

## **A Novel Robust Watermarking Algorithm for Encrypted Medical Image Based on DTCWT-DCT and Chaotic Map**

**Jing Liu<sup>1,5</sup>, Jingbing Li<sup>1,\*</sup>, Jieren Cheng<sup>1</sup>, Jixin Ma<sup>2</sup>, Naveed Sadiq<sup>3</sup>,  
Baoru Han<sup>4</sup>, Qiang Geng<sup>5</sup> and Yang Ai<sup>5</sup>**

**Abstract:** In order to solve the problem of patient information security protection in medical images, whilst also taking into consideration the unchangeable particularity of medical images to the lesion area and the need for medical images themselves to be protected, a novel robust watermarking algorithm for encrypted medical images based on dual-tree complex wavelet transform and discrete cosine transform (DTCWT-DCT) and chaotic map is proposed in this paper. First, DTCWT-DCT transformation was performed on medical images, and dot product was performed in relation to the transformation matrix and logistic map. Inverse transformation was undertaken to obtain encrypted medical images. Then, in the low-frequency part of the DTCWT-DCT transformation coefficient of the encrypted medical image, a set of 32 bits visual feature vectors that can effectively resist geometric attacks are found to be the feature vector of the encrypted medical image by using perceptual hashing. After that, different logistic initial values and growth parameters were set to encrypt the watermark, and zero-watermark technology was used to embed and extract the encrypted medical images by combining cryptography and third-party concepts. The proposed watermarking algorithm does not change the region of interest of medical images thus it does not affect the judgment of doctors. Additionally, the security of the algorithm is enhanced by using chaotic mapping, which is sensitive to the initial value in order to encrypt the medical image and the watermark. The simulation results show that the proposed algorithm has good homomorphism, which can not only protect the original medical image and the watermark information, but can also embed and extract the watermark directly in the encrypted image, eliminating the potential risk of decrypting the embedded watermark and extracting watermark. Compared with the recent related research, the proposed algorithm solves the contradiction between robustness and invisibility of the watermarking algorithm for encrypted medical images, and it has good results against both conventional attacks and geometric attacks. Under geometric attacks in particular, the proposed algorithm performs much better than existing algorithms.

---

<sup>1</sup> College of Information Science and Technology, Hainan University, Haikou, 570228, China.

<sup>2</sup> School of Computing and Mathematical Sciences, Faculty of Liberal Arts and Sciences, University of Greenwich, Greenwich, London, SE10 9LS, UK.

<sup>3</sup> Ocean College, Zhejiang University, Hangzhou, 310058, China.

<sup>4</sup> College of Medical Informatics, Chongqing Medical University, Chongqing, 400016, China.

<sup>5</sup> Faculty of Network Science, Haikou University of Economics, Haikou, 571127, China.

\* Corresponding Author: Jingbing Li. Email: jingbingli2008@hotmail.com; jingliuhnu2016@hotmail.com.

**Keywords:** Encrypted medical images, zero-watermarking, DTCWT, perceptual hash, chaotic map.

## 1 Introduction

Nowdays, with the promotion of big data and cloud platforms, the use of modern diagnostic tools such as medical images to diagnose and predict diseases is more and more widely in the medical industry. However, the medical image is a special kind of digital image, which contains personal information like the patient's name, gender, age et al. and the medical information carried by themselves that reflect the patients' health. When they are transmitted over the internet, there exists a security risk of information leakage [Vengadapurvaja, Nisha, Aarthy et al. (2017); Mothi and Karthikeyan (2019); Qasim, Meziane and Aspin (2018)], especially for some patients with special identities. It is urgent to properly handle this problem as soon as possible in order to ensure the security of information transmission and processing [Elhoseny, Ramirez-Gonzalez, Abu-Elnasr et al. (2018)].

Digital watermarking technology is an effective technique of multimedia copyright protection and has been widely explored by researchers since its appearance. However, most digital watermarking algorithms remain in the plaintext domain [Fan, Chao and Chieu (2019); Bamal and Kasana (2018); Thanh and Tanaka (2017); Kavitha, Palanisamy and Sureshkumar (2018); Soualmi, Alti and Laouamer (2018); Rai and Singh (2017)]. That is to say, the embedding and extraction of the watermark are done in unencrypted carrier images. As a result, on one hand, the embedding of the watermark must be carried out by the owner of the watermark at the same time to ensure data protection [Thanki, Borra, Dwivedi et al. (2017)]. And the embedding and extraction of the watermark cannot be handled by a third party, otherwise, the watermark information could be leaked. On the other hand, since the related operation is performed in the plaintext domain, if the plaintext medical image is intercepted during the transmission process, it is easy to expose the information of the carrier image itself. Therefore, the robust digital watermarking technology of the plaintext medical image can only guarantee the security of the watermark information, ignoring the consideration of the carrier medical images. A medical image is a special type of image that contains a large amount of important information of patients. When applying digital watermarking technology in medical images, the safety of the carrier medical image itself should also be seriously considered [Lakshmi, Thenmozhi, Rayappan et al. (2018)]. Performing the above operations in the encryption domain is a feasible solution.

In order to satisfy the requirements of security, integrity and robustness of both watermark and carrier images, the ciphertext domain robust zero-watermark technique can be used. First, encrypt the patient's plaintext medical image, and invest the obtained encrypted medical image as the carrier image for watermark embedding. After use the privacy information such as the patient's ID, age, gender et al. as the watermark to encrypt, apply zero-watermark technology to embed into the encrypted medical image. In the process of information transmission, as the watermark and the image itself are ciphertext, on the one hand, the probability of occurrence of the information leakage event can be minimized, on the other hand, the embedding and extraction of the watermark can be handled by a third

party. Unlike the digital watermarking scheme in the plaintext domain which embedding and extraction of the watermark needs to be done by the owner of the watermark [Chen, Yin, He et al. (2018)], with the homomorphism of encryption algorithm, watermark and carrier image in ciphertext state can be delivered to a trusted third party [Dai, Wang, Zhou et al. (2016)]. The embedding and extraction of the watermark can be realized by utilizing the resource advantages of the third party (such as a powerful cloud server). Compared with the previous plaintext watermarking method, the encryption domain digital watermarking scheme has obvious security advantages.

To implement digital watermarking in ciphertext domain, the image must be encrypted first. In the aspect of image encryption algorithm, more research results have been obtained. Such as Lavanya et al. [Lavanya and Natarajan (2012)] utilized standard stream cipher for image encryption and selecting non-region of interest tile to embed patient data. Xiong et al. [Xiong, Xu and Shi (2018)] used integer wavelet transform to encrypt image. Liu et al. [Liu, Qu and Xin (2016)] divided the medical image into regions of interest (ROI) and regions of non-interest (RONI). After encrypting the image with the secret key, she connected the least significant bit of the encrypted ROI with Electronic Patient Record (EPR) and embedded the data with the LSB replacement algorithm. Bouslimi et al. [Bouslimi, Bellafqira and Coatrieux (2016)] combined Paillier cryptography with quantitative modulation (QIM), inserted pre-watermark into the image before adding it, and used the modified QIM to encrypt the image. Nematzadeh et al. [Nematzadeh, Enayatifar, Motameni et al. (2018)] proposed a hybrid model of medical image encryption method. It takes the number of secure cryptographic images generated by the coupled mapping lattice as the initial population of the improved genetic algorithm. Laiphrakpam et al. [Laiphrakpam and Khumanthem (2017)] coded pure information as elliptic curvilinear coordinates to eliminate the calculation and improved ElGamal encryption scheme for medical image encryption. Avudaiappan et al. [Avudaiappan, Balasubramanian, Pandiyan et al. (2018)] used double encryption method. First verified puffer fish encryption with signature encryption algorithm, then upgraded the private key and public key by the Opposition based Flower Pollination (OFP). Cao et al. [Cao, Zhou, Chen et al. (2017)] proposed a medical image encryption algorithm with large key space and strong key sensitivity of source image edge mapping. Ismail et al. [Ismail, Said, Radwan et al. (2018)] designed an image encryption algorithm based on pseudo-random sequence generation and realized the safe transmission of medical MRI and X-ray images by using generalized DH mapping.

