# A Robust Zero-Watermarking Algorithm for Encrypted Medical Images in the DWT-DCT Encrypted Domain

Jiangtao Dong, Jingbing Li*, Yucong Duan, Zhen Guo

*College of Information Science and Technology*, Hainan University, Haikou, Hainan, 570228, P.R. China

***Abstract* — Patients' personal information contained in medical images can easily be intercepted and tampered with by unauthorized person when they are transmitted through the Internet. Therefore, it has latent risk of information leakage and should be seriously taken into account. Processing watermarking in the encrypted domain is a reasonable solution. The hybrid Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) based watermarking method improves the robust performance of encrypted domain watermarking scheme. Due to the strict integrity requirement of medical image applications, in this paper, we propose a robust zero-watermarking algorithm in DWT-DCT encrypted domain, which does not modify the pixel value of medical images. Firstly, we scramble the original medical images by utilizing Logistic chaotic map. Then, we extract the DWT-DCT low frequency coefficients as medical images' feature vector. In watermark embedding and extraction phases, we adopt zero-watermarking technique to ensure the integrity of medical images. Taking "db2" wavelet transform for example, we conduct the experiments on the visual quality and robustness of our watermarking scheme. Experimental results demonstrate that our algorithm is not only robust against common attacks such Gaussian noise and JPEG compression, but can also withstand all levels of geometric distortions. Thus it can be effectively put into medical application.**

***Keywords - Robustness; zero-watermarking; feature vector; Homomorphic cryptosystem; DWT-DCT encrypted domain***

## 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 in a medical image without corrupting it. However, the security of watermarking is a challenging issue in watermark community. For most existing watermarking schemes, the embedding and extraction processes are performed in the plaintext domain. Therefore the person performing watermark embedding must be the owner of the watermark or a trusted third party. Otherwise, it leaves a latent risk of exposing the information contained in the media. Considering this reason, numerous efforts had been put into practice. Firstly, to protect the security of text information, numerous image encryption methods have been developed [2-4]. Although preliminary encryption methods such as IDEA, AES, RSA and DES focused on the high correlation among adjacent pixels in digital images, these methods are not efficient enough for suitable image encryption [5, 6]. Homomorphic cryptosystems provide a suitable way for secure signal processing in encrypted domain, since they retain the algebraic relations among plaintext after encryption. In 1978, Rivest, Adleman and Derouzos published a paper of homomorphic encryption [7]. The implementations of the discrete Fourier transform (DFT) and the fast Fourier transform (FFT) in the encrypted domain were proposed by Bianchi et al. [8]. They also conducted an investigation on the encrypted DCT domain [9]. Zheng et al. proposed the implementation of DWT in the encrypted domain [10]. However, besides the encryption algorithm, for image watermarking, robustness is another important and crucial criterion that should also be seriously taken into account. The approaches mentioned before only considered image encryption while ignoring the robustness of watermarking.

Watermarking in the encrypted domain may provide a promising solution to the security signal processing. A Walsh-hadamard transform based image watermarking scheme in the encrypted domain was proposed by Zheng et al. [11] in which the embedding and extracting processes could be performed by a third party without leaking the original images. In [12], an invariant encryption, which leaves the global statistics of the multimedia data, is used for the purpose of implementing commutative watermarking encryption (CWE), while it is used for a particular situation. Therefore, the performance of watermarking scheme in encrypted domain still can be improved. In addition, due to the strict integrity requirements of medical images, that kinds of watermarking methods which modify the pixel values are not suitable for this application.

In this paper, we propose a robust zero-watermarking algorithm for medical images in the DWT-DCT encrypted domain. In section II, we introduce the fundamental theory. In section III, we discuss the zero-watermarking scheme in the DWT-DCT encrypted domain. In section IV, we discuss the robustness of our algorithm under various kinds of attacks based on experimental results, and compared the watermarking methods between plaintext domain and encrypted domain. Finally, we conclude our paper in section V.

