A robust watermarking algorithm for encrypted medical images based on DCT encrypted domain

Jiangtao Dong
College of Information Science and Technology
Hainan University
Haikou, China
jiangtao.dong@hotmail.com

Jingbing Li*
College of Information Science and Technology
Hainan University
Haikou, China
Corresponding author: jingbingli2008@hotmail.com

Yucong Duan
College of Information Science and Technology
Hainan University
Haikou, China
duanyucong@hotmail.com

***Abstract*—The existing watermarking schemes were designed to embed the watermark information into the original images, which are vulnerable to unauthorized access. In this paper, we have proposed a novel and feasible watermarking algorithm in the encrypted domain. First, we encrypted both original medical image and watermark image by using DCT and Logistic map; Then we embedded watermark into the encrypted medical image. In watermarking embedding and extraction phase, zero-watermarking technique has been utilized to ensure the integrity of medical images. At the end of the paper, we compared the robustness of watermarking algorithm between the unencrypted and encrypted approaches. Results demonstrate that in encrypted domain the proposed algorithm is not only robust against common image process such as Gaussian noise, JPEG compression, median filtering, but can also withstand levels of geometric distortions, which can be utilized in information protection of both original medical images and the watermark images.**

Keywords-Robustness; encrypted domain; DCT; Logistic chaotic map; zero-watermarking

I. INTRODUCTION

Digital medical images are important diagnostic tools which are generated using a number of technologies and are mainly used for treating and predicting disease [1]. By using watermarking technique, we can embed personal information such as patient-ID and image hash value into medical image without corrupting it. In addition, with the advance of technology, medical image is widely used on the Internet, which leaves a latent risk for unauthorized access. Thus, it is necessary to encrypt plaintext medical image before it is transmitted through insecure channels. As it is known, digital images have some very characteristic features such as strong correlation among adjacent pixels, bulk data capacity, redundancy of data, being less sensitive compared to the text data and existence of patterns and backgrounds [2]. Therefore, traditional ciphers like DES, AES, IDEA and RSA, are not suitable for real time image encryption as these ciphers require a large computational time and high computing power [3-7]. Accordingly, numerous efforts had been devoted to search the ideal encryption schemes for digital images. In 2010, Patidar et al. in [8] proposed a modified color image encryption algorithm based on standard map and logistic map with fast encryption properties and excellent correlation results considering his early work in [9]. In 2012, Wang et al. in [10] presented a novel color image encryption algorithm based on chaotic logistic map, where the innovation is encrypting the R, G and B components at the same time and therefore the correlation between components is reduced. However, transplanting these existing encryption schemes directly to watermarking in the encrypted domain is a complicated work, due to the limitation of encryption, and the robustness of the watermark in the encrypted domain is another issue that also should be taken into consideration [11]. In 1978, Rivest, Adleman and Derouzos published a paper of homomorphic encryption [12]. The homomorphic cryptosystems provide a suitable way for signal processing in the encrypted domain, since they retain the algebraic relations between the plaintext and the encrypted image. For example, the implementations of the Discrete Fourier Transform (DFT) and the Fast Fourier Transform (FFT) in the encrypted domain were proposed by Bianchi et al. [13]. They also conducted an investigation in the DCT encrypted domain [14]. Zheng et al. proposed the implementation of DWT in the encrypted domain [15].

The approaches mentioned afore only considered image encryption while ignored the robustness of watermarking. However, for medical images watermarking, robustness is a crucial criterion that should be seriously taken into consideration. Thus, we proposed a robust watermarking algorithm in the DCT encrypted domain. This paper is divided into five section. In section III, we describe watermarking scheme in the DCT

encrypted domain. In image encryption phase, we encrypt both original watermark and original medical image. In section IV, through experimental results, we discuss the robustness of our algorithm under various kinds of attacks. Finally, we conclude our paper in section V.

II. THE FUNDAMENTAL THEORY

A. The Discrete Cosine Transform (DCT)

The Discrete Cosine Transform is a signal analysis theory, which is widely used in JPEG and MPEG compression standard. It is well known due to its operation speed and high precision.

The M × N medical images' DCT is defined by:

$$F(u,v) = c(u)c(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cos\frac{\pi(2x+1)\mu}{2M}\cos\frac{\pi(2y+1)v}{2N} \quad (1)$$

u=0,1,...,M-1; v=0,1,...,N-1;

where x, y is the spatial domain sampling value; u, v is the frequency domain sampling value. Digital image pixel are usually square, i.e. M=N.