However, the image encryption algorithms that can be used for robust digital watermarking at this stage are not very mature [Laiphrakpam and Khumanthem (2017); Ismail, Said, Radwan et al. (2018)]. It mainly has the following problems: Firstly, not all image encryption algorithms can guarantee the robustness of digital watermarks in the encrypted domain. For some image encryption algorithms, the watermark can be extracted after being embedded [Liu, Qu and Xin (2016); Xiong, Xu and Shi (2018); Bouslimi, Bellafqira and Coatrieux (2016)]. But under the interference of various watermark attacks such as Gaussian noise, JPEG compression, median filtering, rotation, scaling and translation, the watermark quality is poor, and the watermark robustness cannot be guaranteed. Secondly, in the plaintext domain, although many robust digital watermarking algorithms have been proposed, due to the limitations of encryption

algorithms, it will be quite a complex task to transplant these robust digital watermarking methods directly into the encrypted domain, especially in medical images with special requirements for images.

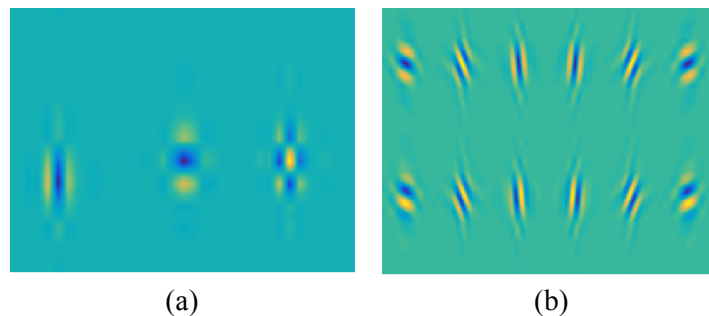
Based on the above reasons, we proposed a robust digital watermarking algorithm for encrypted medical images. It adopts zero-watermark technology, and uses the dual-tree complex wavelet transform and Logistic chaotic map in the encryption domain. A reliable visual vector feature is selected in the encryption domain to embed and extract the encrypted domain watermark. This algorithm enhances the security of the medical image and the watermark. Without any changes to the original image and without decryption, the extraction of the watermark can be completed. With the help of the homomorphic characteristics of the encryption algorithm, the watermark and the carrier image in the encrypted state can be handed in a trusted third party. It not only solves the contradiction between the robustness and the invisibility of common algorithms, but also performs well in resisting conventional attacks and geometric attacks.

## 2 The fundamental theory

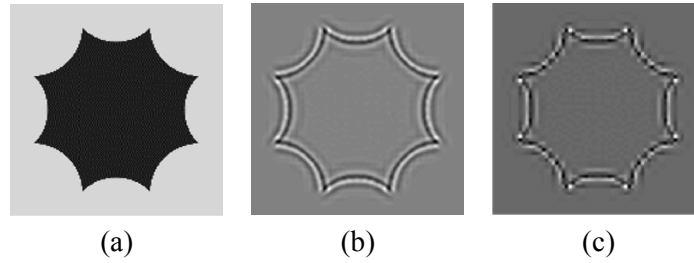
### 2.1 Dual-tree complex wavelet transform (DTCWT)

2D DWT uses the separation and filtering of image rows and columns, and its two-extraction process brings the defects of translation sensitivity and lack of direction selection, which seriously affects the effect of feature extraction. Therefore, dual-tree complex wavelet transform (DTCWT) is born. Fig. 1 and Fig. 2 respectively showed the critical sampling of two-dimensional wavelet and the two-dimensional dual-tree complex wavelet and their two-dimensional edge representation. DTCWT adopted the DWT of binary tree structure and used two trees to represent the generated real and imaginary Numbers respectively [Selvakumar, Jerome and Rajamani (2016)]. The formula is shown as follows:

$$\psi_g(x)\psi_h(y) + \psi_h(x)\psi_g(y) \quad (1)$$

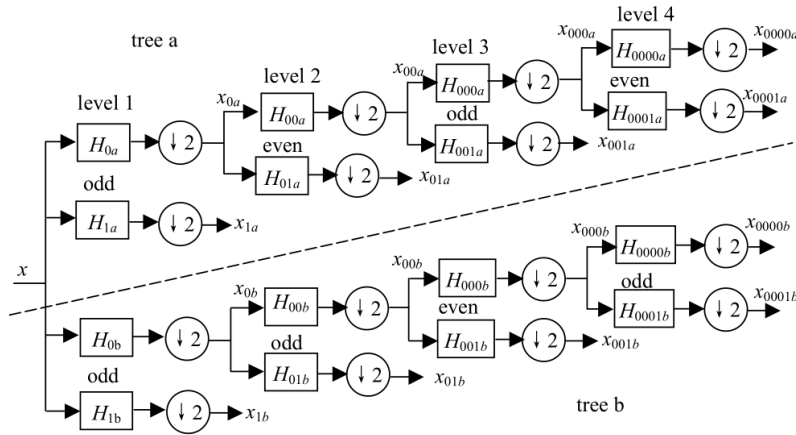


**Figure 1:** Critical sampling of two-dimensional images: (a) DWT, (b) DTCWT



**Figure 2:** Edge representation of a two-dimensional image: (a) DTCWT, (b) DWT

When transforming, two trees are carried out side-by-side with fixed sampling interval, as shown in Fig. 3. The two-dimensional DTCWT will produce six direction ( $\pm 15^\circ$ ,  $\pm 45^\circ$ ,  $\pm 75^\circ$ ) for high frequency sub images [Zebbiche, Khelifi and Loukhaoukha (2018)]. It can effectively overcome the defects of DWT. Combined with other advantages, it has become the preferred transformation for the extraction of medical image features in this paper.



