre chaotic neural networks to scramble the original watermarking image. It uses difference hashing algorithm to construct the watermarking extraction key sequence, which can resist most attacks with better robustness, and realizes the blind detection. At the same time, the new zero-watermarking is very safe and difficult to crack.

The rest of the paper is organized as follows: Section 2 introduces the Legendre chaotic neural network. In Section 3 the three-dimensional discrete wavelet transform is described. In Section 4 the three-dimensional discrete cosine transform and three-dimensional discrete inverse cosine transform are depicted. Section 5 proposes the novel differences hashing algorithm. A zero-watermarking algorithm resisting attacks is proposed in Section 6. Section 7 proposes experiments and analysis. At the end, Section 8 draws conclusion.

2. Legendre chaotic neural network

The paper selects a novel Legendre chaotic neural network. Fig. 1 shows its model.

Definition 1.

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

The Legendre polynomials are $P_n(x)$, which are functions $\rho(x)=1$'s n-orthogonal polynomials. Its range is in the space domain [–1, 1].

Set w_j and c_j are network weights. The Legendre orthogonal polynomials are as hidden layer neuron's activation function. Its input of hidden layer neuron is

$$\text{net}_j = w_j x,\ \ j=0,1,2,L,n. \tag{2}$$

A series of Legendre orthogonal polynomial terms $P_j\left(\text{net}_j\right),\ j=0,1,2,\cdots,n-1$ are output of hidden layer neurons. It is recursion of formula (1). Output of Legendre chaotic neural network is

$$y=\sum_{j=0}^{n} c_j P_j\left(\text{net}_j\right). \tag{3}$$

Set $\left(T_t, d_t\right),\ t=1,2,\cdots,l,$ are the networks training samples. The samples number is l. $T_t=\left(x_{1t}, x_{2t},\cdots, x_{mt}\right)$ is the input of neural network; d_t are the desired outputs of neural network. BP learning algorithm is adopted to adjust network weights.

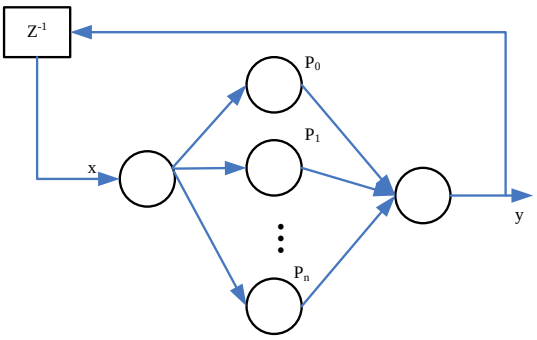


Fig. 1. Legendre chaotic neural network model

Error formula is as follows:

(4) $$e_t = d_t - y_t,$$

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

adjustments w_j and c_j are

(6) $$\Delta c_j = -\eta \frac{\partial E}{\partial c_j} = \eta e_t P_j(\text{net}_j),$$

(7) $$\Delta w_j = -\eta \frac{\partial E}{\partial w_j} = \eta e_t c_j P_j'(\text{net}_j) x_j,$$

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

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

In this paper, the chosen network architecture is 1×3×1. The logistic chaotic function is adopted to generate training samples.

3. Three-dimensional discrete wavelet transform

One of the important methods in signal processing is wavelet transform, which is proposed in 1988. There is a new signal analysis theory rising in recent years [19, 20]. It is a time – frequency analysis method, whose basic idea is to decompose signals based on wavelet function. The local signal is subjected to frequency transformation by wavelet transform. So, it can be used to analyse the local signal more effectively. The wavelet transform is adapted to the new JPEG2000 image compression and video compression standard MPE-4. Therefore, zero-watermarking is constructed using wavelet transform and has a good compatibility with the new image and video compression standard.

Two-dimensional wavelet transform is extended to three-dimensional wavelet transform. The fine multi-resolution analysis features for three-dimensional image are offered by three-dimensional wavelet transform. The three-dimensional digital images are multi resolution decomposed by wavelet transform, which is further

decomposed into different space and different frequency sub-image. Fig. 2 shows decomposition process of three-dimensional wavelet. This paper uses three-dimensional discrete wavelet transform to transform medical volume data in order to obtain the low-frequency sub-band transform coefficients. The original medical volume data is shown in Fig. 3 and is the Matlab2010a's own medical volume data. Fig. 4 shows three-dimensional discrete wavelet transform for the original medical volume data.