## II. THE FUNDAMENTAL THEORY

In this section, we give an introduction to the homomorphic cryptosystem and the implementation of DWT and DCT in the encrypted domain. Since DWT cannot resist the geometric attacks, such as scaling and rotation [13], we combine the DWT-DCT hybrid approach to improve the robustness of our watermarking algorithm.

### *A. Paillier Homomorphic encryption*

In 1978, Rivest et al. first introduced the idea of homomorphic encryption which permits encrypted data to be manipulated without preliminary decryption [7]. It provides a suitable way for secure signal processing. Since it retains the algebraic relations among the plaintext after encryption, so that an algebraic operation on the ciphertext is corresponding to another operation on the plaintexts. The Paillier cryptosystem [14] is a public key cryptosystem with both the homomorphic property and probabilistic property [15]. It is a partial homomorphic cryptosystem, in which only addition or multiplication homomorphism can be achieved.

The reason why we can use the Paillier cryptosystem to encrypt an image is that the Paillier cryptosystem is a homomorphic cryptosystem. Most of the implementations of secure signal processing are based on the homomorphic properties. And the security of Paillier cryptosystem has been proved. There are also a few kinds of secure signal processing techniques based on the Paillier cryptosystem, such as DWT and DCT in the encrypted domain [16]. Our watermarking scheme is based on such transforms in the encrypted domain.

### *B. Implementation of DWT in the encrypted domain*

DWT is a wavelet transform for which the wavelets are sampled at discrete intervals. DWT provides a simultaneous spatial and frequency domain information of the image. In DWT operation, an image can be analyzed by the combination of analysis filter bank and decimation operation. The analysis filter bank consists of a pair of low and high pass filters corresponding to each decomposition level. The low pass filter extracts the approximate information of the image whereas the high pass filter extracts the details such as edges. The application of 2D DWT decomposes the input image into four separate sub-bands: low frequency components in horizontal and vertical direction directions (cA), low frequency component in the horizontal and high frequency component in the vertical direction (cV), high frequency component in the horizontal and low frequency component in the vertical direction (cH) and high frequency component in horizontal and vertical directions (cD). cA, cV, cH and cD can also be represented as LL, LH, HL and HH respectively. The representation of an image I after 1-level DWT with its sub-bands is given by the following equation:

$$I = I_a^1 + I_h^1 + I_v^1 + I_d^1 \tag{1}$$

where $I_a^1$ represents the approximation of input image (smaller scaled form) and $I_h^1$ , $I_v^1$ , $I_d^1$ represent horizontal, vertical and diagonal details respectively, where the powers of the terms represent the level of decomposition. Further decomposition can be achieved by decomposing the *LL* sub-band successively and the resultant image is split into multiple bands.

In this paper, we adopt the 'db2' wavelet, and process the original medical image within just one layer decomposition in order to maintain sufficient computational speed.

### *C. Implementation of DCT in the encrypted domain*

Discrete cosine transform (DCT) is one of the most fascinating transformation methods that transforms data from the spatial domain to another presentation in the frequency domain. Having the property of energy compaction it has been widely applied to the problems of signal and image processing. Most of the energy is concentrated in the lower frequencies and the higher frequency coefficients may be thrown away from its frequency components without too much data quality degradation. A commonly used block size for DCT watermarking is a square of $8\times8$. This is the same size as adopted in the JPEG standard. The two-dimensional DCT with respect to a matrix of $N\times N$ can be expressed as follows:

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

$$u=0,1,...,M-1; \quad v=0,1,...,N-1;$$

The Inverse Discrete Cosine Transform (IDCT) is defined by:

$$f(x,y)=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} c(u)c(v)F(u,v)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)v}{2N} \tag{3}$$

$$x=0,1,...,M-1; \quad y=0,1,...,N-1;$$

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

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*.