**Figure 3:** The dual-tree complex wavelet transform

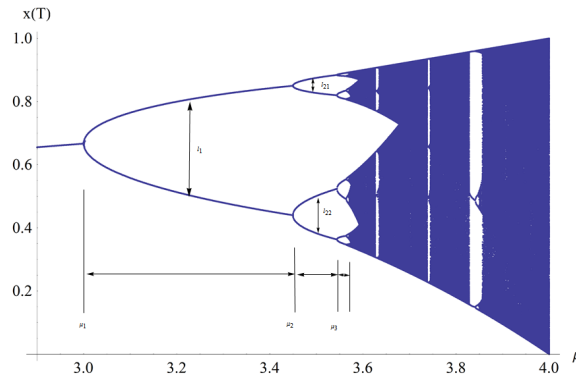
**2.2 Logistic map**

The Logistic map is a typical chaotic model, which uses the following equation for repeated iteration:

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

where,  $x_k \in (0,1)$  represents the system variable,  $0 \leq \mu \leq 4$  is the growth parameter, and  $k \in (0,1,2,\dots,n)$  is the number of iterations [Li, Liu and Liu (2019)]. The performance of the system varies with the value of  $\mu$ . When  $2.8 < \mu \leq 4$ , the obtained graph is shown in Fig. 4. Starting from  $\mu=3$ , the system has two cycles and four cycles. When  $3.569945672 < \mu \leq 4$ , the system enters a chaotic state. And the chaotic state of the Logistic map is extremely sensitive to the initial value which can be used as an ideal sequence of the secret key. This chaos is used in the chaotic encryption of the medical

images and the watermark, and their initial values are set to 0.135 and 0.2, respectively.



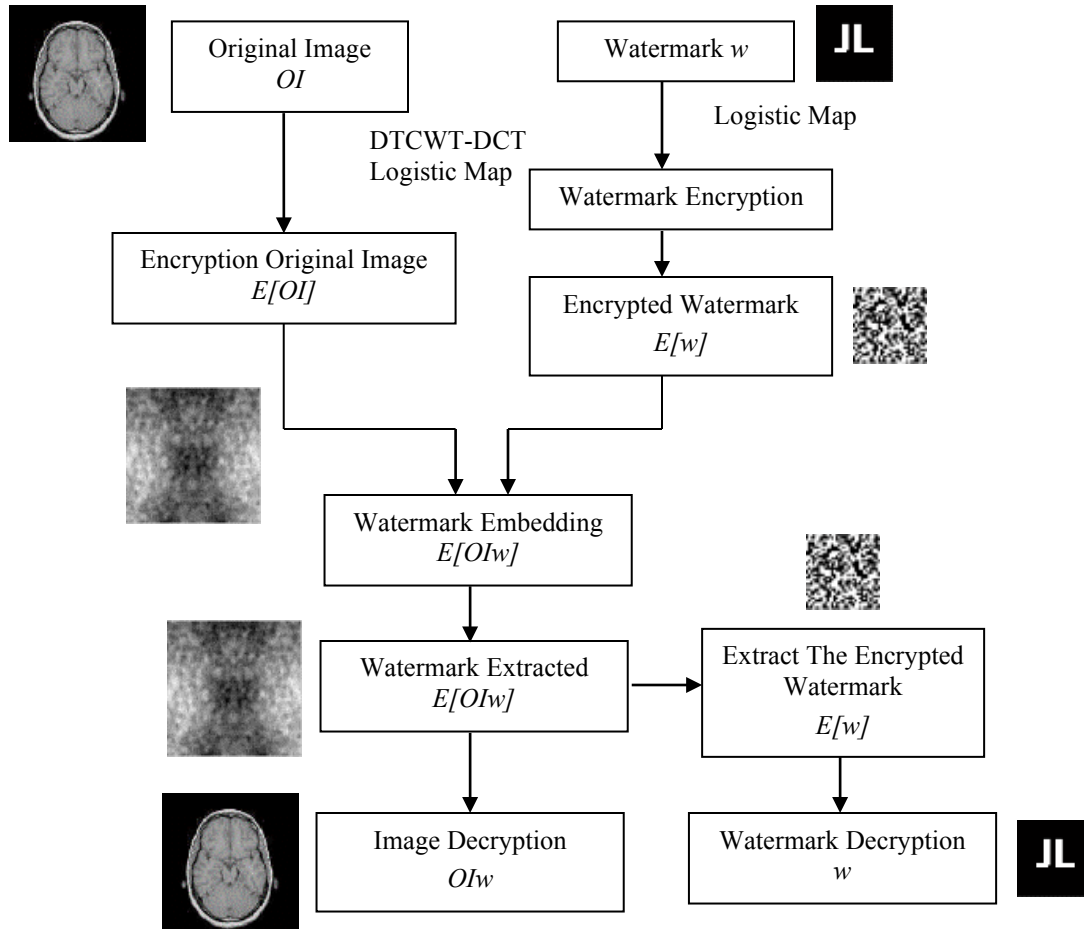
**Figure 4:** The bifurcation diagram of Logistic map

### **2.3 Homomorphic encryption**

Encryption technology plays an important role in the processing of encrypted domain signals. However, not all encryption methods are suitable for signal processing in the encryption domain. Most encryption methods, such as DES and AES, fail to maintain algebraic correspondence between plaintext and ciphertext after encryption. To solve this problem, in 1978, Rivest et al. first proposed the concept of homomorphic encryption [Naqvi, Abbasi, Hussain et al. (2018)]. That is, after performing some operation on the ciphertext encrypted by homomorphism and then decrypting it can obtain the same result by directly performing the same operation on the plain text without encryption. In this way, direct manipulation of ciphertext data can be achieved without initial decryption which provides a feasible approach to secure signal processing. Homomorphic encryption is divided into full homomorphic encryption and partial homomorphic encryption. Due to its high computational complexity and time cost, the full homomorphic encryption algorithm is not ideal in practical application. Therefore, this paper uses the Paillier cipher system to design the encryption scheme. Paillier cryptosystem is a public key cryptosystem with homomorphic and probabilistic properties, and its security has been proved.

### **3 The proposed algorithm**

We propose a robust zero-watermarking scheme for encrypted medical images, which mainly uses DTCWT-DCT transform and Logistic chaotic mapping as shown in Fig. 5. It is divided into the main stages of original medical image encryption, feature extraction and watermark encryption, watermark embedding and extraction. By using the homomorphism of the encryption system, the outputs are watermarked encrypted images after embedding the watermark.



**Figure 5:** The proposed algorithm scheme

Due to the watermark image and the original medical image are both encrypted, the embedding and extraction of the watermark can be safely performed by a third-party cloud server. Furthermore, after the users decrypted, the decryption images that meet the application requirements can be obtained.

**3.1 Medical image encryption**

In order to protect the original medical image, we carry out our watermark algorithm in the encryption domain. Fig. 6. shows the encryption scheme for original medical images. The description is as follows:

