Computers, Materials & Continua CMC, vol.61, no.1, pp.363-378, 2019

A Robust Zero-Watermarking Based on SIFT-DCT for Medical Images in the Encrypted Domain

Jialing Liu[1], Jingbing Li[1, 2, *], Yenwei Chen[3], Xiangxi Zou[1], Jieren Cheng[1, 2], Yanlin Liu[1] and Uzair Aslam Bhatti[1,2]

Abstract: Remote medical diagnosis can be realized by using the Internet, but when transmitting medical images of patients through the Internet, personal information of patients may be leaked. Aim at the security of medical information system and the protection of medical images, a novel robust zero-watermarking based on SIFT-DCT (Scale Invariant Feature Transform-Discrete Cosine Transform) for medical images in the encrypted domain is proposed. Firstly, the original medical image is encrypted in transform domain based on Logistic chaotic sequence to enhance the concealment of original medical images. Then, the SIFT-DCT is used to extract the feature sequences of encrypted medical images. Next, zero-watermarking technology is used to ensure that the region of interest of medical images are not changed. Finally, the robust of the algorithm is evaluated by the correlation coefficient between the original watermark and the attacked watermark. A series of attack experiments are carried out on this method, and the results show that the algorithm is not only secure, but also robust to both traditional and geometric attacks, especially in clipping attacks.

Keywords: Robustness, CT Image, zero-watermarking, SIFT-DCT, encrypted domain.

1 Introduction

With the development of science and technology, big data and cloud storage have become a hot topic. Various data processing methods and remote transmission schemes have been proposed. And cloud storage and data processing also have potential advantages in smart healthcare. In case Diagnosis, such as Feature Selection Method Based on Class Discriminative Degree for Intelligent Medical Diagnosis [Fang, Cai, Sun et al. (2018)], a decision support system that can assist Medical staff to diagnose and treat diseases can be established through Feature extraction of Medical images, which can improve efficiency. But it will encounter the information security question in the data transmission. Medical images contain some sensitive information, which may be leaked

[1] College of Information Science and Technology, Hainan University, Haikou, 570228, China.

[2] State key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou, 570228, China.

[3] Graduate School of Information Science and Engineering, Ritsumeikan University, Shiga, Japan.

[*] Corresponding Author: Jingbing Li. Email: Jingbingli2008@hotmail.com.

or tampered with. Digital watermarking technology is a possible information protection system [Guo, Zheng and Huang (2015)], which provides a way to embed unique code in each original image of distributed content. According to the literatures published in recent years, the digital watermarking technology can be grouped into two classes: The watermarking Information is directly embedded into the digital carrier, such as Information hiding in medical images: a robust medical image watermarking system for E-healthcare [Parah, Sheikh, Ahad et al. (2017)]. The watermarking is embedded in different areas of the carrier, but the medical image is sensitive, and the selected location is crucial. The other method is blind watermarking [Fazlali, Samavi, Karimi et al. (2017)], which does not need to use the original data and only needs the key to detect. It will not destroy the original medical data and not affect the judgment of doctors. For example, Lang et al. [Lang and Zhang (2014)] have proposed a new blind digital image watermarking algorithm based on fractional Fourier transform (FRFT). In Parah et al. [Parah, Sheikh, Loan et al. (2016)], the authors have proposed a new DCT domain blind watermarking algorithm. These methods associate the watermark with the target image to reduce the damage to the original data. Though the watermark embedding method has been improved, they did not protect the privacy of the original image, which is an important factor for medical images.

So privacy protection is also a challenge for smart medicine. Large amounts of medical data are exposed online during transmission. Among the many encryption methods, the most interesting aspect of homomorphic encryption scheme is focused on data processing security [Han and Li (2016); Abdallah, Faragallah, Elsayed et al. (2016)]. Algebraic relations between plaintext are preserved in the encryption domain, providing an appropriate method for secure signal processing. That is, someone else can work with encrypted data, but the process does not leak any of the original content. At the same time, the user with the key decrypts the processed data, resulting in the original data. This encryption has a huge impact in the cloud age. In addition, feature extraction is also a key link [Lv and Wang (2012); Li, Wang and Liu (2012)]. It is mainly divided into global features, such as the classical algorithm Discrete Cosine Transformation(DCT) [Das, Panigrahi, Sharma et al. (2014); Wu, Li, Tu et al. (2018)], and local features, such as Scale Invariant Feature Transform (SIFT) [Priyatham, Nilkanta and Arijit (2014); Han, Zhou, Xu et al. (2017); Zhao, Jiang and Hong (2014); Liu, Li and Liu (2011); Dai and Tian (2014)]. The SIFT algorithm can generate a large number of features even with a small amount of data, and has stability to rotation and translation, which is of profound significance to geometric attacks.

Considering the above mentioned problems, this paper proposes a robust zero-watermarking algorithm based on SIFT-DCT for encrypting medical images in the transform domain. In the transform domain, the original medical image is encrypted with the aid of chaotic mapping. Then feature of the encrypted medical image is extracted with SIFT-DCT. Finally, the correlation coefficients are calculated to evaluate the robustness of the algorithm. This algorithm has the following advantages: (1) It protects the privacy of original medical images through encryption; (2) The zero watermarking technology will not change the original medical images; (3) The feature sequences extracted by this algorithm are more robust to geometrical attacks.

This paper is organized as follows. The theoretical basis of data processing is introduced in the second part. The block diagram of image encryption is discussed in the third part, and the process of watermark is investigated in the fourth part. The simulation results are carried out and analyzed in the fifth part. The sixth part gives the conclusion of the paper.