### *D. Logistic Map*

The Logistic map is one of the most famous 1D chaotic maps. It is a simple dynamic nonlinear return with complex chaotic behavior so that we can reproduce it if we have its parameters and initial values. Its mathematical definition can be expressed in the following equation:

$$x_{k+1} = x_k\left(1-x_k\right) \tag{4}$$

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 differ-

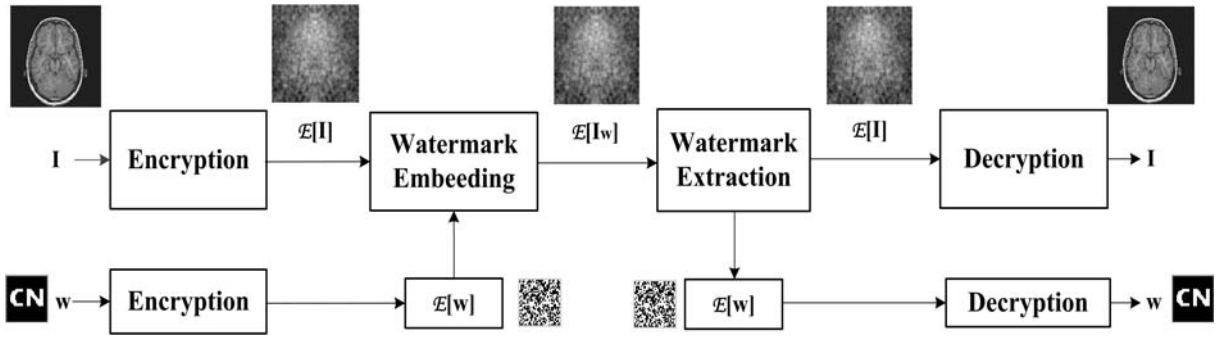



Figure 1. Watermarking scheme in the encrypted domain.

ence 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 $\mu$ =4, and the chaotic sequences are generated by different initial values.

## III. THE ALGORITHM

In this section, we propose a robust image zero-watermarking scheme in the encrypted domain. As shown in Fig. 1, the original image $I$ is firstly encrypted by the homomorphism cryptosystem. A scrambled watermark image $E$[w] is generated from a Logistic sequence $Y(j)$. The watermark embedding is performed in the encrypted domain by a third party, e.g. a cloud server. In order to ensure information security, we have to make sure that the watermark provided to the server is a binary sequence of encrypted 0 and 1. Each watermark bit is encrypted separately. Based on the homomorphic property of the cryptosystem, the output of watermark embedding procedure would be an encrypted version of the watermarked image, $E[I_w]$. After decryption, the user can acquire the decrypted image that meets application requirements.

### *A. Encryption algorithm of the original medical images*

In order to ensure secure signal processing, we conduct our watermarking algorithm in the encrypted domain, Fig. 2 illustrates the encryption scheme of medical images, and the detail encryption scheme can be described as follows:

*a)* Perform DWT on the original medical images to acquire the cA, cH, cV and cD sub-band wavelet coefficients.

*b)* Apply DCT on each sub-band wavelet coefficients cA, cH, cV and cD.

*c)* Encrypt all the sub-band coefficients by dot multiplication operation with a binary matrix $C(i,j)$ generated from another Logistic sequence $X(j)$ which differs from the sequence that encrypts the watermark.

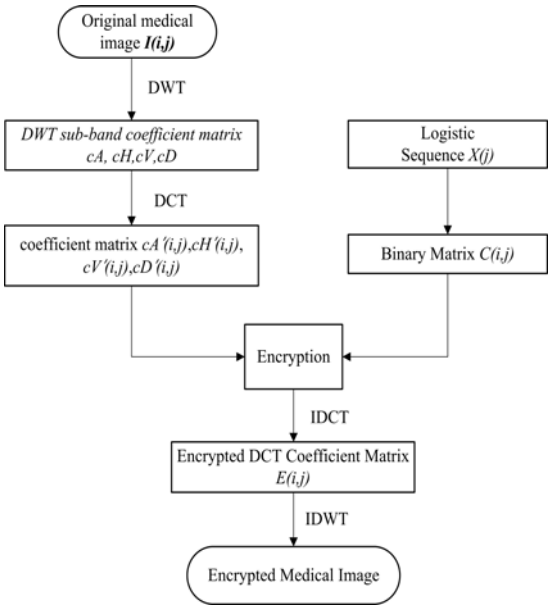



Figure 2. Encryption scheme of medical images.