- 1) Apply two-level DTCWT transform on the original medical images to obtain the six wavelet coefficients high-frequency sub-bands in each layer of the double-tree and two low-frequency coefficients;

$$[Yl, Yh, Yscale] = dtwavexfm2(aa, 2, 'near\_sym\_b', 'qshift\_b') \tag{3}$$

2) Apply DCT transform to each wavelet sub-band coefficient to get the DCT coefficient matrix of the subband coefficient  $D(i, j)$  ;

$$D(i, j) = DCT2(Yl, Yh); \quad (4)$$

3) Obtain the encryption matrix  $C(i, j)$  by using Logistic chaotic mapping structure chaotic sequence  $X(i, j)$  , via the symbolic function  $Sgn(x)$  and  $reshape(X(i, j))$  ;

$$Sgn(x) = \begin{cases} 1, & x(n) \geq 0 \\ -1, & x(n) < 0 \end{cases} \quad (5)$$

$$X'(j) = Sgn(X(j)) \quad (6)$$

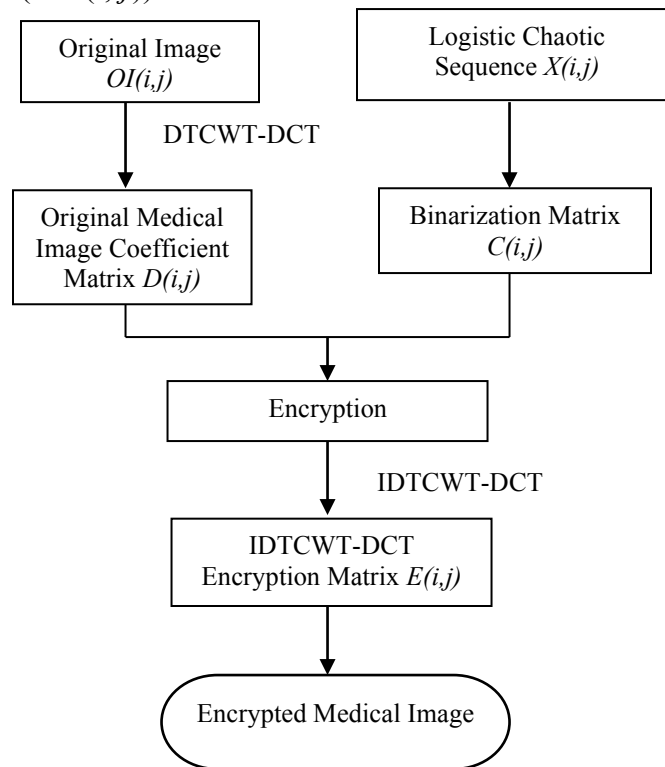
$$C(i, j) = reshape(X'(j)) \quad (7)$$

4) For binary encryption matrix  $C(i, j)$  and dtcwt-dct coefficient matrix  $D(i, j)$  , use the dot multiplication operation to obtain the encryption coefficient matrix  $ED'(i, j)$  ;

$$ED'(i, j) = D(i, j) * C(i, j) \quad (8)$$

5) IDCT transformation is performed on the encryption coefficient matrix  $ED'(i, j)$  to obtain the reconstructed encrypted sub-band wavelet coefficient matrix  $ED(i, j)$  ;

$$ED(i, j) = IDCT(ED'(i, j)) \quad (9)$$



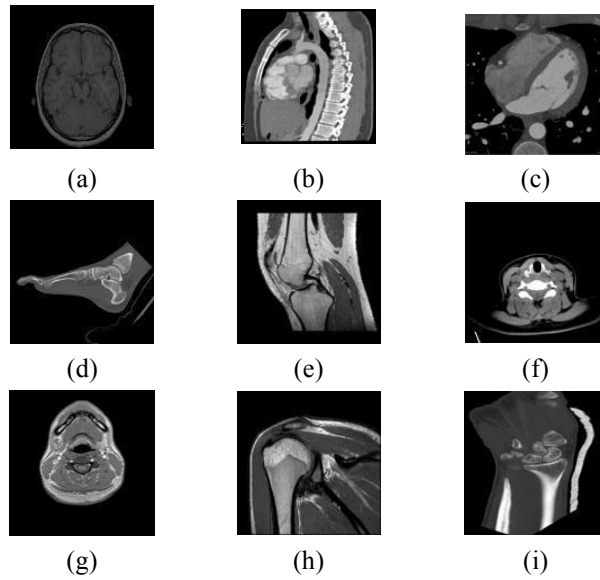
**Figure 6:** Encryption of original medical images



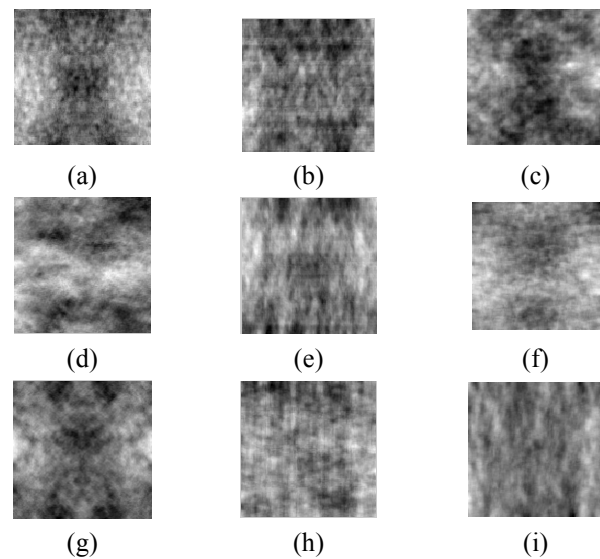
6) IDTCWT transformation is performed on the matrix  $ED(i, j)$  to obtain the encrypted medical image  $E(i, j)$ .

$$E(i, j) = IDTCWT(ED(i, j)) \tag{10}$$

As shown below, Fig. 7 is the original medical image that was randomly selected, while Fig. 8 is the corresponding medical image encrypted by DTCWT-DCT.



**Figure 7:** The original medical images: (a) Brain, (b) Arm, (c) Coronary artery, (d) Foot, (e) Knee, (f) Multi-phase pancreas, (g) Neck, (h) Shoulder, (i) Wrist



**Figure 8:** The encrypted medical images: (a) Encrypted Brain, (b) Encrypted Arm, (c)

Encrypted Coronary artery, (d) Encrypted Foot, (e) Encrypted Knee, (f) Encrypted Multi-phase pancreas, (g) En-encrypted Neck, (h) Encrypted Shoulder, (i) Encrypted Wrist

### 3.2 Feature extraction and watermark encryption

To find a visual feature vector suitable for all encrypted medical images, we randomly selected a normal human brain image of 128 pixels by 128 pixels for encryption, performed DTCWT-DCT transformation on the encrypted image, and carried out various attacks as shown in Tab. 1. By observing the low frequency coefficients of the encrypted images after transformation, we found that although the values of the low frequency coefficients of encrypted brain images after DTCWT-DCT transformation varies greatly under various attacks, their symbols remain basically unchanged. In this paper, 32 low-frequency data is selected for symbol transformation, and all coefficient values greater than zero or equal to zero are replaced by '1', and those less than zero are replaced by '0'. For convenience of explanation, the first nine bits of the data are listed in Tab. 1. Their units are all  $1.0e+04$ . In this way, we get a sequence of low-frequency coefficient symbols '101000000' of the encrypted brain image. And the symbol sequence of all the images being attacked is consistent with the original image which is equal to 1.00.