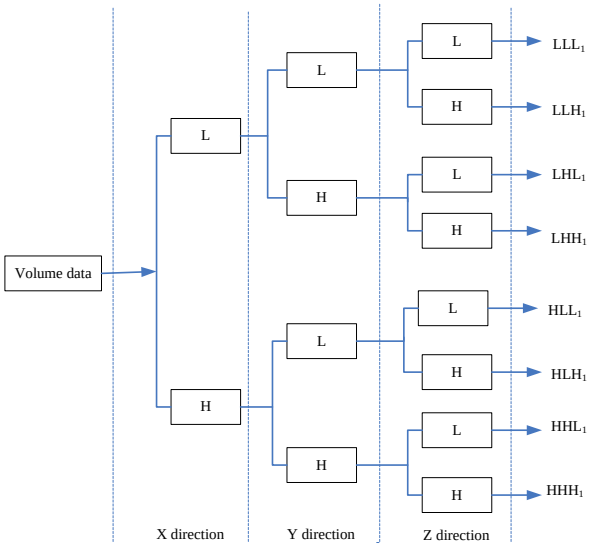


Fig. 2. A layer decomposition process for three-dimensional wavelet

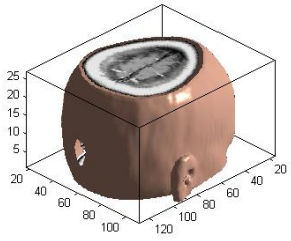


Fig. 3.The original medical volume data

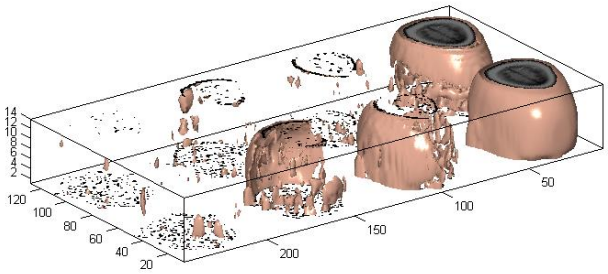


Fig. 4. Three-dimensional discrete wavelet transform for medical volume data

4. Three-dimensional discrete cosine transform

The three-dimensional discrete cosine transform formula is as follows:

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

In the formula,

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

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

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

Its inverse transform formula is as follows:

$$f(x,y,z)=\left[\sum_{\mu=0}^{M-1}\sum_{\upsilon=0}^{N-1}\sum_{\varpi=0}^{P-1}c(u)c(v)c(\omega)F(u,v,w)\times\right.$$
$$\left.\times\cos\frac{(2x+1)u\pi}{2M}\cos\frac{(2y+1)v\pi}{2N}\cos\frac{(2z+1)\omega\pi}{2P}\right], \tag{13}$$
$$x=0,1,\cdots,M-1;\quad y=0,1,\cdots,N-1;\quad z=0,1,\cdots,P-1.$$

Three-dimensional discrete cosine transform for the wavelet low-frequency sub-band transform coefficients is shown in Fig. 5.

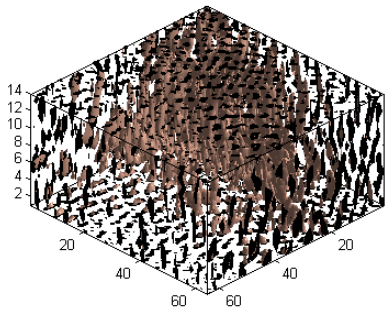


Fig. 5. Three-dimensional discrete cosine transform for the wavelet low-frequency sub-band transform coefficients

5. The novel difference hashing

Perceptual hashing is a brief summary, which is generated by a compressed multimedia object of perceptual features. Difference hashing provides effective support for multimedia content and copyright protection, which are widely used in

the field of content authentication and database searches. Thanks to these advantages, difference hashing has perceptual characteristics.