2 Feature extraction and encryption methods

2.1 Scale invariant feature transform (SIFT)

SIFT is an algorithm for local feature extraction, and its subtlety lies in the adoption of gaussian difference pyramid (see Fig. 1(a)). SIFT realizes feature extraction mainly by three processes: (1) Extract key points, as show in Fig. 1(b); (2) Add detailed information (local features) to the key points and get the feature vector (see Fig. 1(c)).

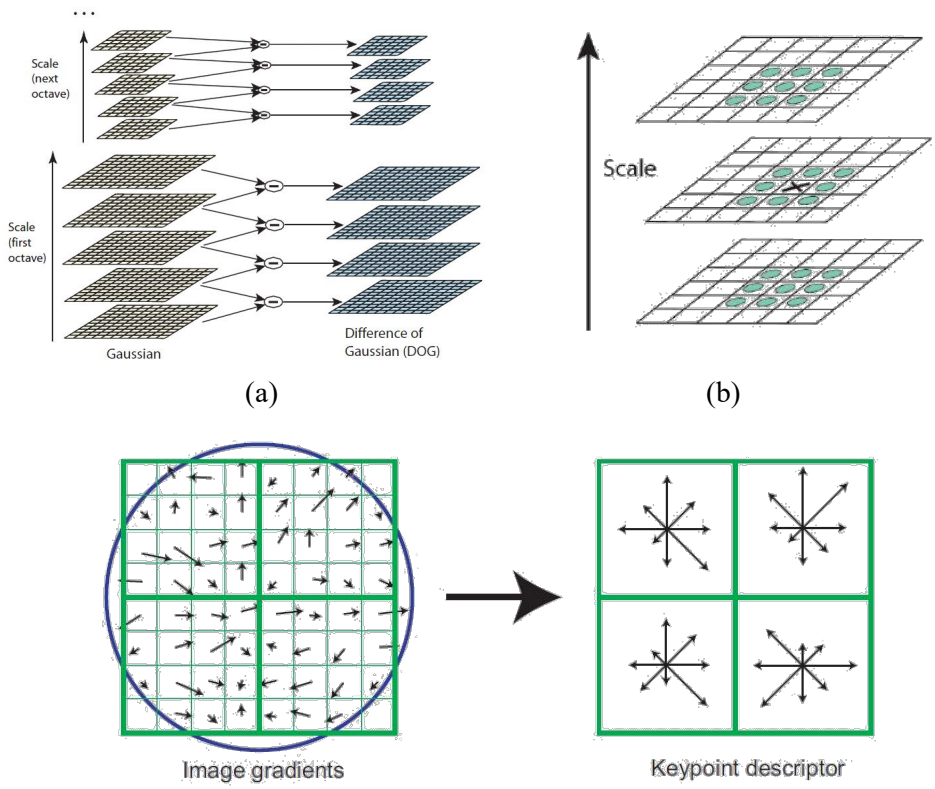
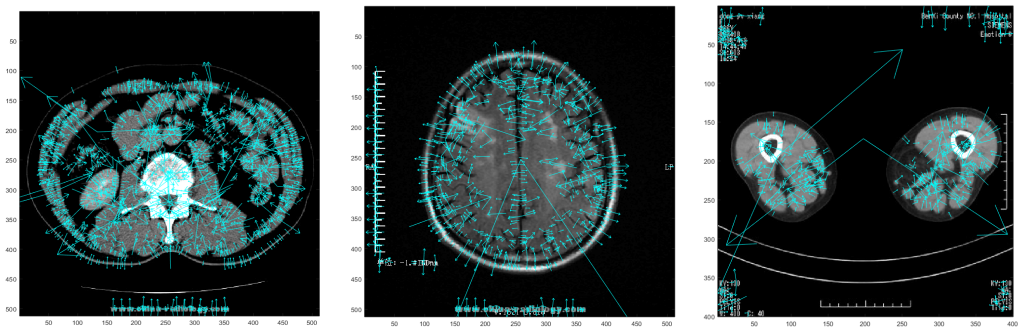


Figure 1: (a) Gaussian pyramid and DOG pyramid; (b) Extract SIFT extreme points; (c) SIFT feature vector generation

SIFT feature is a local feature of the image. Its advantages are invariant to rotation, scale scaling, brightness changes, as well as a certain degree of stability to view changes, affine transformation and noise. It is suitable for fast and accurate matching in massive feature database. It is also multidimensional, and even a few objects can produce a large number

of SIFT feature. The different original medical images have found many key points after SIFT (see Fig. 2). After extracting the medical image features by SIFT, the feature matrix is compressed by DCT to extract the feature sequences. the SIFT-DCT is the improvement of feature extraction algorithm in this study. Combining global feature and local feature, a more robust feature sequence is extracted.

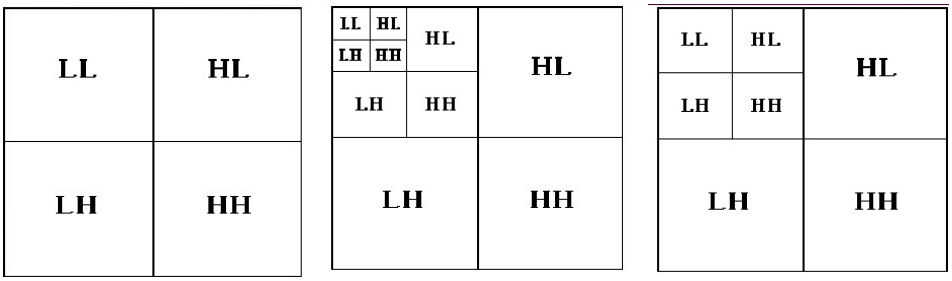


(a) (b) (c)

Figure 2: Key points of different original medical images after SIFT (a) Abdominal CT image, (b) Brain CT image, (c) CT image of leg

2.2 The discrete wavelet transform (DWT)

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, 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 diagram is shown as Fig. 3.