B. Logistic Map

A chaotic system has a noise like behavior while it is exactly deterministic so we can reproduce it if we have its parameters and initial values. These signals are extremely sensitive to initial conditions. One of the most famous chaotic systems is Logistic Map, which is a nonlinear return map given by

$$x_{k+1} = \mu x_k (1 - x_k) \quad (2)$$

where $0 \le \mu \le 4$ and $x_k \in (0,1)$ are the system variable and parameter respectively, and k is the number of iteration. Logistic Map system works under chaotic condition when $3.569945 \le \mu \le 4$. It can be seen that a small difference in initial conditions would lead to a significant difference of chaotic sequences. These statistical characteristics are the same as white noise, so the above sequence is an ideal secret-key sequence. In this paper, we set μ=4, and the chaotic sequences are generated by different initial values.

III. THE ALGORITHM

A. Encryption algorithm of the original medical images and watermark images

Step 1. Encryption of the medical images

First, obtain the DCT coefficient matrix $D(i, j)$ of the original medical image $I(i, j)$ by using DCT; Then, utilize logistic map to create an chaotic sequence $X(j)$. After sign operation and dimension rising, we can get an binary encrypted matrix $C(i, j)$. We can encrypt the coefficient matrix $D(i, j)$ with $C(i, j)$ by using dot multiplication process, and therefore we get matrix $ED(i, j)$. At last, IDCT is performed on matrix $ED(i, j)$ to achieve the encrypted medical image $E(i, j)$.

$$D(i, j) = \mathrm{DCT2}(I(i, j)) \quad (3)$$

$$ED(i, j) = D(i, j) .* C(i, j) \quad (4)$$

$$E(i, j) = \mathrm{IDCT2}(ED(i, j)) \quad (5)$$

Step 2. Encryption of the watermark images

Employing the same approach but different initial values with that in encrypting original medical image to encrypt the original watermark image.

TABLE I. CHANGE OF DCT COEFFICIENTS UNDER DIFFERENT ATTACKS FOR ENCRYPTED MEDICAL IMAGES

Image processing	**PSNR** (dB)	**C(1,1)**	**C(1,2)**	**C(1,3)**	**C(1,4)**	**C(1,5)**	**C(1,6)**	**C(1,7)**	**C(1,8)**	**C(1,9)**	**C(1,10)**	**Sequence of coefficient signs**	**NC**
Encrypted original image	-	8.21	-0.01	1.74	0.11	-1.84	0.10	-2.07	0.05	-1.26	0.05	1011010101	1.00
Gaussian noise(1%)	20.45	8.49	-0.01	1.79	0.07	-1.7	0.13	-1.93	0.06	-1.16	0.04	1011010101	1.00
JPEG compression (10%)	26.39	8.27	-0.01	1.84	0.11	-1.74	0.10	-2.03	0.04	-1.19	0.06	1011010101	1.00
Median filter [5x5] (20 times)	25.47	7.99	-0.01	1.65	0.11	-1.87	0.11	-2.07	0.06	-1.25	0.05	1011010101	1.00
Rotation (clockwise, 5°)	17.74	8.21	0.03	1.67	0.26	-1.87	0.26	-1.93	0.15	-1.10	0.03	1111010101	0.86
Scaling (×0.5)	-	4.11	0.01	0.87	0.06	-0.91	0.05	-1.03	0.03	-0.62	0.03	1111010101	0.86
Translation (5%, down)	16.62	7.87	0.01	1.66	0.11	-1.85	0.09	-1.94	0.05	-1.18	0.05	1111010101	0.86
Cropping (20%,Y direction)	-	7.85	0.01	1.65	0.11	-1.97	0.08	-1.91	0.05	-1.13	0.07	1111010101	0.86

DCT transform coefficient unit: 1.0e+003

B. Acquire the feature vector of medical images

First, the original image is computed by using DCT. Then, we choose 10 low-frequency coefficients (C(1,1), C(1,2), …C(1,10)) for formation of the feature vector, as shown in Table I. We find that the value of the low-frequent coefficients may change after attacking the image, while the signs of the coefficients remain unchanged. Let "1" represents a positive or zero coefficient, and "0" represents a negative coefficient. Then we can obtain the sign sequence of low-frequency coefficients, as shown in the column "Sequence of coefficient signs" in Table I. After attack, the sign sequence remains unchanged, and the Normalized Cross-correlation (NC) is approximate to 1.0. This means that the signs of the sequence can be regarded as the feature vector of the encrypted medical images.

