A Robust Watermarking Algorithm for Encrypted 3D Medical Images Based on 3D-DCT

Lian XU, Jing-bing LI*

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

***Abstract* — This work proposes a novel scheme for robust watermarking in encrypted 3D medical images. In the first phase, the owner of the 3D medical image encrypts the 3D medical image in the DCT domain using Logistic Map. Then the third party embeds or extracts the watermark in the encrypted 3D medical image. The watermarking embedding phase does not affect the image data of the encrypted 3D medical image for exploiting the zero-watermarking method. The watermark is calculated with the feature vector of the 3D medical image using exclusive OR, thus generating a watermark embedding key which will be used in the watermark extraction phase. The experimental results show that the proposed watermarking scheme has good robustness to some normal and geometric attacks.**

Keywords - 3D medical image; image encryption; zero watermarking; feature vector; robustness.

I. Introduction

Watermarking is widely used to protect the copyright of digital media. Most of the existing watermarking schemes implement watermark embedding and extraction on the plain media. With people's more and more attention to information security, people might be worried about privacy leakage when the watermark embedder is an untrusted third party, so that watermark embedding in the ciphertext is required to protect the plain media. Moreover, medical images play a significant role in diagnosis in many diseases, so more care is required to embed the watermark in the medical image without affecting quality of image.

In recent years, image processing in the encrypted domain has become a research hotspot. Zhang[1] firstly proposed a reversible data hiding scheme for encrypted images, which embedded the data through modifying the LSB of the encrypted image, and extracted the embedded data with the aid of the spatial correlation in natural image, however only one bit can be embedded in each block, which leads to a low data hiding capacity. Lavanya[2] applied Zhang's scheme[1] in the medical images, with the selection of Region of Interest(ROI) added in. Zhang[3] proposed a new scheme creating a sparse space to accommodate some additional data through compressing the LSBs of the encrypted image. It can not guarantee that the data can be totally extracted as it still exploits the spatial correlation in natural image when extracting data. Based on the Zhang's scheme, Hong[4] improved the correctness of the extracted data and accuracy of the recovered image by using side match. Based on the existing reversible data hiding schemes, Ma[5] proposed a method by reserving room before encryption, which can achieve real reversibility, data extraction and image recovery free of error. The image processing schemes above are in the spatial domain, there are some in the transform domain. Bianchi[6] proposed the implementation of DFT and FFT in the encrypted domain. Zheng[7] proposed an implementation of DWT in the encrypted domain and the method to reduce the data expansion after encryption. Hsu[8] used the scale-invariant feature transform(SIFT) to extract the image feature in the encrypted domain. Zhao[9] proposed a watermarking scheme in the encrypted domain with flexible watermarking capacity, which was robust to image compression and enabled image tampering detection. Zheng[10] implemented Walsh-Hadamrd transform in the homomorphic encrypted domain and applied it in the image watermarking. Guo[11] proposed a robust watermarking scheme in the encrypted domain combining DWT and DCT. Lian[12] proposed a commutative encryption and watermarking scheme for video, which encrypted the intra-prediction mode, motion vector difference and the signs of DCT coefficients and embedded the watermark in the amplitudes of DCT coefficients.

Most of the image processing schemes in the encrypted domain use cipher stream to encrypt the plain image. While encryption in the frequency domain is more secure and it is compatible with the international general compression methods, therefore it is more robust to JPEG compression. There is no research on the watermarking scheme for 3D encrypted images at present, while there are a large number of 3D medical images being produced every day, i.e. CT, MRI images.

This paper proposes a robust watermarking scheme for DCT domain-encrypted 3D medical images. Chaotic Map is used to encrypt the significant feature of the 3D medical image in the DCT domain, converting the plaintext content into unreadable cipher text, while remaining the feature of the cipher text in the DCT domain. In order not to affect the quality of image, the watermark is not directly embedded in the encrypted 3D medical image, but calculated with the feature vector of the encrypted 3D medical image using exclusive OR, generating a key to be used in the watermark extraction. This kind of zero-watermarking scheme has another excellent advantage of no limitation to the embedding capacity. The experimental results show the proposed watermarking scheme is robust to some normal and geometric attacks.