(a) (b) (c)

Figure 3: The image in DWT (a) Single Level Decomposition, (b) Two-Level Decomposition, (c) Three Level Decomposition

2.3 The discrete cosine transform (DCT)

The DCT is a classical global feature extraction transform. It uses only real numbers and concentrates most of its energy on the low frequencies. It is widely used in the field of image processing.

The DCT transform formula for N×N images is as follows:

$$F(u,v) = C(u) \bullet C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \bullet \cos\left[\frac{(x+0.5)\pi}{N} \bullet u\right] \bullet \cos\left[\frac{(y+0.5)\pi}{N} \bullet v\right] \quad (1)$$

$$C(v) = \begin{cases} \sqrt{\frac{1}{N}}, & u = 0 \\ \sqrt{\frac{2}{N}}, & u \neq 0 \end{cases} \quad (2)$$

where f (x, y) is the pixel value, F (u, v) is the 2D-DCT transform coefficients for f (x, y).

2.4 Logistic mapping

Logistic mapping is widely used in secure communication. Logistic mapping works in a chaotic state, that is to say, the sequence generated by the initial condition X0 under the action of Logistic mapping is non-periodic and non-convergent. Outside this range, the resulting sequence must converge to a particular value. The mathematical formula is as follows:

$$x_{k+1} = \mu \cdot x_k \cdot (1 - x_k) \quad (3)$$

where the range of x_k is 0 to 1, 0<μ<=4; besides, when 3.5699456<μ<=4, the logistic map gets a chaotic state and the chaotic sequence can be used as an ideal key sequence.

3 The encryption of medical image

Homomorphic encryption is used in medical images to better protect patient privacy and has a profound impact on future development. In this section, we propose a robust zero-watermarking scheme for the image in the encrypted domain. DWT and DCT are combined to encrypt the original image with chaotic mapping in Fig. 4.

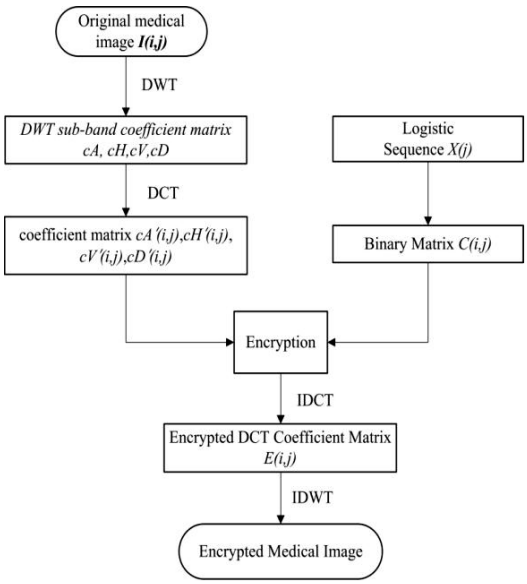


Figure 4: Encryption scheme of original medical images

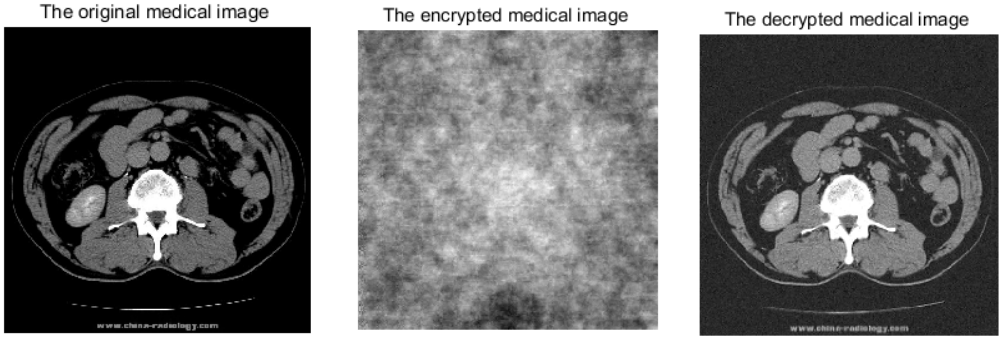
Here are main steps:

Step 1. Transform the original image using DWT-DCT.

Step 2. Generating binary sequences through chaotic mapping.

Step 3. The chaos sequence and the transformed coefficient matrix are taken as the dot product.

Step 4. Perform inverse DCT (IDCT) and inverse DWT (IDWT) to obtain encrypted medical images (see Fig. 5).



(a) (b) (c)

Figure 5: The medical image in the encrypted domain: (a) The original medical image; (b) The encrypted medical image; (c) The decrypted medical image

4 Zero watermarking algorithm

Compared with traditional embedded watermarking methods, the zero-watermarking can better guarantee the original information, which is of great significance in medical image and is beneficial to improve the robustness of algorithm. This section mainly introduces watermarking embedding and extraction. The robustness of the algorithm is evaluated by the correlation coefficient between the original watermark and the attacked watermark.

4.1 Watermarking embedding

The watermarking embedding process is shown in Fig. 6. Here are main steps:

Step 1. Transform the encrypted CT image using SIFT-DCT.

Step 2. Select the transform coefficient (4×8).

Step 3. Obtain a 32-bit binary feature sequence of the medical image.