*d)* Perform inverse DCT (IDCT) on each sub-band.

*e)* Perform inverse DWT (IDWT) on the reconstructed coefficients to acquire the encrypted medical images.

### *B. Acquire the feature vector of encrypted medical images*

Taking both the robustness and visual quality into account, we extract the low-frequency coefficients after applying DWT-DCT hybrid operation. The implementation is given as:

*a)* Perform DWT on the original medical images to acquire the cA, cH, cV, cD sub-band wavelet coefficients;

*b)* Apply DCT to the low frequency coefficients cA($i$,$j$);

TABLE I. CHANGE OF DWT-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, no attack | 90.10 | 1.296 | -0.014 | -0.413 | -0.012 | -0.102 | -0.009 | -0.133 | -0.004 | -0.079 | -0.002 | 10000 00000 | 1.00 |
| Gaussian noise(3%) | 15.54 | 1.330 | -0.009 | -0.390 | -0.005 | -0.083 | -0.006 | -0.118 | -0.011 | -0.067 | -0.008 | 10000 00000 | 1.00 |
| JPEG compression (30%) | 18.33 | 9.382 | -0.083 | -3.714 | -0.074 | -0.483 | -0.067 | -0.947 | -0.015 | -0.476 | -0.004 | 10000 00000 | 1.00 |
| Median filter [5x5] (10 times) | 27.24 | 1.288 | -0.013 | -0.416 | -0.012 | -0.107 | -0.009 | -0.132 | -0.004 | -0.080 | -0.002 | 10000 00000 | 1.00 |
| Rotation (clockwise,3°) | 20.84 | 1.290 | -0.018 | -0.419 | -0.009 | -0.106 | -0.010 | -0.131 | -0.007 | -0.079 | -0.004 | 10000 00000 | 1.00 |
| Scaling (×0.6) | - | 7.624 | -0.006 | -2.644 | -0.050 | -0.707 | -0.015 | -0.852 | -0.014 | -0.468 | -0.001 | 10000 00000 | 1.00 |
| Translation (10%, down) | 15.09 | 1.234 | -0.013 | -0.403 | -0.012 | -0.103 | -0.009 | -0.120 | -0.004 | -0.076 | -0.001 | 10000 00000 | 1.00 |
| Cropping (10%,Y direction) | - | 1.298 | -0.013 | -0.424 | -0.012 | -0.108 | -0.009 | -0.126 | -0.004 | -0.080 | -0.001 | 10000 00000 | 1.00 |

DWT-DCT transform coefficients unit: 1.0e+004.

*c)* Extract the low and middle frequency coefficients of DCT matrix cA'(*i,j*), after binary processing which represented in Equation (5), we can obtain a binary sign sequence of coefficients as the feature vector.

$$\mathrm{sgn}(x) = \begin{cases} 1, & cA'(i,j) \geq 0 \\ 0, & cA'(i,j) < 0 \end{cases} \qquad (5)$$

As shown in Table 1, after numerous experiments, we found that the value of DWT-DCT low-frequency coefficients may change after attacking the encrypted image, while the signs of the coefficients still remain unchanged. Let "1" represents a positive or zero coefficient, and "0" represents a negative coefficient. We can obtain the sign sequence of low-frequency coefficients, as shown in the column "Sequence of coefficient signs" in Table 1. After the attack, the sign sequence is unchanged, and the Normalized Cross-correlation (NC) is equal to 1.0. Thus we can adopt the coefficient signs as the feature vector of the encrypted medical images.

### *C. Watermark embedding in the encrypted domain*

In order to implement the watermark embedding algorithm in the encrypted domain, we need to utilize the homomorphic property and the encrypted domain transform discussed in section II. Fig. 3 shows the watermark embedding scheme. The embedding algorithm in the encrypted domain can be described as:

*a)* Watermark scrambling. Firstly, we generate a binary logistic sequence *k(n)* by using Logistic map. After that, perform XOR operation between *k(n*) and the original watermark *w(j)* to acquire the scrambled watermark *ew(j)*.