II. Proposed Scheme

A. Image Encryption

Image encryption is implemented in the DCT domain. Assume the size of the *3D* medical image ***I*** is M×N×P, the three-dimensional DCT for an input image can be defined as

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

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

Where

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

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

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

The three-dimensional inverse DCT can be represented as

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

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

Where (x,y,z) is the sampling value in the spatial domain and (u,v,w) is the sampling value in the frequency domain.

Logistic Map is one of the most widely used Chaotic maps for briefness of expression and good performance. Logistic Map is defined as

$$f(x)=\mu x(1-x) \quad x\in[0,1]$$

Where μ is a constant. Consider only a case when $x\in[0,1]$, $f(x)\in[0,1]$, so μ should meet the requirement of $0<\mu\le 4$.

Assume $\mu_\infty=3.569945672\cdots$, when $\mu_\infty<\mu\le 4$, the Logistic Mapping sequence $\{x_n\}$ has three characteristics as follows, a. initial value sensitivity, b. aperiodicity, c. having strange attractors, the first two are exactly basic properties of and encryption key or a stream cipher.

The process of image encryption is described in detail as follows,

- Apply 3D-DCT on the whole 3D medical image ***I*** and obtain a matrix of 3D-DCT coefficients ***F***.
- Logistic Map is used to generate a sequence of real numbers. A threshold τ is used to transform the sequence to a symbol matrix ***S*** which contains only ±1.

$$S(n)=\begin{cases}1, & x_n\ge\tau\\ -1, & x_n<\tau\end{cases} \quad (3)$$

$$S=reshape(S,[M,N,P]) \quad (4)$$

- Each coefficient of ***F*** is multiplied by the corresponding coefficient of ***S*** in the in the same coordinate respectively.
- Apply 3D-IDCT on the output of the last step and obtain the encrypted 3D medical image ***I'***.

B. Watermark Embedding

In the watermarking embedding phase, the watermark is not actually embedded in the encrypted 3D medical image, but calculated with the feature vector of the encrypted 3D medical image using exclusive OR, the result is saved as a key which will be used in the watermarking extraction phase. The image data of the encrypted 3D medical image remains unchangeable in the process of watermark embedding and there is no limit to the number of the watermark. The size of each watermark depends on the length of the feature vector of the encrypted 3D medical image.

Generally watermarking schemes in the transform domain are more robust than those in the spatial domain. In order to improve the watermark robustness, we extract the feature vector in the transform domain. After applying DCT on an image, most of the significant information of the image is concentrated on the upper left corner of the coefficient matrix and the proposed image encryption does not change this characteristic. The detailed procedure is as follows.

- Apply 3D-DCT on the encrypted 3D medical image ***I'*** and a feature vector ***v*** is generated by comparing the value of the first L DCT coefficients ***F'*** on the upper left corner of the coefficient matrix with 0.

$$v(n)=\begin{cases}1 & F'(n)\ge 0\\ 0 & F'(n)<0\end{cases} \quad (5)$$

$$n=1,2,\cdots,L$$

- In order to improve the watermark security, the original watermark ***w*** is scrambled by Arnold transformation and the scrambled watermark is represented as ***s***.

- The exclusive OR result of the scrambled watermark ***s*** and the feature vector ***v*** of the encrypted medical image is calculated as follows, and the output ***k*** is saved as a key which will be used in the watermark extraction phase.

$$k = s \oplus v \tag{6}$$

C. *Watermark Extraction*

In this phase, the third party extracts the watermark in the received encrypted medical image $\boldsymbol{I_r}$. We consider the third party has the watermark embedding key ***k*** and the watermark scrambling key. The detailed procedure is as follows.