Step 4. The original watermarking is encrypted by generating a chaos sequence.

Step 5. Generat the key sequence of watermarking extraction through XOR operation.

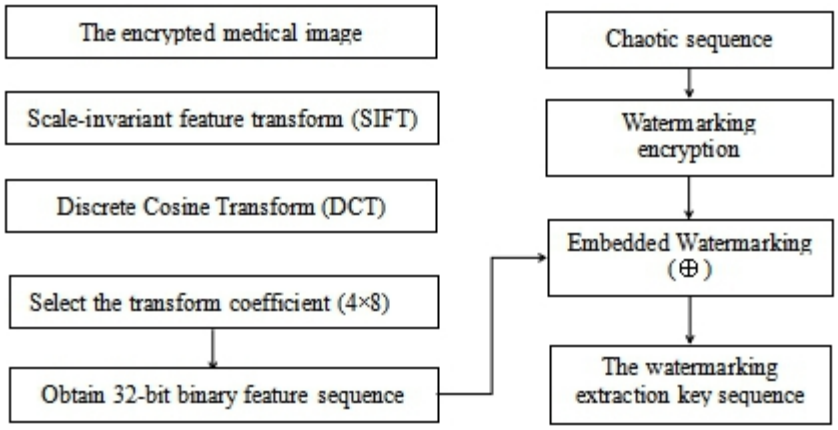


Figure 6: The watermarking embedding process

4.2 Watermarking extraction

The watermarking extraction process is shown in Fig. 7. The specific steps are as follows:

Step 1. Transform the attacked encrypted CT image using SIFT-DCT.

Step 2. Using the same method as embedding to obtain the 32-bit binary feature sequence of attacked CT image.

Step 3. Let the binary feature sequence of attacked medical image XOR the watermarking extraction key sequence.

Step 4. Inverse the scramble watermarking image.

Step 5. Calculate the correlation coefficient between the original watermarking and the attacked watermarking.

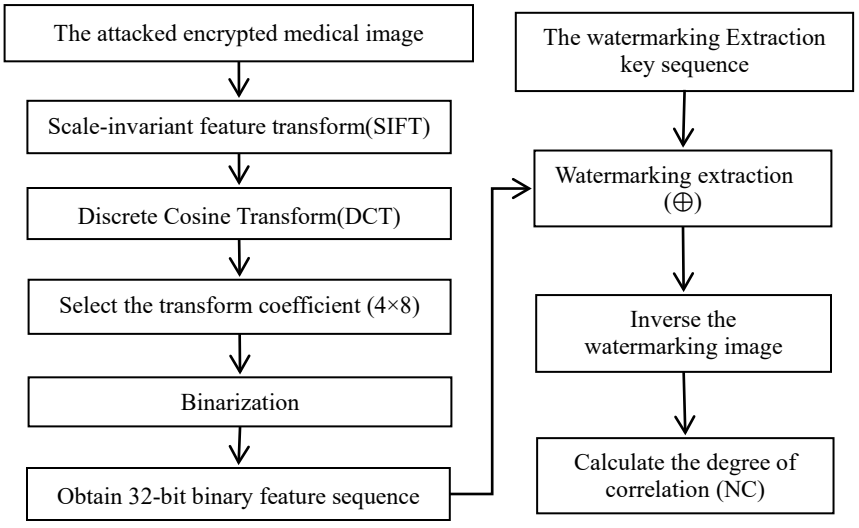


Figure 7: The watermarking extraction process

5 Experiments

We use the abdominal CT image (see Fig. 8(a)) as the research object in the experiment. Firstly, the original CT image is encrypted in the transform domain (DWT-DCT), and then the features of the encrypted medical image are extracted based on SIFT-DCT algorithm. The selected watermarking is a 32-bit image, so a 4-by-8 module is selected in the encrypted image to obtain a 32-bit binary feature sequence. The robustness of the proposed algorithm is evaluated by calculating the correlation of feature sequences between the original watermark and the attacked watermark, that is the value of NC. NC value is between 0 and 1, where 1 means no change. At this time, the algorithm is the best robust. In addition, a large number of experimental studies have shown that when the NC value is greater than 0.5, the embedded watermarking can still be extracted, so here we believe that the algorithm is robust when the NC value is greater than 0.5. The Fig. 8(b) shows the encrypted medical image under no attacks, and the Fig. 8(c) shows the key points of the encrypted medical image after SIFT. At this time, the NC value is 1.0 (see Fig. 8(d)).

