




Contourlet-DCT based multiple robust watermarkings for medical images

Xiaoqi Wu¹ · Jingbing Li^{1,2}  · Rong Tu³ · Jieren Cheng¹ · Uzair Aslam Bhatti¹ · Jixin Ma⁴

Received: 29 May 2018 / Revised: 5 November 2018 / Accepted: 13 November 2018

Published online: 05 December 2018

© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract

In the current medical system, the privacy and security of the medical information with respect to its transmission and storage is a key challenge. In pursuit of this, we proposed a contourlet transform and Discrete Cosine Transform (DCT) based multiple robust watermarking algorithms for medical imaging. The proposed scheme uses contourlet transform to extract multidirectional and multiscale texture information, and then the DCT was used to acquire the feature vector in the low frequency directional subbands. Then we used Logistic Map to encrypt the watermark to ensure the security of the original watermarking information under a chaotic system. In watermark embedding and extraction phases, we adopted zero-watermarking technique to ensure the integrity of the medical images. Our experimental results show that the proposed algorithm can embed much more data with less complexity and dose not change the pixel value of the original image. Moreover, the proposed algorithm can extract the watermark effectively with good invisibility and robustness to common and geometric attacks.

Keywords Medical image · Contourlet-DCT · Zero watermarking · Robust

1 Introduction

Because of the rapid development of in science, technology and information communication, most of the medical systems have also become data-based. A large amount of data related to the medical information and the privacy details of the patient have been

✉ Jingbing Li
Jingbingli2008@hotmail.com

✉ Rong Tu
turong37472@126.com

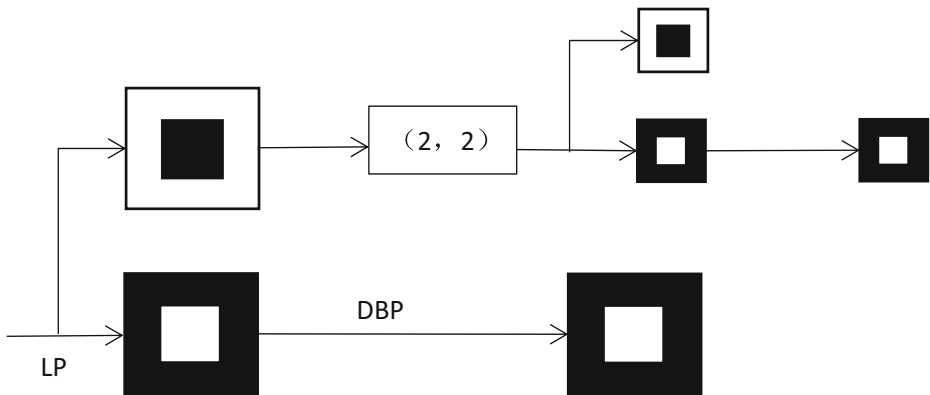


Fig. 1 The contourlet transformation flow

transmitted and stored on the internet [8]. Compared with the traditional encryption technology, digital watermarking technology [9] can directly embed the information into a digital carrier without affecting the original data. So the privacy information of the patient can be embedded as a watermark in the original image, and the watermark information can be extracted completely due to the robustness in the whole transmission process.

Medical images are an important basis for doctors to obtain the pathological information of the patient, so the data is strictly required. We can use the important features of the image to construct the watermark information to achieve the zero-watermark. It is a good solution to the contradiction between the robustness and perception of the invisible digital watermarks. In recent years, medical watermarking algorithms have been rapidly developed at home and abroad. Kevin Rangel-Espinoza et al. [12] proposed a removable visible watermarking system; Mohammad Ali Akhaee et al. [2] proposed an improved multiplicative image watermarking system. The tradeoff between the transparency and robustness of the watermark data is solved in a novel fashion. Shuli Zheng et al. [20] proposed a coverless steganographic method based on robust image hashing. The method did not modify the content of the image itself and had a higher robustness. The problem that the watermark information is encrypted and hidden was the focus of our attention. Qili Zhou et al. [22] proposed a steganographic method using a reversible texture synthesis based on the seeded region growing and Least Significant Bit (LSB), Yi Cao et al. [5] proposed a novel coverless information hiding method based on molecular