C. Watermark embedding algorithm

First, obtain the coefficient matrix $FD(i, j)$ of encrypted medical image $E(i, j)$ through DCT; Then, choose the $m \times n$ submatrix coefficients on the top left corner, and apply sign operation to acquire the sign sequence vector $V(j)$; Finally, process the sign sequence vector $V(j)$ and watermark $W(j)$ by using hash algorithm to embed watermark and therefore get the encrypted $Key(j)$ sequence.

$$FD(i, j) = DCT2(E(i, j)) \tag{6}$$

$$V(j) = sign(FD(i, j)) \tag{7}$$

$$Key(j) = V(j) \oplus W(j) \tag{8}$$

D. Watermark extraction algorithm

First, use DCT to obtain the coefficient matrix $FD'(i, j)$ of the tested medical image $E'(i,j)$ which had been encrypted; Then, choose the $m \times n$ submatrix coefficients on the top left corner, and apply sign operation to acquire the sign sequence vector $V'(j)$; Finally, decrypt the sign sequence vector $V'(j)$ by ultilizing hash algorithm to get the extracted watermark sequence $W'(j)$.

$$FD'(i, j) = \mathrm{DCT2}(E'(i, j)) \tag{9}$$

$$V'(j) = sign(FD'(i, j)) \tag{10}$$

$$W'(j) = Key(j) \oplus V'(j) \tag{11}$$

E. Watermark evaluation algorithm

1） The Normalized Cross-correlation (NC) is used for measuring the quantitative similarity between the embedded and extracted original watermark, which is defined as:

$$\mathrm{NC} = \frac{\sum_i \sum_j W(i, j) W'(i, j)}{\sum_i \sum_j W^2(i, j)} \tag{13}$$

After detecting $W'(i,j)$, compute the NC value between $W(i,j)$ and $W'(i,j)$ to determin whether the watermark information is embedded. The larger the NC value, the higher similarity between the extracted and original watermark image is.

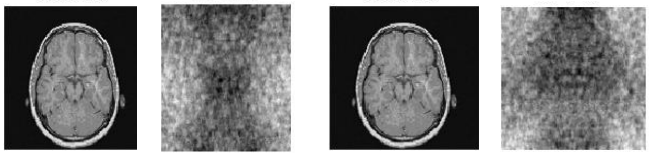
2） The Peak Signal to Noise Ratio (PSNR) is used for measuring the distortion of the watermarked image, which is defined as:

$$PSNR = 10 \lg \left[\frac{MN \max_{i,j} \left(\mathrm{I}(i,j) \right)^2}{\sum_i \sum_j \left(\mathrm{I}(i,j) - \mathrm{I}'(i,j) \right)^2} \right] \tag{14}$$

where $I(i,j)$ and $I'(i,j)$ denote the pixel gray values of the coordinates (i, j) in the original image and the watermarked images respectively; M, N represent the image row and column numbers of pixels respectively.

IV. EXPERIMENTS AND RESULTS

In our experiment, we select the tenth slice of one medical volume data as the original medical image and choose a significant binary image as the original watermarking image. Fig. 1(a) shows the original medical image, one brain slice. Fig. 2(a) shows the original binary image $W=\{W(i,j) \mid W(i,j)=0, 1; 1 \leqslant i \leqslant 32, 1 \leqslant j \leqslant 32\}$. The parameters for encrypting the binary watermark images are: $x_0 = 0.2$, $\mu = 4$; and the parameters for encrypting the medical images are: $x_0' = 0.135$, $\mu' = 4$. Fig. 1 (b) ~ (d) are the encrypted medical image, the decrypted image using the right key, and the decrypted image using a wrong key respectively.



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

Figure 1. Encryption and decryption of medical image: (a) original medical image; (b) encrypted image; (c) decrypted image using the right key; (d) decrypted image using a wrong key.

To verify the effectiveness of the proposed algorithm, we carried out the simulation in Matlab R2010a platform to test the robustness of withstanding common attacks and geometric attacks.

Table II and III shows the results. As can be seen, PSNR and NC values remain stable before and after encryption, which demonstrates the ideal homomorphism of our proposed algorithm.

TABLE II. THE PSNR AND NC VALUES BETWEEN ENCRYPTED AND UNENCRYPTED APPROACHES UNDER COMMON ATTACKS

Common attacks		Gaussian noise			JPEG			Median filter		
		1%	3%	5%	2%	20%	40%	[3x3] 20times	[5x5] 20times	[7x7] 20times
PSNR	Encrypted	20.45	16.17	14.19	20.10	28.94	31.08	25.76	22.26	20.23
	Unencrypted	11.50	7.07	5.11	14.96	15.14	15.25	23.54	19.85	18.82
NC	Encrypted	0.94	0.90	0.82	0.91	0.81	0.85	1.00	0.84	0.70
	Unencrypted	0.93	0.87	0.82	0.93	0.94	1.00	0.96	0.69	0.94