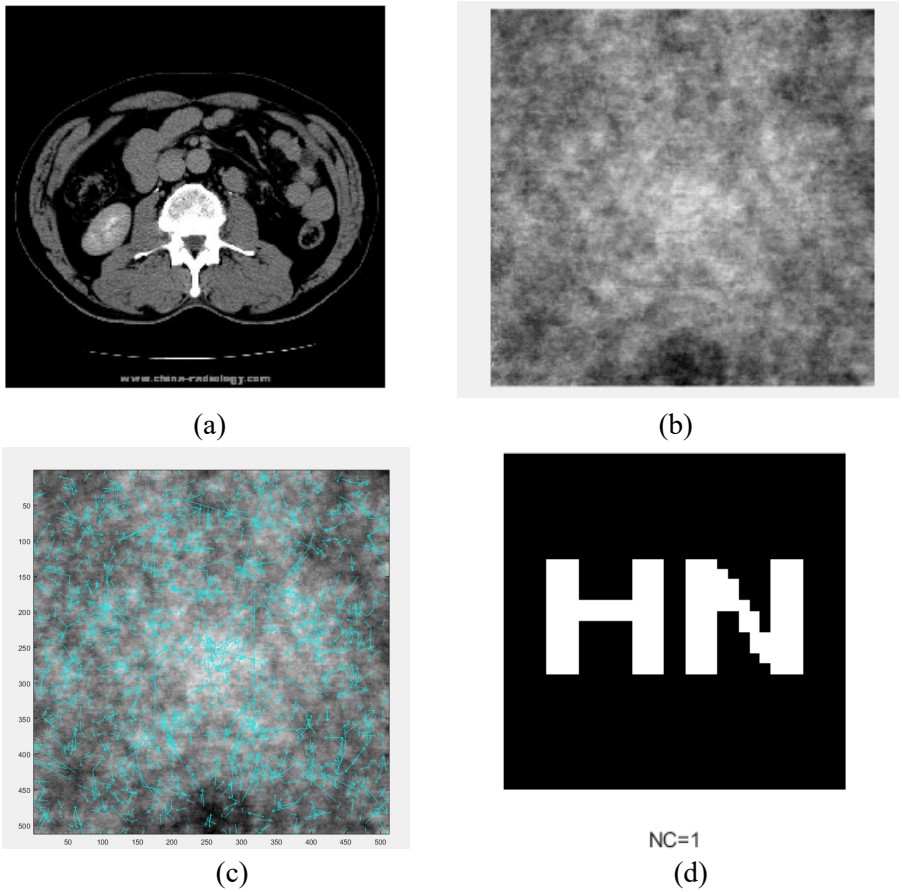


Figure 8: (a) The original abdominal CT image; (b) The encrypted medical image; (c) Key points of the encrypted medical image after SIIFT; (d) The original Extracted watermarking

5.1 Conventional attacks

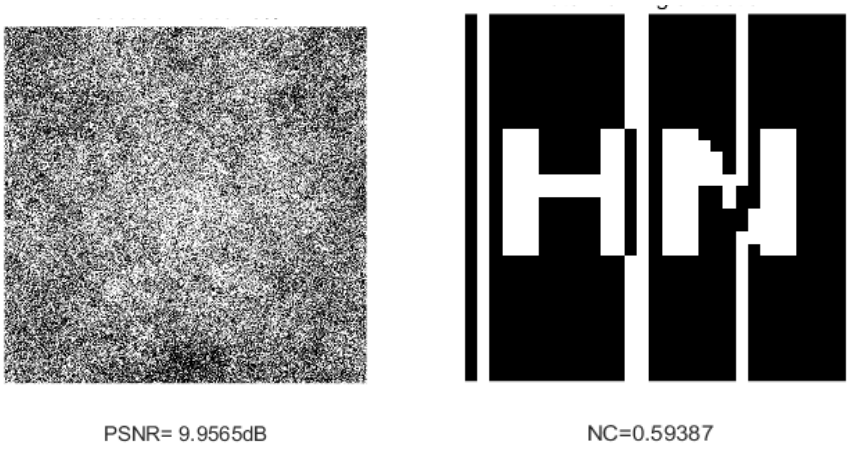
Conventional attacks on the encrypted CT image are carried out with various strengths, and NC values are calculated to test the robustness of the new algorithm (see Tab. 1). It can be found that the value of NC is near 0.6 in Gaussian noise attacks. When JPEG compression attack is 2%, its value of NC can get 0.65. So, the proposed watermarking algorithm is performing satisfactorily.

Table 1: The PSNR and NC values under Conventional Attacks based on SIFT-DCT

Conventional attack	Gaussian noise			JPEG compression		
	3%	8%	15%	2 %	10 %	30 %
PSNR (dB)	15.31	11.72	9.96	24.88	30.05	34.19
NC	0.66	0.69	0.60	0.65	0.74	0.90

5.1.1 Gaussian noise

When the encrypted medical image is under Gaussian noise (15%) attacks, the value of NC is 0.60. The data proved that the algorithm is robust against Gaussian noise attacks. The result is shown in Fig. 9.

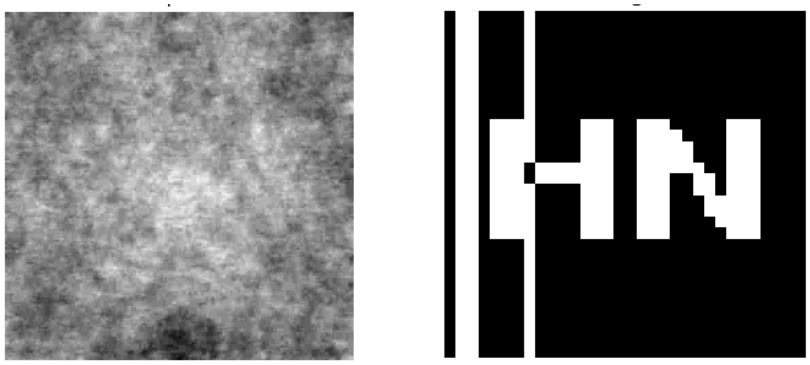


(a) The encrypted medical image (b) The extracted watermarking

Figure 9: Medical image and Extracted watermarking under Gaussian noise attack 15%

5.1.2 JPEG compression

When the encrypted medical image is under JPEG compression (10%) attacks, the value of NC is 0.74. The data proved that the algorithm is robust against JPEG compression attacks. The result is shown in Fig. 10.