- A feature vector ***v***' of the received encrypted medical image $\boldsymbol{I_r}$ is generated in the same way as mentioned in the watermark embedding phase.
- The exclusive OR is applied on the feature vector ***v***' and the watermark embedding key k and the output is the extracted scrambled watermark ***s***'.
- Perform the inverse Arnold transformation on the extracted scrambled watermark ***s***' and obtain the extracted watermark ***w***'.
- The correlation coefficient value is calculated between the extracted watermark and the original one.

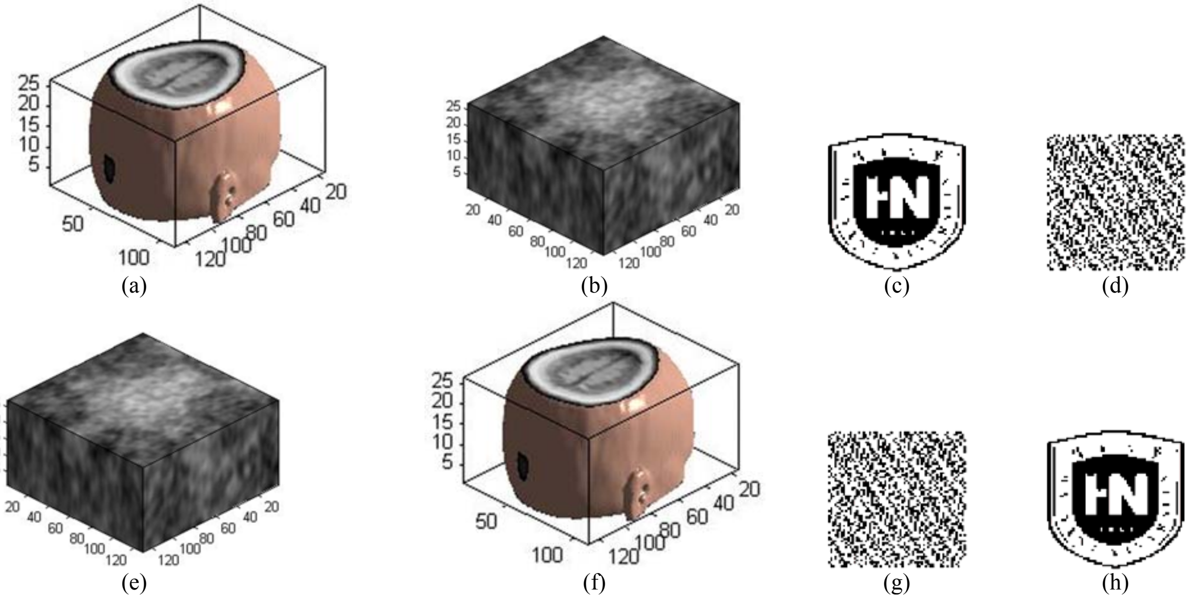
III. EXPERIMENTAL RESULTS

The test 3D medical image sized $128 \times 128 \times 27$ shown in Fig.1(a) was used as the original image in the experiment. We let $\mu = 4$, the initial value of Logistic Map $x_0 = 0.135$. After image encryption, the DCT coefficients were encrypted to generate an encrypted 3D medical image shown in Fig.1(b). We let the length of the feature vector L= 64, the original watermark is chosen as a binary image sized 64×64, which is shown in Fig.1(c), and the scrambled watermark is shown in Fig.1(d). The encrypted 3D medical image containing the watermark is shown in Fig.1(e). We could extract the scrambled watermark embedded in the encrypted 3D medical image using the watermark embedding key. The extracted scrambled watermark and its decryption are shown in Fig.1(g)-1(h). With the encryption key, the original 3D medical image could recover from the encrypted 3D medical image containing the embedded watermark, shown in Fig.1(f).