The paper first analyzes the basic differences hashing algorithm. The novel differences hashing algorithm is proposed based on the multiple transform domain. It has high robustness and can achieve both resisting conventional attacks and resisting geometric attacks. The novel differences hashing algorithm's flow is depicted in Fig. 6. The specific steps are as follows:

Step 1. Reduce the size in multiple transform domains.
Step 2. Select the transformed coefficients (4×5×4).
Step 3. Build feature matrix.
Step 4. Calculate the difference value.
Step 5. Obtain hashing value.

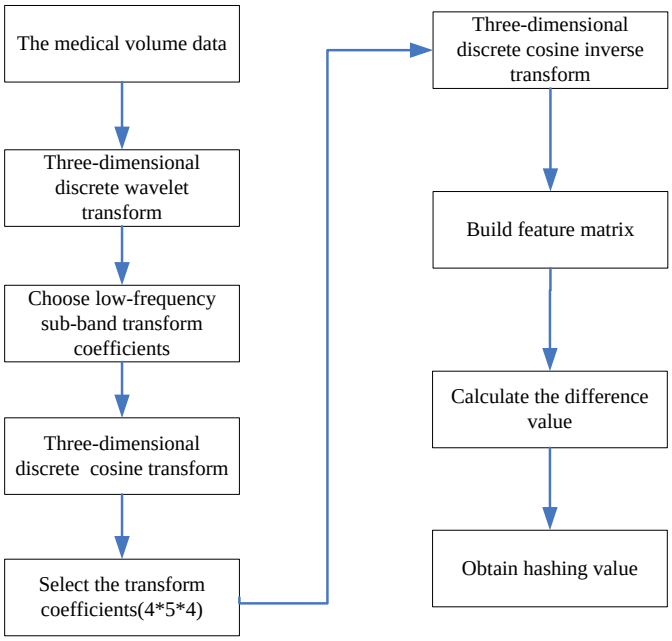


Fig. 6. The novel differences hashing algorithm's flow

6. Zero-watermarking algorithm

The new zero-watermarking algorithm mainly consists of the watermarking embedding process and extraction process.

6.1. Watermarking embedding algorithm

Step 1. Three-dimensional medical volume data could be processed by three-dimensional discrete wavelet transform and three-dimensional discrete cosine transform; selecting some coefficients (4×5×4) of the transform.

Step 2. The selected coefficients (4×5×4) are transformed by three-dimensional discrete cosine inverse transform.

Step 3. The feature sequence is obtained by the novel differences hashing algorithm.

Step 4. Legendre chaotic neural network generates appropriate length of the chaotic sequence for scrambling the original watermarking image.

Step 5. The HASH function is used to generate the watermarking extraction key sequence through the XOR operation.

The zero-watermarking embedding process is shown on Fig. 7.