TABLE III. THE PSNR AND NC VALUES BETWEEN ENCRYPTED AND UNENCRYPTED APPROACHES UNDER GEOMETRIC ATTACKS

Geometric attacks		Rotation (clockwise)			Scaling			Translation (down)			Cropping (Y direction)		
		1°	2°	4°	x0.2	x0.8	x2	1%	4%	10%	4%	10%	20%
PSNR	Encrypted	25.55	21.45	18.52	-	-	-	24.17	18.05	16.62	-	-	-
	Unencrypted	27.16	23.11	19.42	-	-	-	21.28	14.89	14.18	-	-	-
NC	Encrypted	1.00	0.87	0.87	0.85	0.91	1.00	1.00	0.81	0.63	0.94	0.74	0.50
	Unencrypted	1.00	1.00	1.00	0.69	0.88	1.00	1.00	0.69	0.56	0.82	0.69	0.75

V. CONCLUSION

The existing watermarking schemes were designed to embed the watermark information into the original images, which are vulnerable to unauthorized access. In this paper, we have proposed a novel watermarking algorithm in the encrypted domain. The method embed the watermark information into encrypted image by using DCT and Logistic map. In watermark embedding phase, zero watermarking technique has been utilized to ensure integrity of encrypted medical images. Results demonstrate that the proposed algorithm has not only good robustness against common attacks and geometric attacks, but also ideal homomorphism, which can be utilized in the protection of both original image and watermark image.

ACKNOWLEDGMENT

This work is supported by National Natural Science Foundation of China (No. 61263033 and 61363007), and by International Science and Technology Cooperation Project of Hainan (NO. KJHZ201504) and the Institutions of Higher Learning Scientific Research Special Project of Hainan (NO. Hnkyzx2014-2).

REFERENCES

[1] A.Kanso, M.Ghebleh, "An efficient and robust image encryption scheme for medical applications," Commun Nonlinear Sci Numer Simulat 24, pp.98–116, 2015.

[2] Ch. K. Volos, I. M. Kyprianidis, I.N. Stouboulos, "Image encryption process based on chaotic synchronization phenomena," Signal Processing 93, pp.1328–1340, 2013.

[3] F. B. Muhaya, M. Usama, M. K. Khan, "Modified aes using chaotic key generator for satellite imagery encryption," Emerg. Intell. Comput. Technol. Appl. 5754, pp.1014–1024, 2009.

[4] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki, "A modified aes based algorithm for image encryption," Int. J. Comput. Sci. Eng. 1 (1), 70, 2007.

[5] G. Chen, Y. Mao, C. K. Chui, "Asymmetric image encryption scheme based on 3d chaotic cat maps," Chaos Solitons Fractals 21(3), pp.749-761, 2004.

[6] P. P. Dang, P. M. Chau, "Image encryption for secure internet multimedia applications," IEEE Trans. Consum. Electron. 46(3), pp.396–403, 2000.

[7] A. J. Menezes,P. C. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, FL, USA.

[8] V. Patidar, N. Pareek, G. Purohit, K.Sud, "Modified substitution–diffusion image cipher using chaotic standard and logistic maps," Commun. Nonlinear Sci. Numer. Simul. 15, pp.2755–2765, 2010.

[9] V. Patidar, N. K. Pareek, K. K. Sud, "A new substitution–diffusion based image cipher using chaotic standard and logistic maps, Commun. Nonlinear Sci. Numer. Simul. 14(7), pp.3056–3075, 2009.

[10] X. Wang, L.Teng, X.Qin, "A novel colour image encryption algorithm based on chaos," Signal Process. 92(4), pp.1101–1108, 2012.

[11] Jianting Guo, Peijia Zheng, Jiwu Huang. "Secure watermarking scheme against watermark attacks in the encrypted domain," J. Vis. Commun. Image R. 30, pp.125-135, 2015.

[12] R.L. Rivest, L. Adleman, M.L. Dertouzos, "On data banks and privacy homomorphisms," Found. Secure Comput. 4 (11), pp.169‑180, 1978.

[13] T. Bianchi, A. Piva, M. Barni, "On the implementation of the discrete fourier transform in the encrypted domain," IEEE Trans. Inform. Forensics Secur. 4 (1), pp.86‑97, 2009.

[14] T. Bianchi, A. Piva, M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems," EURASIP J. Inform. Secur. , 2009.

[15] P. Zheng, J. Huang, "Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain," IEEE Trans. Image Process. 22 (6), pp. 2455-2468, 2013.