In order to evaluate the relevance, we compute the Normalized Cross Correlation (NC) of the original watermark and the decryption of the extracted watermark, the expression of NC is given as

$$NC = \frac{\sum_i \sum_j W(i,j) W'(i,j)}{\sum_i \sum_j W^2(i,j)} \tag{7}$$

Where $W(i,j)$ and $W'(i,j)$ are the gray value of the original watermark and the decryption of the extracted watermark respectively. The NC value is greater, the relevance of the two is higher.



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig.1 Experimental Results: (a)The original 3D medical image; (b) The encrypted 3D medical image; (c) The watermark; (d)The scrambled watermark; (e)The watermarked encrypted 3D medical image; (f)The decryption of the watermarked encrypted 3D medical image; (g)The extracted watermark from the encrypted 3D medical image; (g)The decryption of the extracted watermark

In order to prove that the feature vectors of different encrypted 3D medical image in the proposed method are different, experiments were performed on six 3D images, i.e. Head, Liver1, Liver2, Engine, Teddy Bear and Tooth, shown in Fig.2(a)-2(f). They were encrypted using the proposed image encryption scheme. The results are shown in Fig.3(a)-3(f). We calculated the NC values between different encrypted 3D images. The results displayed in the Table I show that the relevance of different 3D images after encryption is close to zero, except that NC between liver1 and liver2 after encryption is relatively higher as the original images of liver1 and liver 2 are similar.

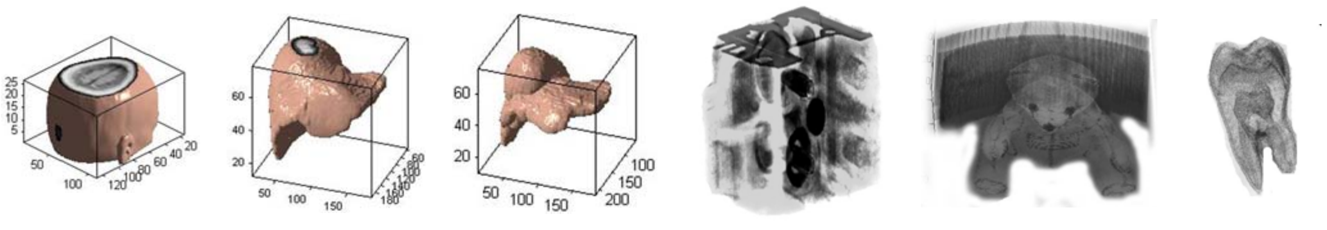


Fig.2 Different 3D images: (a)head; (b)liver1; (c)liver2; (d)engine; (e)teddy bear; (f)tooth

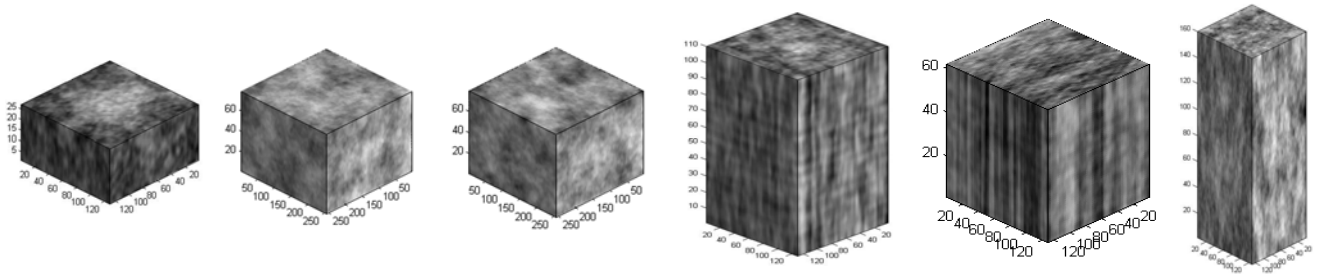


Fig.3 The corresponding encrypted images of different volume data: (a)the encrypted head; (b)the encrypted liver1; (c)the encrypted liver2; (d)the encrypted engine; (e)the encrypted teddy bear; (f)the encrypted tooth.