*b)* Acquire feature vector *V(j)*. Firstly, perform hybrid DWT-DCT transform on the encrypted medical image. Then, acquire the feature vector. Taking the robustness and visual quality into account, we extract the DWT-DCT low-frequency coefficients, and utilize the sign operation mentioned in Equation (5). Thus, we can get the extracted feature vector *V(j)* which contains only 0 and 1.

*c)* Employ XOR operation between *V(j)* and *ew(j)* to acquire the *Key(j)*. Once the key is generated, the watermark is embedded in.

Note that we adopt zero-watermarking technique here, rather than the method that modifies the image pixel value. Due to its good property in maintaining image integrity, it can be an ideal method to be put into practice in severely strict conditions, medical image application, for example.

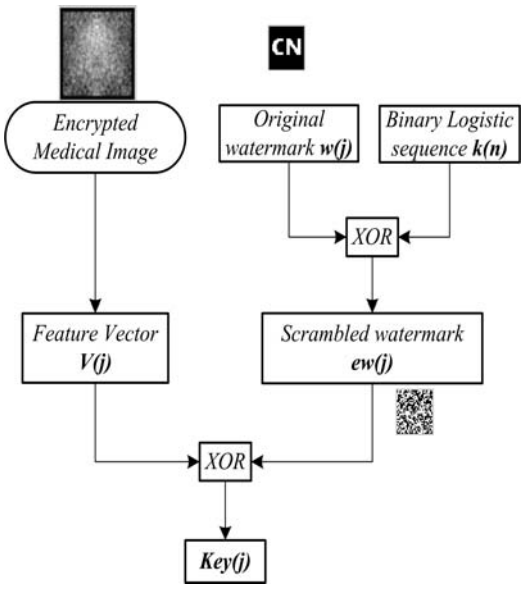



Figure 3. Watermark embedding algorithm.

*D. Watermark extraction in the encrypted domain*

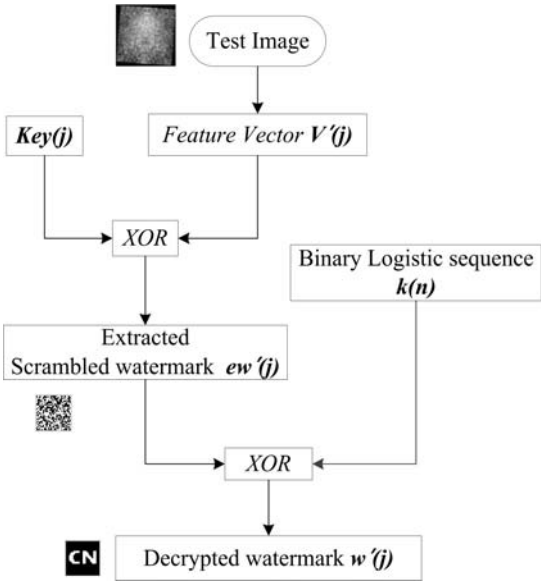



Figure 4. Watermark extraction algorithm.

Fig. **4** is the flow chart of extracting watermark image. The implementation of extraction algorithm in the encrypted domain can be described as:

*a)* Perform DWT-DCT on the test image to extract its feature vector *V′(j)*.

*b)* Employ XOR operation between *V'(j)* and *Key(j)* to acquire the extracted scrambled watermark *ew'(j)*.

*c)* Recover the watermark image by applying XOR operation between *ew'(j)* and the binary Logistic sequence *k(n)*, so we can get the extracted watermark image *w'(j)*.