(a) The encrypted medical image (b) The extracted watermarking

Figure 10: Medical image and Extracted watermarking under JPEG compression 10%

5.2 Geometric attacks

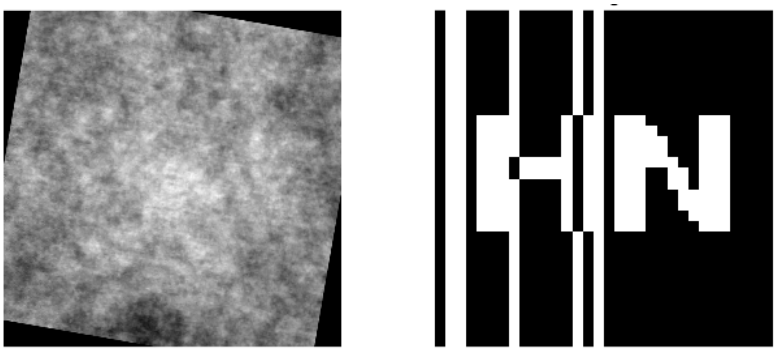
The robustness of geometric attacks is always a problem. A series of geometric attacks are tested through this algorithm, and the results are shown in Tab. 2.

Table 2: The PSNR and NC value under Geometric Attacks based on SIFT-DCT

Geometric attacks	Attack strength	PSNR (dB)	NC
Rotation (clockwise)	2°	20.02	0.72
	8°	15.71	0.51
	10°	15.11	0.60
Scaling	×0.8	-	0.62
	×1.5	-	0.79
	×3.0	-	0.65
Translation (left)	3%	22.59	0.89
	4%	20.95	0.81
Translation (right)	2%	25.52	0.89
	4%	21.45	0.81
Translation (up)	1%	25.35	0.90
	3%	22.43	0.90
Clipping (Y direction)	5%	-	0.90
	30%	-	0.72
	45%	-	0.69
Clipping (X direction)	5%	-	0.88
	25%	-	0.72
	30%	-	0.66

5.2.1 Rotation attack.

When the encrypted medical image is rotated 10° (clockwise), the extracted watermark is shown in Fig. 11. In this case, the degree of correlation is 0.60. So, the proposed algorithm has a good robustness against the rotation attacks.

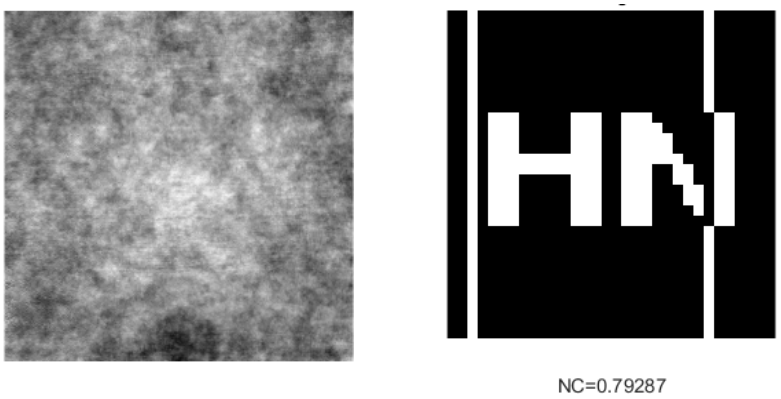


(a) The encrypted medical image (b) The extracted watermarking

Figure 11: Medical image and Extracted watermarking under rotation attack 10°

5.2.2 Scaling attack

When the encrypted medical image is Scaling (×1.5), the extracted watermark is shown in Fig. 12. In this case, the degree of correlation is 0.79. So, the proposed algorithm has a good robustness against the scaling attacks.

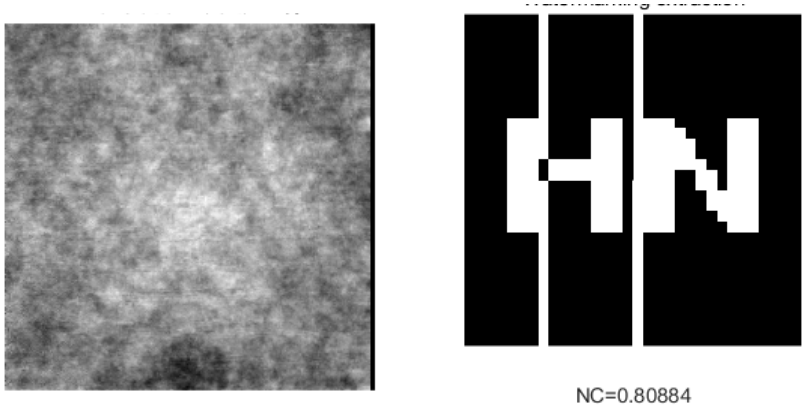


(a) The encrypted medical image (b) The extracted watermarking

Figure 12: Encrypted Medical image and Extracted watermarking under scaling attack (×1.5)

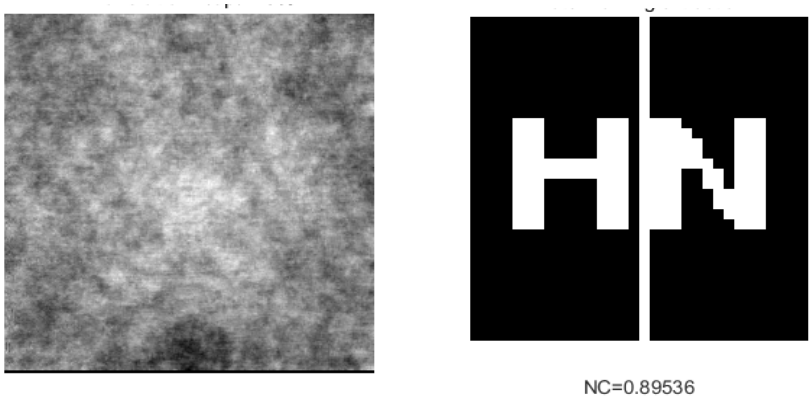
5.2.3 Translation attacks

The encrypted CT image is translated attack. When left translated 4%, the value of NC is 0.81 (see Fig. 13). When up translated 3%, the value of NC is 0.90 (see Fig. 14). And the watermarking is close to the original watermarking. This show that the algorithm has a fine robustness against translation attacks.