TABLE I. NC BETWEEN DIFFERENT ENCRYPTED 3D IMAGES

	Va	**Vb**	**Vc**	**Vd**	**Ve**	**Vf**
Va	1	-0.09	-0.03	0.19	-0.16	-0.19
Vb	-0.09	1	0.5	0.16	-0.14	0.16
Vc	-0.03	0.5	1	0.03	-0.08	0.34
Vd	0.19	0.16	0.03	1	0.03	0.06
Ve	-0.16	-0.14	-0.08	0.03	1	0.09
Vf	-0.19	0.16	0.34	0.06	0.09	1

A. *Performance Against Attacks*

Some attacks such as salt & pepper noise, compression, resizing, rotation and cropping have been applied on the watermarked encrypted 3D medical image, the experimental results show the performance of the proposed watermarking scheme against different attacks with varying degrees respectively as follows.

1) Salt & Pepper Noise

We use the function imnoise() to add salt & pepper noise to the watermarked encrypted 3D medical image. When the variance of noise is 0.04, the decryption of the extracted watermark is shown in Fig.4(b). From Table II, we can conclude that the proposed watermarking scheme has good robustness against salt & pepper noise.

TABLE II. The Experimental Data of Adding Salt & Pepper Noise

Variance (%)	**1**	**4**	**8**	**10**	**15**	**20**
NC	0.97	0.94	0.91	0.85	0.81	0.72

2) JPEG compression

JPEG compression is applied on the watermarked encrypted 3D medical image. When the compression quality is 12%, the decryption of the extracted watermark is shown in Fig.4(c). From Table III, we can conclude that the proposed watermarking scheme has strong robustness against JPEG compression.

TABLE III. The Experimental Data of JPEG Compression

Compression Quality(%)	**4**	**8**	**12**	**20**	**30**	**35**
NC	0.78	0.91	0.94	0.94	0.94	1

3) Resizing

Resize the watermarked encrypted medical volume data from size128×128×27 to 256×256×27. The decryption of the extracted watermark is shown in Fig.4(d). From Table IV, we can conclude that the proposed algorithm has strong robustness against resizing attacks.

TABLE IV. The Experimental Data of Resizing

Resizing Factor	**0.1**	**0.4**	**0.8**	**1.2**	**2**
NC	0.81	0.84	0.94	1	1

4) Rotation

When the watermarked encrypted medical volume data is rotated 5° clockwise. The decryption of the extracted watermark is shown in Fig.4(e). From Table V, we can conclude that the proposed algorithm can resist rotation attacks within a small range.

TABLE V. The Experimental Data of Rotation

Rotational Degree	**-5**	**-3**	**-1**	**1**	**3**	**5**
NC	0.72	0.84	0.88	0.88	0.75	0.66

Note: The minus sign denotes C.C.W., no sign denotes C.W..

5) Cropping

When cropping 1/64 of the volume of the watermarked encrypted 3D medical image randomly, the decryption of the extracted watermark is shown in Fig.4(f). From Table VI, we can conclude that the proposed algorithm has good robustness against random cropping attacks.

TABLE VI. The Experimental Data of Cropping

Cropping Percentage(%)	**1/4**	**1/16**	**1/64**	**1/256**	**1/1024**
NC	0.5	0.69	0.81	0.91	1

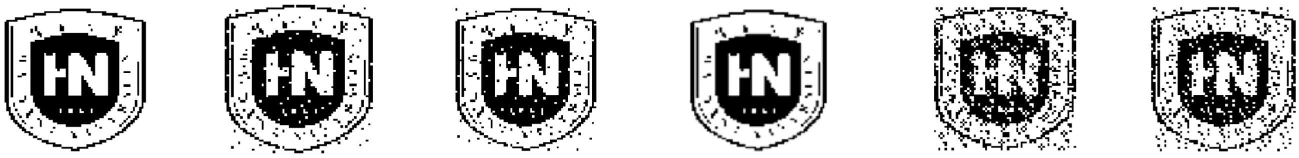


Fig.4 The decryption of the extracted watermark: (a)under no attacks(NC=1); (b)under salt & pepper noise(noise variance=0.04, NC=0.94; (c)under JPEG compression(compression quality=12%, NC=0.94; (d)under resizing(from 128×128×27 to 256×256×27, NC=1); (e)under rotation of 5° clockwise(NC=0.72); (e)under cropping(1/64 of the volume cropped, NC=0.81)