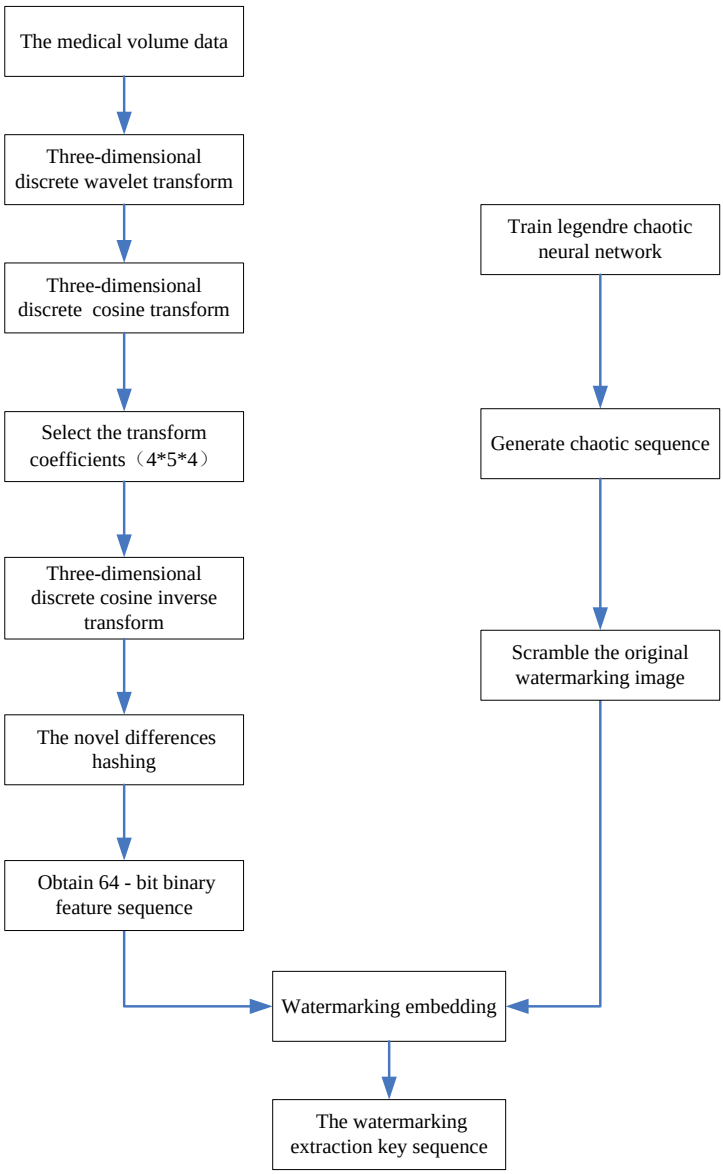


Fig. 7. The zero-watermarking embedding process

6.2. Watermarking extraction algorithm

The steps are four.

Step 1. The tested medical volume data is processed with the same method in order to get the tested medical volume data feature sequence.

Step 2. The tested medical image feature sequence and the watermarking extraction key sequences are XORed, which can get the scrambled image watermarking image.

Step 3. The scrambled watermarking image is done by Legendre chaotic neural network inverse scrambling, which can get the tested medical image's watermarking image.

Step 4. Correlation degree is calculated to judge a watermarking embedding.

The zero-watermarking extraction process is shown on Fig. 8.

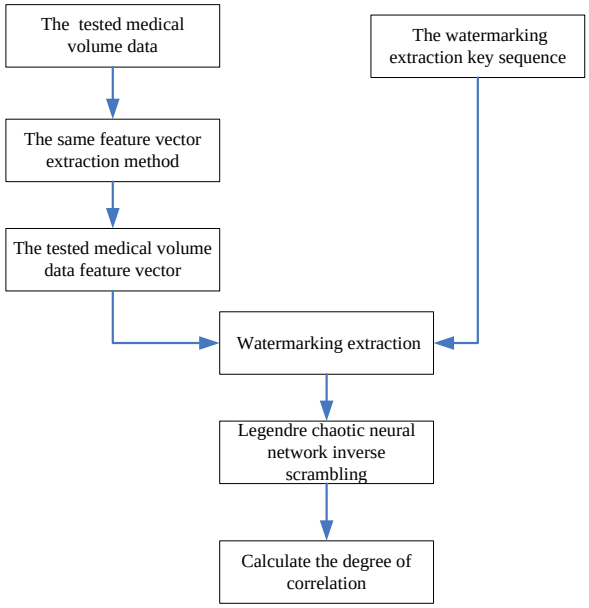


Fig. 8. The zero-watermarking extraction process

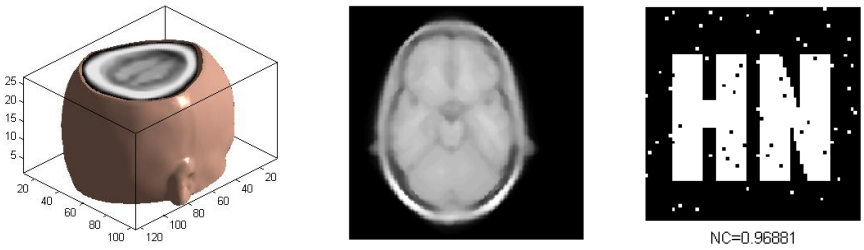
7. Experiments

The experimental platform is Matlab2010a. The robustness of the new zero-watermarking algorithm is validated by filtering attack, JPEG compression attack, zooming attack, upward shift attack and shear attack. The specific attack simulations are shown as follows.

7.1. Filtering attack

The medical volume data is filtered by [2×2] median filter, which is repeated 15 times. Fig. 9 shows the corresponding medical volume data, the slice image and the

extracted watermarking image. The degree of correlation is 0.96881, which indicates that the watermarking algorithm has good resisting median filter ability.