*E. Watermark evaluation*

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

$$NC = \frac{\sum_i \sum_j W(i,j)W'(i,j)}{\sum_i \sum_j W^2(i,j)} \qquad (6)$$

  After detecting *W'(i,j)*, we compute the NC values between *W(i,j)* and *W'(i,j)* to determine whether the watermark is embedded inside. The larger the NC value, the higher similarity between the extracted and embedded watermark image is.
- The Peak Signal to Noise Ratio (PSNR) is used for measuring the distortion of the watermarked image, which is defined as:

$$PSNR = 10\lg\left[\frac{MN\max_{i,j}\left(I(i,j)\right)^2}{\sum_i\sum_j\left(I(i,j)-I'(i,j)\right)^2}\right] \qquad (7)$$

- where *I(i,j)* and *I'(i,j)* denote the pixel grey values of the coordinates *(i,j)* in the original images and the watermarked images respectively. M and N represents the image row and column numbers of pixels respectively.

## IV. EXPERIMENTAL RESULTS

In our experiment, we select the tenth slice of one medical volume medical data as the original medical image ($128 \times 128$) and choose a significant binary image ($32 \times 32$) as the original watermark image. Fig. **5** (a) shows the original medical image. Fig. **5** (c) 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 $x_0' = 0.135$, $\mu' = 4$ for encrypting the medical images respectively. Firstly, we test our algorithm in the plaintext domain and then in the encrypted domain. We show some original images in Fig. **6**. Although eight test images have been used during experimentation, only results based on "mir-1" are presented.

*A. Experiments in the plaintext domain*

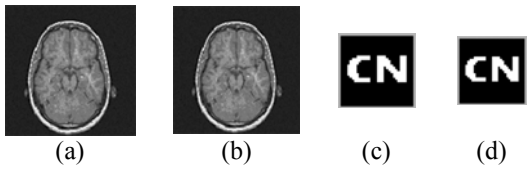



Figure 5. Watermarking in the plaintext domain: (a) original medical image, (b) watermarked medical image, (c) original watermark, and (d) extracted watermark.

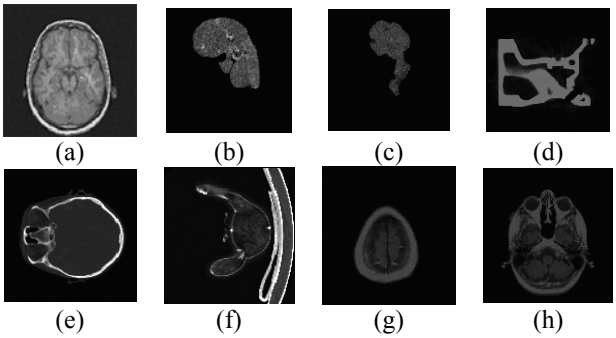
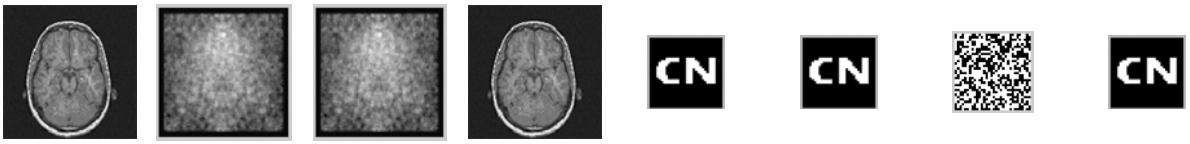



Figure 6. Some examples of the original standard tested images: (a) mir-1, (b) mir-2, (c) mir-3, (d) engine, (e) head, (f) teddy bear, (g) mir-1back1, and (h) mir-1back.



(a) (b) (c) (d) (e) (f) (g) (h)

Figure 7. Watermarking in the encrypted domain: (a) original medical image "mir-1", (b) encrypted "mir-1" image, (c) watermarked image, (d)decrypted watermarked image, (e) original watermark, (f) plaintext domain extraction, (g) encrypted domain extraction, and (h) decrypted watermark.

In this case, we used the plaintext image, i.e. the unencrypted medical image as the original image, and did not scramble the original watermark. Fig. 5 shows the watermarking in the plaintext domain. Due to the ideal property of zero-watermarking technique, after watermark embedding, the watermarked medical image maintains excellent visual perceptibility that we cannot visually identify the difference between the original images and the watermarked images.