**Table 1:** Changes of DTCWT-DCT coefficients under different attacks for the encrypted original image

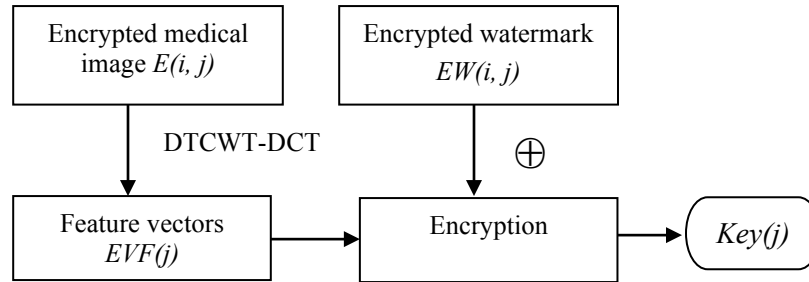
Image processing	PSNR (dB)	EI (1,1)	EI (1,2)	EI (1,3)	EI (1,4)	EI (1,5)	EI (1,6)	EI (1,7)	EI (1,8)	EI (1,9)	Sequence of coefficient signs	NC				
Original image	/	1.4509	-	0.1304	-	0.0790	-	0.0011	0.0408	-	0.3127	0.0025	-	0.0691	101000000	1.00
Gaussian noise (1%)	20.20	1.4593	-	0.1379	-	0.0801	-	0.0019	0.0383	-	0.3045	0.0036	-	0.0695	101000000	1.00
JPEG compression (4%)	23.89	1.4575	-	0.1242	-	0.0830	-	0.0083	0.0407	-	0.2985	0.0037	-	0.0730	101000000	1.00
Median filter [3x3] (10 times)	28.85	1.4463	-	0.1253	-	0.0786	-	0.0019	0.0423	-	0.3185	0.0033	-	0.0695	101000000	1.00
Scaling ( $\times 0.5$ )	/	7.2554	-	0.6499	-	0.3937	-	0.0058	0.2030	-	1.5658	0.0123	-	0.3456	101000000	1.00
Translation (5%, right)	14.39	1.4354	-	0.2417	-	0.0942	-	0.0077	0.0538	-	0.1824	0.0051	-	0.0832	101000000	1.00
Translation (4%, down)	17.35	1.4439	-	0.1305	-	0.2474	-	0.0004	0.0583	-	0.2947	0.0021	-	0.0529	101000000	1.00
Cropping (10%, Y direction)	/	1.4393	-	0.1288	-	0.1964	-	0.0015	0.0573	-	0.2076	0.0023	-	0.0488	101000000	1.00

Based on the above conclusions, we performed the same experiments on a large number of CT images and MRI images and calculated the normalized correlation coefficient values between them using their respective 32 bits symbol vectors. Tab. 2 lists the test results of the encrypted medical images which are shown in Fig. 8. It is apparent from the results that the NC values are both less than 0.5 compared with others, and their own NC values are all 1.0. Hence, the low-frequency coefficients of the encrypted medical images transformed by DTCWT-DCT can be used as the effective visual feature vectors.

**Table 2:** Values of the correlation coefficients between different images (32 bits)

	EImg1	EImg2	EImg3	EImg4	EImg5	EImg6	EImg7	EImg8	EImg9
EImg1	1.00	0.20	-0.16	0.22	-0.06	0.02	-0.07	0.42	0.40
EImg2	0.20	1.00	-0.02	0.37	0.25	-0.07	-0.25	0.02	0.31
EImg3	-0.16	-0.02	1.00	-0.06	0.24	0.02	0.28	0.11	-0.11
EImg4	0.22	0.37	-0.06	1.00	-0.14	0.42	-0.12	-0.07	0.42
EImg5	-0.06	0.25	0.24	-0.14	1.00	-0.07	0.25	0.28	0.06
EImg6	0.02	-0.07	0.02	0.42	-0.07	1.00	-0.06	-0.16	0.24
EImg7	-0.07	-0.25	0.28	-0.12	0.25	-0.06	1.00	0.37	-0.06
EImg8	0.42	0.02	0.11	-0.07	0.28	-0.16	0.37	1.00	0.11
EImg9	0.40	0.31	-0.11	0.42	0.06	0.24	-0.06	-0.06	1.00

**3.3 Watermark embedding and extraction**



**Figure 9:** Watermark embedding process

A medical image is a special type of image, which has strict requirements regarding image data integrity. Therefore, we use zero-watermark technology to complete the embedding of the watermark. In the embedding process, the watermark embedding is completed by associating the feature vector of the encrypted image with the watermark sequence  $EW(j)$ , which is described as follows:

- 1) Extract the feature vector  $EVF(j)$  from the encrypted medical image  $E(i, j)$ ;
- 2) Obtain the encrypted watermark sequence  $EW(j)$  via encrypting the original watermark;

3) Perform a XOR operation on symbol sequence  $EVF(j)$  and encrypted watermark sequence  $EW(j)$  to obtain a secret key  $Key(j)$ , and the embedding of watermark is completed.

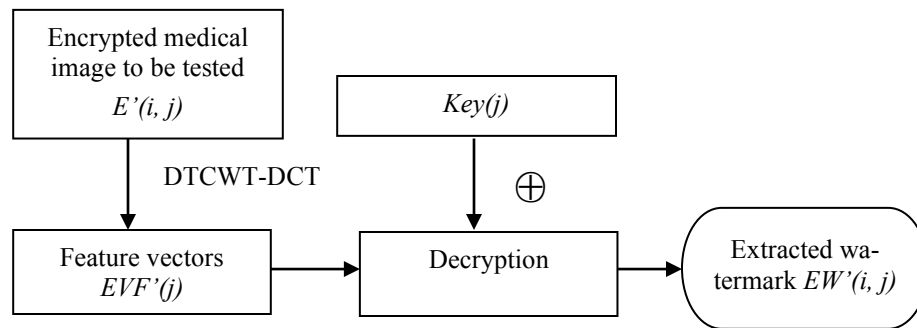
$$Key(j) = EVF(j) \oplus EW(j) \quad (11)$$

The steps to extract the watermark in ciphertext domain are as follows:

- 1) Extract the feature vector  $EVF'(j)$  of the medical image to be tested  $E'(i, j)$ ;
- 2) Perform a XOR operation on the feature vector  $EVF'(j)$  and key sequence  $Key(j)$  to obtain the extracted watermark  $EW'(j)$ ;

$$EW'(j) = EVF'(j) \oplus Key(j) \quad (12)$$

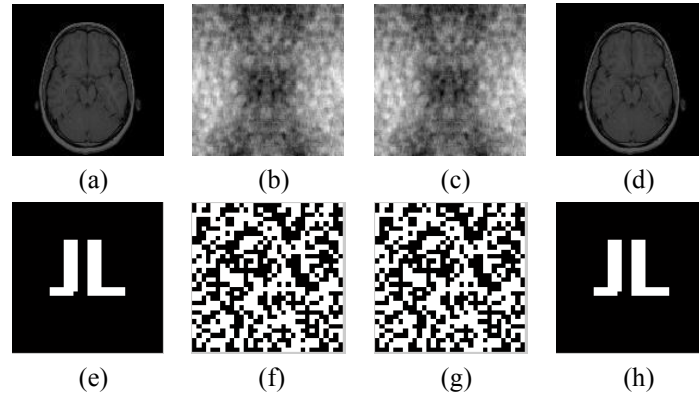
- 3) The extracted encrypted watermark is decrypted to obtain the restored watermark.



**Figure 10:** Watermark extraction process

#### 4 Simulation and analysis

Based on matlab 2016, all the encrypted medical images in randomly selected in Fig. 8 were simulated. The sizes of the selected encrypted medical images are 128 pixels×128 pixels, and the watermark image is 32 pixels×32 pixels which is selected as a meaningful image. Taking the image of Fig. 7(a) as an example, the proposed algorithm is used to encrypt the image and the watermark, generating the encrypted image embedded with watermark and their decryption effect images. As is apparent from Fig. 11, the encrypted image and the watermark are identical to the original image without being attacked, NC=1.0. After chaotic encryption, the medical image and the watermark can no longer distinguish the initial shape and the content. Different initial values enhance the security of the encryption algorithm.