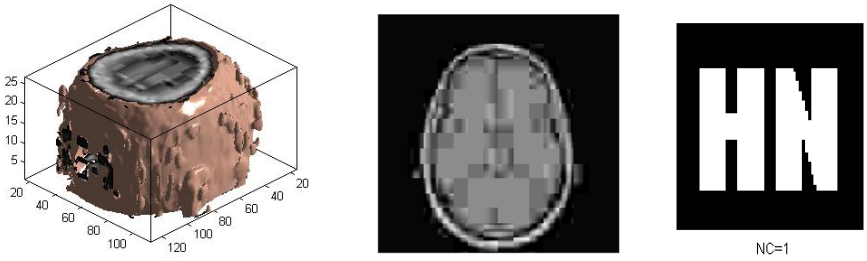


(a) (b) (c)

Fig. 9. Experiments under [2×2] median filtering attack

7.2. JPEG compression attack

JPEG compression attack capability is determined by compression quality percentage. The compression factor is smaller that image quality is worse. Fig. 10 shows the experimental results when the compression is 8%. The degree of correlation is 1, which indicates that the watermarking algorithm holds good resisting JPEG compression capability.

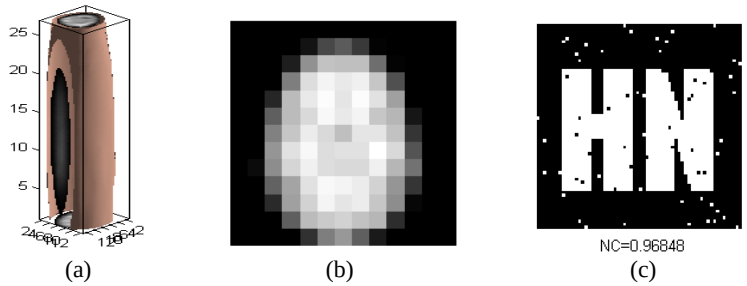


(a) (b) (c)

Fig. 10. Experiments under JPEG compression attack

7.3. Zooming attack

The medical volume data is zoomed and its zooming factor is 0.1. Fig. 11 shows the corresponding medical volume data, the slice image and the extracted watermarking image. The degree of correlation is very high. This shows that the watermarking algorithm is robust against zoom attacks.

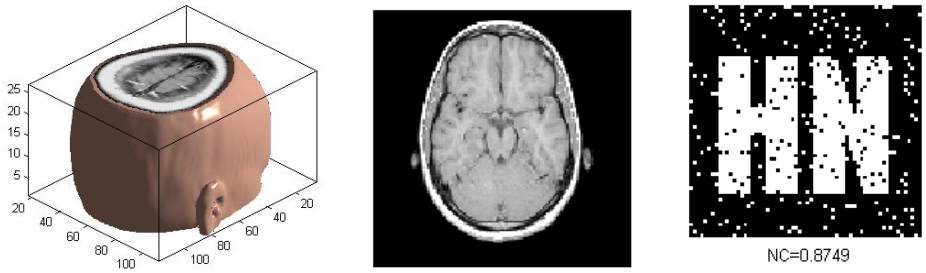


(a) (b) (c)

Fig.11. Experiments under zooming attack

7.4. Upward shift attack

Medical volume data is upward shifted with 8%. The corresponding experimental results are as shown on the Fig. 12. In this case, the degree of correlation is 0.8749. So the watermarking algorithm can be provided with a better capability against upward shift attack.

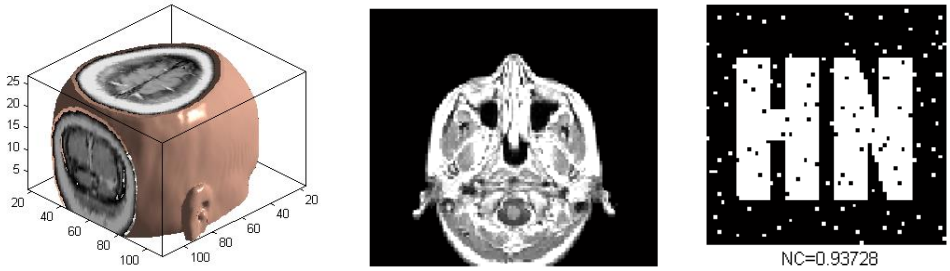


(a) (b) (c)

Fig. 12. Experiments under upward shift attack

7.5. Shear attack

In the *Y*-axis direction, shear the medical volume data about 10%, the medical volume has a part missing data. Fig. 13 shows the corresponding medical volume data, the slice image and the extracted watermarking image. As it is seen from Fig. 13, the watermarking can be accurately extracted. So the watermarking algorithm has a fine resisting shear capability.