### *B. Experiments in the encrypted domain*

Watermark attacks may be performed on the encrypted images or the decrypted ones. In this subsection, we conduct our experiment in the encrypted domain to study the performance of the watermarking scheme under the encrypted domain attacks.

Fig. **7** shows the watermarking in the encrypted domain. Similar to that in the plaintext domain, we also utilize zero-watermarking technique in the encrypted domain. Fig. 5 (c) and (d) shows the original watermark and the extracted watermark in the plaintext domain. The watermark can be correctly extracted with NC=1.00 without watermark attacks. In addition, we show some original test images in Fig. 6.

TABLE II. THE PSNR AND NC VALUES OF WATERMARKED IMAGES IN PLAINTEXT AND ENCRYPTED DOMAIN

| Attacks | Parameters | PSNR (dB) | | NC | |
|---|---|---|---|---|---|
| | | Plaintext | Encrypted | Plaintext | Encrypted |
| **Gaussian noise** | 1% | 21.05 | 20.18 | 0.85 | 0.87 |
| | 3% | 16.78 | 15.54 | 0.67 | 0.81 |
| | 5% | 14.65 | 13.59 | 0.65 | 0.76 |
| **JPEG** | 10% | 21.22 | 18.09 | 0.81 | 0.94 |
| | 20% | 21.51 | 18.29 | 0.76 | 0.88 |
| | 40% | 21.58 | 18.35 | 0.84 | 0.84 |
| **Median filtering** | [3x3], 10times | 24.98 | 27.24 | 0.96 | 0.89 |
| | [5x5], 10times | 21.14 | 24.11 | 0.81 | 0.81 |
| | [7x7], 10times | 19.77 | 22.99 | 0.75 | 0.82 |
| **Rotation (clockwise)** | 1° | 29.01 | 26.73 | 0.73 | 0.81 |
| | 2° | 24.58 | 22.79 | 0.65 | 0.75 |
| | 4° | 20.59 | 19.72 | 0.56 | 0.75 |
| **Scaling** | x0.2 | - | - | 0.51 | 0.50 |
| | x0.8 | - | - | 0.51 | 0.51 |
| | x2.0 | - | - | 0.62 | 0.70 |
| **Translation (down)** | 1% | 22.24 | 24.88 | 1.00 | 0.91 |
| | 2% | 18.11 | 20.96 | 1.00 | 0.78 |
| | 6% | 14.83 | 16.57 | 0.84 | 0.65 |
| **Cropping (Y direction)** | 4% | - | - | 0.94 | 0.76 |
| | 10% | - | - | 0.88 | 0.65 |
| | 20% | - | - | 0.57 | 0.65 |

### C. Data Analysis

To verify our algorithm, we test the watermarking scheme on Matlab R2014a platform with a computer contains four Intel(R) Core(TM) i5-4590 CPUs at 3.30GHz. In the case of embedding a $32 \times 32$ binary watermark image into a $128 \times 128$ image, the execution time of encryption and decryption are about 2.5s and 2.5s. The execution time of encrypted domain watermark embedding is about 0.5s and the extraction time is about 0.5s in the encrypted domain.

We use the peak signal to noise ratio (PSNR) value to evaluate the visual quality of the watermarked images. The robustness of the scheme is measured by the Normalized Cross-correlation (NC). Experimental results of watermark attacks in the plaintext and encrypted domains are illustrated in Table **2**. We can observe that the performance of the encrypted domain watermarking scheme is close to that of the plaintext domain under watermark attacks. In addition, the proposed watermarking scheme can resist majority of the attacks that are available in the encrypted domain.

## V. CONCLUSIONS

Most of the existing watermarking schemes were designed to embed the watermark information in the plaintext domain, which are vulnerable to unauthorized access. In this paper, we propose a robust watermarking scheme in the encrypted domain. The main contributions are listed as follows.