IV. Conclusion

In this paper, a novel scheme for robust watermarking in the encrypted 3D medical image is proposed, which consists of image encryption, watermark embedding and watermark extraction phases. In the first phase, the owner of the 3D medical image encrypts the original 3D medical image in the DCT domain using Logistic Map. The watermark is not actually embedded in the encrypted 3D medical image, but calculated with the feature vector of the encrypted 3D medical image using exclusive OR, so that there is no restriction on the number of the embedded watermarks, while the size of each watermark is dependent on the length of the feature vector. The experimental results show that the proposed watermarking scheme has good robustness to some normal and geometric attacks.

Acknowledgment

This work is partly supported by the National Natural Science Foundation of China (NO: 61263033), and by the International Science and Technology Cooperation Project of Hainan (NO: KJHZ2015-04) and the Institutions of Higher Learning Scientific Research Special Project of Hainan(Hnkyzx2014-2).

References

[1] X. Zhang. “Reversible Data Hiding in Encrypted Image”, IEEE Signal Processing Letters, vol.18, no.4, pp. 255-258, April 2011.

[2] A. Lavanya. “Watermarking Patient Data in Encrypted Medical Images”, Indian Academy of Science, vol.37, part 6, pp. 723-729, December 2012.

[3] X. Zhang. “Separable Reversible Data Hiding in Encrypted Image”, IEEE Transactions Information Forensics and Security, vol.7, no.2, pp.826-832, April 2012.

[4] W. Hong. “An Improved Reversible Data Hiding in Encrypted Images Using Side Match”, IEEE Signal Processing Letters, vol.19, no.4, pp. 199-202, April 2012.

[5] K. Ma. “Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption”, IEEE Transactions Information Forensics and Security, vol.8, no.3, pp.553-562, March 2013.

[6] T. Bianchi, A. Piva, M. Barni. “On the Implementation of the Discrete Fourier Transform in the Encrypted Domain”, IEEE Transactions Information Forensics and Security, vol.4, no.1, pp.86-97, March 2009.

[7] P. Zheng, J. Huang, “Discrete Wavelet Transform and Data Expansion Reduction in Homomorphic Encrypted Domain”, IEEE Transactions on Image Processing, vol.22, no.6, pp. 2455-2468, June 2013.

[8] C. Hsu, C. Lu, S. Pei, “Image Feature Extraction in Encrypted Domain With Privacy-Preserving SIFT”, IEEE Transactions on Image Processing, vol.21, no.11, pp. 4593-4607, November 2012.

[9] B. Zhao, W. Kou, H. Li, et al., “Effective Watermarking Scheme in the Encrypted Domain for Buyer-seller Watermarking Protocol”, Information Sciences, vol.180, pp. 4672-4684 , August 2010.

[10] P. Zheng, J. Huang, “Walsh-Hadamard Transform in the Homomorphic Encrypted Domain and Its Application in Image

Watermarking”, Information Hiding, Springer, vol.7692, pp. 240-254, 2013.

[11] J. Guo, P. Zheng, J. Huang, “Secure Watermarking Scheme Against Watermark Attacks in the Encrypted Domain”, Journal of Visual Communication and Image Representation, Elsevier, no.30, pp.125-125, 2015.

[12] S. Lian, Z. Liu, Z. Ren, et. al., “Commutative Encryption and Watermarking in Video Compression”, IEEE Transactions on Circuits and Systems for Video Technology, vol.17, no.6, pp.774-778, June 2007.