(a) (b) (c)

Fig. 13. Experiments under shear attack

8. Discussion

In [21] is present a region-based algorithm based on multiple watermarking in the frequency and spatial domains. In [22] is present a zero-watermarking scheme implemented in the composite Contoured Transform-Singular Value Decomposition (SVD) domain for unambiguous authentication of medical images. It can be seen from Table 1 that the proposed watermarking algorithm is applied to the 3D medical volume data. In [21, 22] are applied to the 2D medical images, but the medical images produced by the existing medical equipment are mostly 3D medical volume data. So, the proposed watermarking algorithm is very practical.

The robust watermarking algorithm of the study and those proposed in [21, 22] are applicable to medical images. The specificity of medical data is that the embedded watermarking can not affect the doctor's diagnosis, cannot significantly change the contents of medical data, especially can not to change the interest area of medical data. The embedded watermarking of the [21] can change the contents of medical volume data and could affect medical diagnosis. The proposed watermarking algorithm and the ones suggested in [22] are zero-watermarking algorithms. These embedded watermarking can not influence the quality of the original medical image and will not influence the doctor's diagnosis. Compared with the [22] algorithms, the original watermarking image scrambling of the watermarking algorithm proposed here adopts the Legendre chaotic neural network, which greatly enhances the security of the watermarking. In short, the watermarking for medical volume data proposed in this study has the ideal anti-attack capability.

Table 1. Comparison of the proposed algorithm with the MIW algorithms given in [21, 22]

Algorithm	Object	Medical image content	Embedding technique	Blind	Robustness	Scrambling
[21]	2D image	Change	Frequency and spatial domains	Yes	Yes	No
[22]	2D image	Unchanged	Zero-watermarking	Yes	Yes	Arnold
The proposed algorithm	3D volumes	Unchanged	Zero-watermarking	Yes	Yes	Legendre chaotic neural network

9. Conclusion

For security protection of medical volume data watermark information, a new zero-watermarking algorithm resisting conventional attacks and geometric attacks is proposed. The new algorithm uses the multiple transform domain and differences hashing algorithm to construct the watermarking extraction key sequence. It realizes zero-watermarking embedding and blind watermarking extraction. The watermarking can be extracted without the original medical volume data. The new zero-watermarking algorithm security can be enhanced by Legendre chaotic neural network. Therefore, the new zero-watermarking algorithm is theoretically absolutely secure. Experimental results indicate that the new zero-watermarking algorithm has excellent robustness against conventional attacks and geometric attacks, which would play an important role in medical volume data protection. In addition, it can also be used for three-dimensional data protection and authentication watermarking information in other fields.

***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 KJHZ2015-04), the Higher School Outstanding Young Backbone Teachers Funded Project of Hainan Province (No 2014-129) and the Institutions of Higher Learning Scientific Research Special Project of Hainan Province (Hnkyzx2014-2).