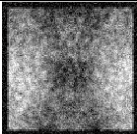

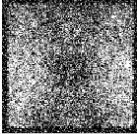
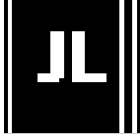
**Figure 11:** The medical image and watermark in the encrypted domain: (a) Original medical image (b) Encrypted medical image; (c) Encrypted watermarked medical image; (d) Decrypted watermarked medical image; (e) Original watermark; (f) Chaotic encryption watermark; (g) Extracted watermark; (h) Decrypted watermark

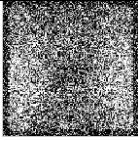
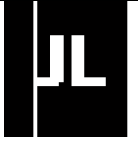

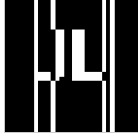
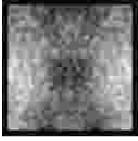

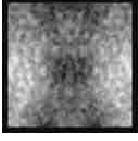

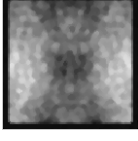
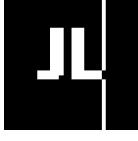
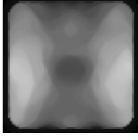

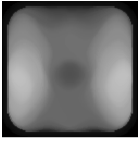
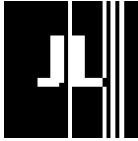
Then, we attacked all the encrypted medical images in Fig. 8 and measured the extracted watermarks with PSNR values and NC values to verify the robustness of the algorithm. The results of their attacks are as follows. Although we have tested all the images, for the sake of illustration, the attacked results are analyzed with Fig.ss 8 (a) as an example.

**4.1 Conventional attacks**

The performance of the tested encrypted medical image under conventional attacks are shown in Tab. 3. Observing the data of Tab. 3, with Gaussian noise, JPEG compression and median filtering attacks intensity increasing, the PSNR values and the NC values of the watermarked encrypted medical images showed a decreasing trend. Even when the Gaussian noise intensity reached 25%, JPEG compression reached as low as 4%, and the median filtering size reached 11 x 11, in the case of 10 filtering times, although the encrypted medical images have undergone great changes, their average NC value is still as high as 0.85, which demonstrates good robustness.

**Table 3:** The PSNR and NC values under conventional attacks

Common attacks	Intensity of attacks	PSNR	NC
Gaussian noise	1%	 PSNR=20.20 dB	 NC=1.00
	10%		

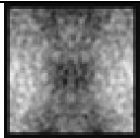

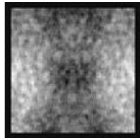

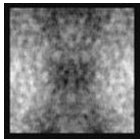
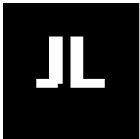
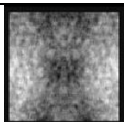

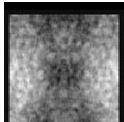

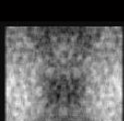

		PSNR=11.44 dB	NC=0.90
	25%		
		PSNR=9.01 dB	NC=0.86
JPEG compression	4%		
		PSNR=23.63 dB	NC=0.84
	6%		
		PSNR=26.09 dB	NC=0.90
	15%		
		PSNR=29.78 dB	NC=1.00
Median filter (10 times)	[3×3]		
		PSNR=28.85 dB	NC=0.94
	[7×7]		
		PSNR=21.99 dB	NC=0.88
	[11×11]		
		PSNR=19.21 dB	NC=0.84

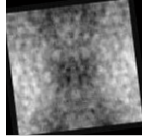
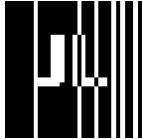
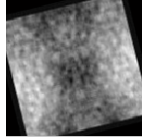

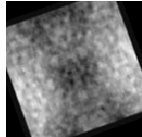

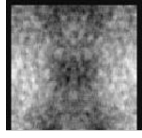

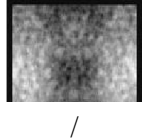

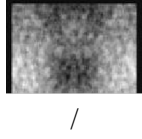

#### 4.2 Geometrical attacks

Tab. 4 shows the PSNR and NC values of watermarked encrypted medical images under geometric attacks and their corresponding images. When the watermarked encrypted medical image was translated down by 17%, nearly one-fifth of the image watermark was

lost. The watermark can still be accurately extracted, and NC=0.61. When it is attacked counterclockwise, rotated by 20 degrees and cut by 1/3 on the Y-axis, the watermark can still be clearly extracted. In addition, almost 100% of the watermark of encrypted medical images can be extracted, which means almost no loss at all under the scaling attacks. These data results show that the proposed algorithm is robust to geometric attacks, and it has a wide range of variabilities and high NC values.

**Table 4:** The PSNR and NC values under geometrical attacks

Geometrical attacks	Intensity of attacks	PSNR	NC
Scaling	×0.5	 /	 NC=1.00
	×1.5	 /	 NC=1.00
	×8.0	 /	 NC=1.00
Translation (down)	3%	 PSNR =19.45 dB	 NC=0.90
	7%	 PSNR =16.19 dB	 NC=0.86
	17%	 PSNR =13.04 dB	 NC=0.61

Rotation (counterclockwise)	7°		
		PSNR =15.37 dB	NC=0.65
	14°		
		PSNR =13.33 dB	NC=0.61
	20°		
		PSNR =12.36 dB	NC=0.53
Cropping (Y direction)	5%		
		/	NC=0.90
	24%		
		/	NC=0.83
	30%		
		/	NC=0.67

To verify the homomorphism of the proposed algorithm, we compared the quality of the image after the attacks and the extracted NC values of both the watermarked unencrypted medical image and the watermarked encrypted image in Tab. 5. The experimental data results are basically consistent in the encrypted and unencrypted domains, indicating that the encryption algorithm we use has good homomorphism.

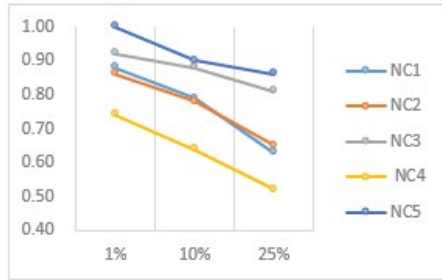


**Table 5:** The PSNR and NC values in DTCWT-DCT plaintext and encrypted domain

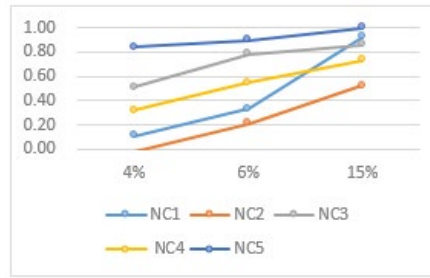
Attack Types	Intensity	PSNR/dB		NC	
		Plaintext Domain	Encrypted Domain	Plaintext Domain	Encrypted Domain
Gaussian noise	1%	14.17	20.20	0.97	1.00
	5%	7.70	13.75	0.91	0.93
	25%	3.64	9.01	0.82	0.86
JPEG compression	4%	19.56	23.63	0.91	0.84
	9%	22.67	27.15	0.81	0.93
	15%	23.96	25.70	0.81	1.00
Median filter (10 times)	[7×7]	18.92	21.99	0.72	0.88
	[9×9]	17.99	20.60	0.68	0.82
	[11×11]	16.82	19.21	0.65	0.84
Rotation (counterclockwise)	5°	18.17	16.65	0.42	0.61
	10°	15.45	14.31	0.30	0.61
	20°	14.36	12.36	0.27	0.53
Scaling	×0.2	-	-	0.75	0.63
	×0.8	-	-	0.93	0.82
	×2.0	-	-	1.00	1.00
Translation (down)	5%	14.35	16.77	0.94	0.90
	10%	13.68	15.16	0.91	0.83
	15%	12.81	13.49	0.73	0.61
Cropping (Y direction)	5%	-	-	0.75	0.90
	15%	-	-	1.00	0.83
	30%	-	-	0.70	0.67