(a) The encrypted medical image (b) The extracted watermarking

Figure 13: Experimental results under Translation left 4% attack

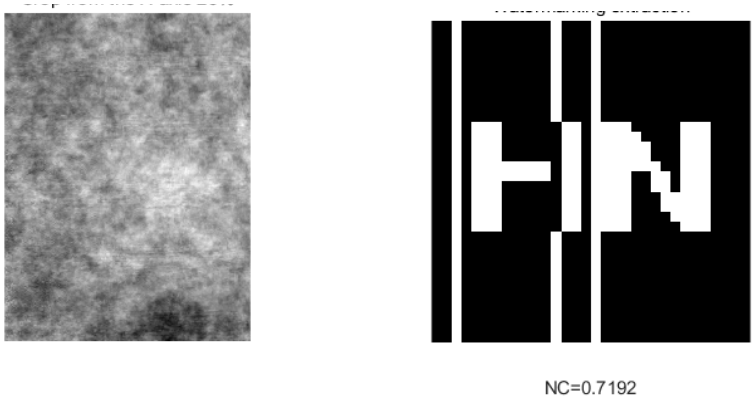


(a) The encrypted medical image (b) The extracted watermarking

Figure 14: Experimental results under Translation up 3% attack

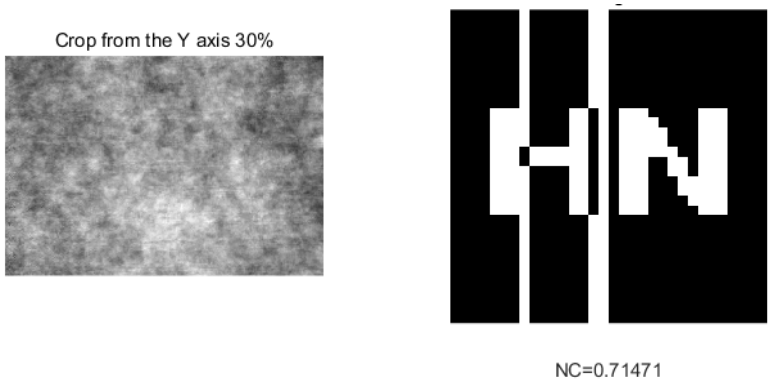
5.2.4 Clipping attacks

The CT image is clipped about 25% in the x direction. The cropped medical image is given in Fig. 15. The degree of correlation is 0.72. When it is clipped about 30% in the y-axis direction, the clipped medical image is shown in Fig. 16. The degree of correlation is 0.71. Therefore, the watermarking algorithm has strong robustness against clipping attacks.



(a) The encrypted medical image (b) The extracted watermarking

Figure 15: Experimental results under Clipping x-axis 25% attack



(c) The encrypted medical image (d) The extracted watermarking

Figure 16: Experimental results under Clipping y-axis 30% attack

5.3 Comparison with unencrypted Algorithm

The algorithm is compared with the unencrypted data, and it is shown in Tab. 3. The experimental results show that the NC value of ciphertext domain is not significantly different from that of plaintext domain, which indicates that the encryption algorithm has homomorphism.

Table 3: Comparison with unencrypted Algorithm based on SIFT-DCT

Attacks strength	NC value	
	Plaintext Domain	Encrypted Domain
Gaussian noise 8%	0.59	0.69
JPEG compression 10%	0.48	0.74
Rotation 10 ° (clockwise)	0.80	0.60

Scaling ×1.5	0.61	0.79
Translation 4% (left)	0.89	0.81
Translation 4% (right)	0.88	0.81
Translation 3% (up)	0.85	0.90
Cropping 25% (X axis)	0.87	0.72
Cropping 30% (Y axis)	0.61	0.72

5.4 Comparison with other encrypted Algorithms.

The NC value of this algorithm in ciphertext domain is compared with that of the classical feature extraction method, and the data is recorded in Tab. 4.

Table 4: Comparison with other encrypted Algorithms

Attacks strength	NC value			
	SIFT-DCT	DCT	DWT	DWT-DCT
Gaussian noise 8%	0.59	0.89	0.79	0.88
JPEG compression 10%	0.48	1.00	0.88	1.00
Rotation 10 ° (clockwise)	0.80	0.41	0.71	0.41
Scaling ×1.5	0.61	1.00	0.59	1.00
Translation 4% (left)	0.89	0.63	0.37	0.62
Translation 3% (up)	0.85	0.80	0.02	0.81
Cropping 25% (X axis)	0.87	0.04	1.00	0.04
Cropping 30% (Y axis)	0.61	0.42	1.00	0.34

Through experiments, it can be found that the feature extraction method based on SIFT-DCT is not as effective as the classical DCT in conventional attacks, especially in JPEG compression. Because the key points of SIFT include location, length, direction and so on. When compression or filtering attacks are carried out, the key points extracted by SIFT vary greatly, making the algorithm no longer has good robust. However, in terms of geometric attacks, the features extracted based on SIFT-DCT have better robust, which is significantly improved compared with the other three classical algorithms. In actual transmission, geometric attack is more challenging, so the improvement of robust of this algorithm in geometric attack has great significance.