References

1. Giakoumaki, A., S. Pavlopoulos, D. Koutsouris. Multiple Image Watermarking Applied to Health Information Management. – Information Technology in Biomedicine, IEEE Transactions on, Vol. **10**, 2006, No 4, pp. 722-732.
2. Preda, R. O., D. N. Vizireanu. A Robust Digital Watermarking Scheme for Video Copyright Protection in the Wavelet Domain. – Measurement, Vol. **43**, 2010, No 10, pp. 1720-1726.
3. Panduranga, H. T., S. K. Naveen Kumar, Kiran. Image Encryption Based on Permutation-Substitution Using Chaotic Map and Latin Square Image Cipher. – The European Physical Journal Special Topics, Vol. **223**, 2014, No 8, pp. 1663-1677.
4. Deng, X., Z. Chen, F. Zeng, Y. Zhang, Y. Mao. Authentication and Recovery of Medical Diagnostic Image Using Dual Reversible Digital Watermarking. – Journal of Nanoscience and Nanotechnology, Vol. **13**, 2013, No 3, pp. 2099-2107.
5. Deng, X. H., Z. G. Chen, X. H. Deng et al. A Novel Dual-Layer Reversible Watermarking for Medical Image Authentication and EPR Hiding. – Advanced Science Letters, Vol. **4**, 2011, No 11, pp. 3678-3684.
6. Tan, C. K., J. C. Ng, X. Xu, C. L. Poh, Y. L. Guan, K. Sheah. Security Protection of DICOM Medical Images Using Dual Layer Reversible Watermarking with Tamper Detection Capability. – Journal of Digital Imaging, Vol. **24**, 2011, No 3, pp. 528-540.
7. Memon, N. A., A. Chaudhry, M. Ahmad, Z. A. Keerio. Hybrid Watermarking of Medical Images for ROI Authentication and Recovery. – International Journal of Computer Mathematics, Vol. **88**, 2011, No 10, pp. 2057-2071.
8. Han, B., J. Li, L. Zong. A New Robust Zero-Watermarking Algorithm for Medical Volume Data. – International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. **6**, 2013, No 6, pp. 245-258.
9. Run, R. S., S. J. Horng, J. L. Lai. An Improved SVD Based Watermarking Technique for Copyright Protection. – Expert Systems with Applications, Vol. **39**, 2012, No 1, pp. 673-689.
10. Seo, J. S., C. D. Yoo. Localized Image Watermarking Based on Feature Points of Scale-Space Representation. – Pattern Recognition, Vol. **37**, 2004, No 7, pp. 1365-1375.
11. Han, B., J. Li. A Robust Watermarking Algorithm for Medical Volume Data Based on Hermite Chaotic Neural Network. – International Journal of Applied Mathematics and Statistics, Vol. **48**, 2013, No 18, pp. 128-135.
12. Li, L., H. H. Xu, C. C. Chang, Y. Y. Ma. A Novel Image Watermarking in Redistributed Invariant Wavelet Domain. – Journal of Systems and Software, Vol. **84**, 2011, No 6, pp. 923-929.
13. He, Z., W. Lu, W. Sun, J. Huang. Digital Image Splicing Detection Based on Markov Features in DCT and DWT Domain. – Pattern Recognition, Vol. **45**, 2012, No 12, pp. 4292-4299.
14. Wen, Q., T. Sun, S. Wang. Concept and Application of Zero-Watermark. – Acta Electronica Sinica, Vol. **431**, 2003, No 2, pp. 214-216.
15. Wang, X., Y. Zhan. Robust Zero Watermarking Scheme for 3D Point Model. – Computer Engineering and Applications, Vol. **47**, 2011, No 28, pp. 7-11.
16. Hamadou, A., X. M. Sun, L. Y. Gao, S. A. Shah. A Fragile Zero-Watermarking Technique for Authentication of Relational Databases. – International Journal of Digital Content Technology and Its Applications, Vol. **5**, 2011, No 5, pp. 189-200.
17. Liu, C., M. Wang. A Zero-Watermarking Algorithm Resisting JPEG Compression on Images. – Microcomputer & its Applications, Vol. **33**, 2014, No 14, pp. 32-35.
18. Changbo, Q. U., W. Dongfeng. Robust Zero Watermarking Algorithm Based on Bit Plane Theory and Singular Value Decomposition. – Journal of Computer Applications, Vol. **34**, 2014, No 12, pp. 3462-3465.
19. Anuradha, R. P. Singh. DWT Based Watermarking Algorithm Using Haar Wavelet. – Journal of Electronics and Computer Science Engineering, Vol. **1**, 2012, No 1, pp. 1-6.
20. Kannammal, A., S. S. Rani. Authentication of Medical Images Using Integer Wavelet Transforms. – International Journal of Emerging Technology and Advanced Engineering, Vol. **2**, 2012, No 9, pp. 104-108.
21. Al-Haj, A. A. Amer. Secured Telemedicine Using Region-Based Watermarking with Tamper Localization. – Journal of Digital Imaging, Vol. **27**, 2014, No 6, pp. 737-750.
22. Seenivasagam, V., R. Velumani. A QR Code Based Zero-Watermarking Scheme for Authentication of Medical Images in Teleradiology Cloud. – Computational and Mathematical Methods in Medicine, Vol. **2013**, 2013, pp. 1-13.