**4.3 Algorithm comparison**

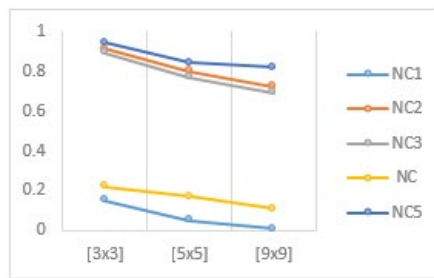
In order to further verify the robustness of the proposed algorithm, especially under geometric attacks, we replaced the encrypted medical image with a ‘Luna’ image to mask the difference between the results of selecting different samples. Then, the proposed algorithm is compared with the existing algorithm [Zear, Singh and Kumar (2018); Thanki, Borra, Dwivedi et al. (2017); Nematzadeh, Enayatifar, Motameni et al. (2018); Laiphrakpam and Khumanthem (2017)]. Their comparison results are shown in Tab. 6-Tab. 7 and Figs. 12-18, respectively. Observing this comparative data, we can find that although the proposed algorithm performs slightly inferiorly to the algorithm proposed by Nematzadeh et al. [Nematzadeh, Enayatifar, Motameni et al. (2018)] under the scaling attacks, it is clearly superior to the existing algorithm in both conventional attacks and geometric attacks in general. Besides, the proposed algorithm encrypted the medical image itself, which enhanced the security of the algorithm.



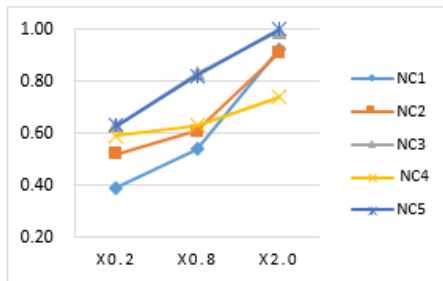
**Figure 12:** The NC data of different algorithms under Gaussian Noise attacks



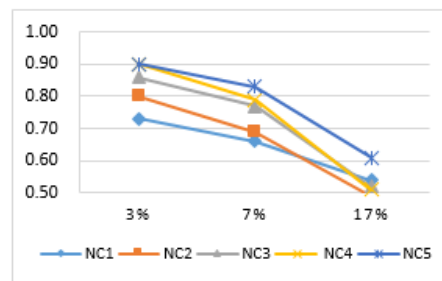
**Figure 13:** The NC data of different algorithms under JPEG attacks



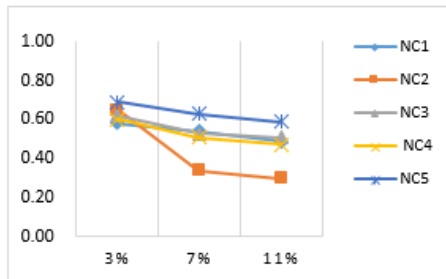
**Figure 14:** The NC data of different algorithms under Median Filter (10 times) attacks



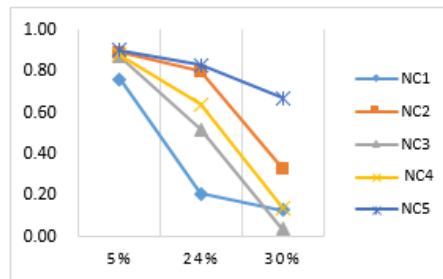
**Figure 15:** The NC curves of different algorithms under Scaling attacks



**Figure 16:** The NC curves of different algorithms under Down Translation attacks



**Figure 17:** The NC curves of different algorithms under Right Translation attacks



**Figure 18:** The NC curves of different algorithms under Cropping attacks

**Table 6:** Comparison values of different algorithms under conventional attacks

Conventional Attacks	Intensity of attacks	Zear et al. (2018)	Thanki et al. (2017)	Nematzadeh et al. (2018)	Laiphrakpam et al. (2017)	Proposed algorithm
		NC1	NC2	NC3	NC4	NC5
Gaussian Noise	1%	0.88	0.86	0.92	0.74	1.00
	10%	0.79	0.78	0.88	0.64	0.90
	25%	0.63	0.65	0.81	0.52	0.86
JPEG Compression	4%	0.11	-0.02	0.51	0.32	0.84
	6%	0.33	0.21	0.78	0.55	0.90
	15%	0.92	0.52	0.86	0.73	1.00
Median Filter (10 times)	[3×3]	0.15	0.91	0.89	0.22	0.94
	[5×5]	0.05	0.80	0.77	0.17	0.84
	[9×9]	0.01	0.72	0.69	0.11	0.82

**Table 7:** Comparison values of different algorithms under geometrical attacks

Geometrical Attacks	Intensity of attacks	Zear et al. (2018)	Thanki et al. (2017)	Nematzadeh et al. (2018)	Laiphrakpam et al. (2017)	Proposed algorithm
		NC1	NC2	NC3	NC4	NC5
Scaling	×0.2	0.39	0.52	0.63	0.59	0.63
	×0.8	0.54	0.61	0.83	0.63	0.82
	×2.0	0.92	0.91	0.99	0.74	1.00
Translation (Down)	3%	0.73	0.80	0.86	0.90	0.90
	7%	0.66	0.69	0.77	0.79	0.83
	17%	0.54	0.49	0.52	0.51	0.61
Translation (Right)	3%	0.58	0.65	0.62	0.60	0.69
	7%	0.54	0.34	0.53	0.51	0.63
	11%	0.49	0.30	0.51	0.47	0.59
Cropping (Y direction)	5%	0.76	0.89	0.87	0.88	0.90
	24%	0.21	0.80	0.52	0.64	0.83
	30%	0.13	0.33	0.04	0.14	0.67

Therefore, the algorithm presented in this paper is outstanding in all kinds of attacks, in particular solving the problem that existing algorithms cannot balance geometric attacks and security robustness. It has strong resistance to geometric attacks and exhibits good robustness.