(1) We have proposed a watermarking algorithm in the encrypted domain, which is robust against the watermark attacks in the encrypted domain. By using the homomorphic property of the cryptosystem, we can extract watermark. We have proposed a watermarking algorithm in the encrypted domain, which is robust against the watermark attacks in the encrypted domain. By using the homomorphic property of the cryptosystem, we can extract watermark directly in the DWT-DCT encrypted domain without preliminarily decrypting the watermarked image. Therefore, the watermark embedding and extraction processing can be safely manipulated on the third party platform, i.e., the cloud server.

(2) We have adopted the zero-watermarking technique which did not modifies the image pixel value, thus it can be used in special conditions like medical images etc. that strictly demands image quality.

(3) By utilizing our watermarking method, the computational speed can easily meets practical requirements.

## ACKNOWLEDGEMENTS

This work is supported by National Natural Science Foundation of China (No. 61263033 and 61363007), International Science and Technology Cooperation Project of Hainan (NO. KJHZ201504), the Institutions of Higher Learning Scientific Research Special Project of Hainan (NO. Hnkyzx2014-2) and Natural Science Foundation of Hainan (NO. 20166217).

## REFERENCES

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

[2] Zhao T, Ran Q and Chi Y, "Image encryption based on nonlinear encryption system and public-key cryptography", *Opt Commun*, Vol. 338, 2015, pp. 64-72.

[3] Murillo-Escobar MA, Cruz-Hernández C, Abundiz-Pérez F, López-Gutiérrez RM and Acosta Del Campo OR, "A RGB image encryption algorithm based on total plain image characteristics and chaos", *Signal Process*, Vol. 109, 2015, pp. 119-31.

[4] Eyebe Fouda JSA, Effa JY and Ali M, "Highly secured chaotic block cipher for fast image encryption", *Appl Soft Comput*, Vol. 25, 2014, pp. 435-44.

[5] Li S, Chen G, Cheung A, Bhargava B and Lo K-T, "On the design of perceptual MPEG video encryption algorithms", *IEEE Trans Circuits Syst Video Technol*, Vol. 17, 2007, pp. 214-23.

[6] Zhang G, Liu Q. "A novel image encryption method based on total shuffling scheme", *Opt Commun*, Vol. 284, 2011, pp. 2775-80.

[7] R. L. Rivest, L. Adleman and M. L. Dertouzos. "On data banks and privacy homomorphisms", *Found. Secure Comput*, Vol. 11, no. 4,1978, pp. 169-180.

[8] T. Bianchi, A. Piva and M. Barni, "On the implementation of the discrete fourier transform in the encrypted domain", *IEEE Trans. Inform. Forensics Secur*. Vol. 4 , no. 1, 2009, pp. 86-97.

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

[10] P. Zheng, J. Huang. "Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain", *IEEE Trans. Image Process*, Vol. 22, no. 6, 2009, pp. 2455-2468.

[11] P. Zheng, J. Huang. "Walsh-Hadamard transform in the homomorphic encrypted domain and its application in image watermarking", *Information Hiding, Lecture Notes in Computer Science*, Vol. 7692, Springer, 2013, pp. 240-254.

[12] R. Schmitz, S. Li, C. Grecos and X. Zhang. "A new approach to commutative watermarking-encryption, in: B. De Decker, D. Chadwick (Eds.)", *Communication and Multimedia Security, Lecture Notes in Computer Science*, Vol. 7394, Springer, Berlin Heidelberg, 2012, pp. 117-130.

[13] X. Kang, J. Huang, Y. Shi and Y. Lin. "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression", *IEEE Trans.CIirc.Syst.Vedio Technol*, Vol. 13, no. 8, 2003, pp. 776-786.

[14] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes", *Advances in Cryptology-EUROCRYPT' 99*, Springer, 1999, pp.223-238.

[15] S. Goldwasser, S. Micali. "Probabilistic encryption". *J. Comput. Syst. Sci.* Vol. 28, no.2, 1984, pp. 270-299.

[16] P. Failla, Y. Sutcu and M. Barni. "Esketch: a privacy-preserving fuzzy commitment scheme for authentication using encrypted biometrics", *Proceedings of the 12th ACM workshop on Multimedia and Security, ACM*, 2010, pp. 241-246.