6 Conclusion

In this paper, two different methods are combined to improve the traditional digital watermarking algorithm, which is a robust zero-watermarking algorithm based on SIFT-DCT for medical images in the encryption domain. The original image is encrypted to protect the privacy of the original medical image. Then, zero-watermarking technology is

adopted. The advantage of this technology is that the original medical image will not be damaged, which will not affect the doctor's judgment on the sensitive areas of tumors and other diseases in medical images. In addition, the algorithm uses SIFT-DCT to extract image features, Combining scale invariance of SIFT and energy concentration of DCT, and the selected features have strong robust in geometric attacks, which also solves one of the difficulties in transmission. Moreover, this algorithm is flexible, which can not only play a prominent role in medical image processing and ensure the security of image transmission, but also be applicable to other image recognition and retrieval.

Acknowledgement: This work is supported by the Key Reach Project of Hainan Province [ZDYF2018129], the National Natural Science Foundation of China [61762033], and the National Natural Science Foundation of Hainan [2018CXTD333], the Key Innovation and Entrepreneurship Project of Hainan University [Hdcxcyxm201711], and the Higher Education Research Project of Hainan Province (Hnky2019-73) and the Key Research Project of Haikou College of Economics [HJKZ18-01].

References

Abdallah, H. A.; Faragallah, O. S.; Elsayed, H. S.; Mohiy, M. H.; Shaalan, A. A. et al. (2016): Robust image watermarking method using homomorphic block-based KLT. *Optik*, vol. 127, no. 4, pp. 2374-2381.

Chen, Y.; Li, B.; Rong, D. (2013): Contourlet-SIFT feature matching algorithm. *Electronics and Information Technology*, pp. 203-209.

Das, C.; Panigrahi, S.; Sharma, V. K.; Mahapatra, K. K. (2014): A novel blind robust image watermarking in DCT domain using. inter-block coefficient correlation. *International Journal of Electronics and Communications,* vol. 68, no. 3, pp. 244-253.

Dai, S. S.; Tian, Y. L. (2014): Research on SIFT algorithm based on image texture features. *Semiconductor Optoelectronics*, pp. 107-110.

Fang, S. Q.; Cai, Z. P.; Sun, W. C.; Liu, F.; Liang, Z. et al. (2018): Feature selection method based on class discriminative degree for intelligent medical diagnosis. *Computers, Materials & Continua*, vol. 55, no. 3, pp. 419-433.

Fazlali, H. R.; Samavi, S.; Karimi, N.; Shirani, S. (2017): Adaptive blind image watermarking using edge pixel concentration. *Multimedia Tools and Applications*, vol. 76, no. 2, pp. 3105-3120.

Guo, J. T.; Zheng, P. J.; Huang, J. W. (2015): Secure watermarking scheme against watermark attacks in the encrypted domain. *Journal of Visual Communication and Image Representation*, vol. 30, pp. 125-135.

Han, B. R.; Li, J. B. (2016): Watermarking algorithm for medical volume data anti-geometric attacks. *Biomedical Research*, vol. 27, no. 2, pp. 308-312.

Han, L.; Zhou, G. Y.; Xu, L.; Fang, L. (2017): Beyond SIFT using binary features in loop closure detection. *IEEE International Conference on Intelligent Robots and Systems*, pp. 4057-4063.

Kim, H. D.; Lee, J. W.; Oh, T. W. (2012): Robust dt-cwt watermarking for dibr 3D

images. *IEEE Trans Broadcast*, vol. 58, no. 4, pp. 533-543.

Lang, J.; Zhang, Z. G. (2014): Blind digital watermarking method in the fractional fourier transform domain. *Optics and Lasers in Engineering*, vol. 53, pp. 112-121.

Liu, J. L.; Li, J. B.; Chen, J.; Zou, X. X.; Chen, J. R. et al. (2018): Medical image watermarking based on SIFT-DCT perceptual hashing.

https://link.springer.com/book/10.1007/978-3-030-00012-7.

Liu, Z. Q.; Li, Q.; Liu, J. R. (2011): SIFT based image hashing algorithm. *Chinese Journal of Scientific Instrument*, vol. 32, no. 9, pp. 2024-2028.

Li, Q. L.; Wang, G. Y.; Liu, J. G. (2012): Robust scale-invariant feature matching for remote sensing image registration. *IEEE Geoscience and Remote Sensing Letters*, vol. 6, no. 2, pp. 287-291.

Lv, X. D.; Wang, J. (2012): Perceptual image hashing based on shape contexts and local feature points. *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1081-1093.

Parah, S. A.; Sheikh, J. A.; Ahad, F. (2017): Information hiding in medical images: a robust medical image watermarking system for E-healthcare. *Multimedia Tools and Applications*, vol. 76, no. 8, pp. 10599-10633.

Parah, S. A.; Sheikh, J. A.; Loan, N. A.; Bhat, G. M. (2016): Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. *Digital Signal Processing*, vol. 53, pp. 11-24.

Priyatham, B.; Nilkanta, S.; Arijit, S. (2014): SIFT based robust image watermarking resistant to resolution scaling. *IEEE International Conference on Image Processing*, pp. 5507-5510.

Wu, X. Q.; Li, J. B.; Tu, R. (2018): Contourlet-DCT based multiple robust watermarkings for medical images.

https://doi.org/10.1007/s11042-018-6877-5.

Zhao, M.; Jiang, J. G.; Hong, R. C. (2014): SIFT matching optimization based on RANSAC. *Optoelectronic Engineering*, pp. 62-69.