**5 Conclusions**

This paper proposed a new robust watermarking algorithm for encrypted medical images based on DTCWT-DCT. The security of medical image transmission is enhanced by encrypting the medical image itself and setting different initial values of chaos. It used the low-frequency coefficient of the DTCWT-DCT transform domain of the encrypted medical

image as its feature vector, performed logical operations with the chaotic encrypted watermark to generate the secret key to realize the embedding and extraction of the encrypted medical image. Using the homomorphism of the encryption algorithm, the watermark can be extracted easily without the original image or decryption. The simulation results show that the proposed algorithm can solve the contradiction between robustness and invisibility well, and is robust to both conventional attacks and geometric attacks.

**Acknowledgement:** This work is supported by the Key Research Project of Hainan Province [ZDYF2018129], the Higher Education Research Project of Hainan Province (Hnky2019-73), the National Natural Science Foundation of China [61762033], the Natural Science Foundation of Hainan [617175], the Special Scientific Research Project of Philosophy and Social Sciences of Chongqing Medical University [201703] and the Key Research Project of Haikou College of Economics [HJKZ18-01].

## References

- Avudaiappan, T.; Balasubramanian, R.; Pandiyan, S. S.; Saravanan, M.; Lakshmanaprabu, S. K. et al.** (2018): Medical image security using dual encryption with oppositional based optimization algorithm. *Journal of Medical Systems*, vol. 42, no. 11, pp. 208-220.
- Bamal, R.; Kasana, S. S.** (2018): Slantlet based hybrid watermarking technique for medical images. *Multimedia Tools and Applications*, vol. 77, no. 10, pp. 12493-12518.
- Bouslimi, D.; Bellafqira, R.; Coatrieux, G.** (2016): Data hiding in homomorphically encrypted medical images for verifying their reliability in both encrypted and spatial domains. *38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 2496-2499.
- Cao, W. J.; Zhou, Y. C.; Chen, C. L. P.; Xia, L. M.** (2017): Medical image encryption using edge maps. *Signal Processing*, vol. 132, pp. 96-109.
- Chen, Y. Y.; Yin, B. X.; He, H. J.; Yan, S.; Chen F. et al.** (2018): Reversible data hiding in classification-scrambling encrypted-image based on iterative recovery. *Computers, Materials & Continua*, vol. 56, no. 2, pp. 299-312.
- Dai, Y.; Wang, H. Z.; Zhou, Z. X.; Jin, Z. Y.** (2016): Research on medical image encryption in telemedicine systems. *Technology and Health Care*, vol. 24, no. 2, pp. 435-442.
- Elhoseny, M.; Ramirez-Gonzalez, G.; Abu-Elnasr, O. M.; Shawkat, S. A.; Arunkumar, N. et al.** (2018): Secure medical data transmission model for Iot-based healthcare systems. *IEEE Access*, vol. 70, pp. 20596-20608.
- Fan, T. Y.; Chao, H. C.; Chieu, B. C.** (2019): Lossless medical image watermarking method based on significant difference of cellular automata transform coefficient. *Signal Processing-Image Communication*, vol. 70, pp. 174-183.
- Ismail, S. M.; Said, L. A.; Radwan, A. G.; Madian, A. H.; Abu-Elyazeed, M. F.** (2018): Generalized double-humped logistic map-based medical image encryption. *Journal of Advanced Research*, vol. 10, pp. 85-98.

**Kavitha, V.; Palanisamy, C.; Sureshkumar, T.** (2018): Robust and secured medical image watermarking using Daub4 and CoAST transforms. *Journal of Medical Imaging and Health Informatics*, vol. 8, no. 9, pp. 1857-1864.

**Laiphrakpam, D. S.; Khumanthem, M. S.** (2017): Medical image encryption based on improved ElGamal encryption technique. *Optik*, vol. 147, pp. 88-102.

**Lakshmi, C.; Thenmozhi, K.; Rayappan, J. B. B.; Amirtharajan, R.** (2018): Encryption and watermark-treated medical image against hacking disease-an immune convention in spatial and frequency domains. *Computer Methods and Programs in Biomedicine*, vol. 159, pp. 11-21.

**Lavanya, A.; Natarajan, V.** (2012): Watermarking patient data in encrypted medical images. *Sadhana-Academy Proceedings in Engineering Sciences*, vol. 37, no. 6, pp. 723-729.

**Li, R. Z.; Liu, Q.; Liu, L. F.** (2019): Novel image encryption algorithm based on improved logistic map. *IET Image Processing*, vol. 13, no. 1, pp. 125-134.

**Liu, Y. L.; Qu, X. X.; Xin, G. J.** (2016): A ROI-based reversible data hiding scheme in encrypted medical images. *Journal of Visual Communication and Image Representation*, vol. 39, pp. 51-57.

**Mothi, R.; Karthikeyan, M.** (2019): Protection of bio medical iris image using watermarking and cryptography with WPT. *Measurement*, vol. 136, pp. 67-73.

**Naqvi, N.; Abbasi, A. T.; Hussain, R.; Khan, M. A.; Ahmad, B.** (2018): Multilayer partially homomorphic encryption text steganography (MLPHE-TS): a zero steganography approach. *Wireless Personal Communications*, vol. 103, no. 2, pp. 1563-1585.

**Nematzadeh, H.; Enayatifar, R.; Motameni, H.; Guimaraes, F. G.; Coelho, V. N.** (2018): Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. *Optics and Lasers in Engineering*, vol. 110, pp. 24-32.

**Qasim, A. F.; Meziiane, F.; Aspin, R.** (2018): Digital watermarking: applicability for developing trust in medical imaging workflows state of the art review. *Computer Science Review*, vol. 27, pp. 45-60.

**Rai, A.; Singh, H. V.** (2017): SVM based robust watermarking for enhanced medical image security. *Multimedia Tools and Applications*, vol. 76, no. 18, pp. 18605-18618.

**Selvakumar, K.; Jerome, J.; Rajamani, K.** (2016): Robust face identification using DTCWT and PCA subspace based sparse representation. *Multimedia Tools and Applications*, vol. 75, no. 23, pp. 16073-16092.

**Soualmi, A.; Altı, A.; Laouamer, L.** (2018): A new blind medical image watermarking based on weber descriptors and arnold chaotic map. *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 7893-7905.

**Thanh, T. M.; Tanaka, K.** (2017): An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information. *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13455-13471.

**Thanki, R.; Borra, S.; Dwivedi, V.; Borisagar K.** (2017): An efficient medical image watermarking scheme based on FDCuT-DCT. *Engineering Science and Technology, an International Journal*, vol. 20, no. 4, pp. 1366-1379.

**Vengadapurvaja, A. M.; Nisha, G.; Aarthy, R.; Sasikaladevi, N.** (2017): An efficient homomorphic medical image encryption algorithm for cloud storage security. *Procedia Computer Science*, vol. 115, pp. 643-650.

**Xiong, L.; Xu, Z.; Shi, Y. Q.** (2018): An integer wavelet transform based scheme for reversible data hiding in encrypted images. *Multidimensional Systems and Signal Processing*, vol. 29, no. 3, pp. 1191-1202.

**Zear, A.; Singh, A. K.; Kumar, P.** (2018): A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimedia Tools and Applications*, vol. 77, no. 4, pp. 4863-4882.

**Zebbiche, K.; Khelifi, F.; Loukhaoukha, K.** (2018): Robust additive watermarking in the DTCWT domain based on perceptual masking. *Multimedia Tools and Applications*, vol. 77, no. 16, pp. 21281-21304.