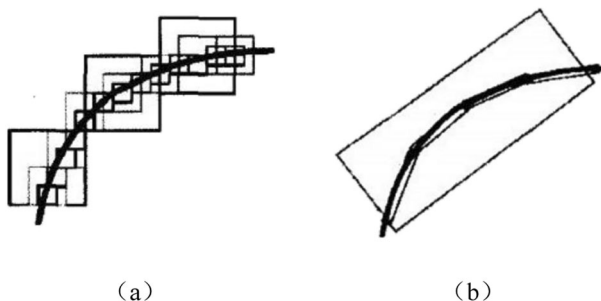


Fig. 2 Comparison between (a) Wavelet and (b) Contourlet

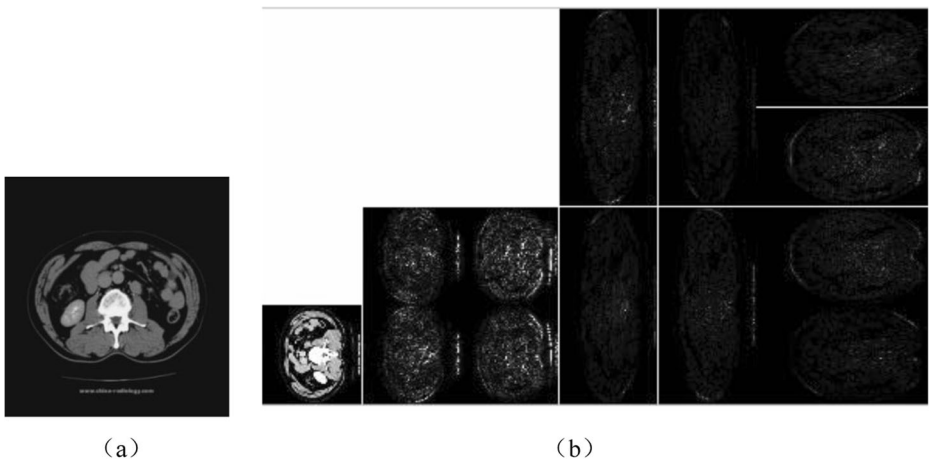


Fig. 3 Contourlet transform of medical images: **a** original image **b** contourlet transform

structure image of material (MSIM). Their method exhibited a better performance in the security and capacity. Donghui Hu et al. [10] proposed a novel steganographic image without embedding the method based on the deep convolutional generative adversarial network. Chaotic encryption technology is also widely used to improve the security of the digital image watermarking in medical images [18]. Currently, research carried out in the field of digital image watermarking for medical images focuses on the spatial and the transform domain. The embedding of the watermark is achieved by the gray value of some pixel values in the spatial domain or by the change in coefficient value in the transform domain [21]. However, the robustness of the image is still a difficult problem to solve [19], and there is less research carried out on robust image watermarking based on the contourlet transform.

In this paper was propose a method based on the combination of the Contourlet Transform and Discrete Cosine Transform (DCT) to process the original image and extract the feature vector. The chaotic technology was used to encrypt the watermark and the security of the watermark information was improved. The experimental results showed that the algorithm could complete the embedding and extraction of zero watermarks, and exhibited a robustness against conventional attacks and partial geometric attacks.

Table 1 Change of DCT coefficients under attacks for the original images

Image manipulation	F(1,1)	F(1,2)	F(1,3)	F(1,4)	F(1,5)	F(1,6)	F(1,7)	F(1,8)	F(1,9)	Symbol sequence
The original image	1.78	0.01	-1.03	-1.78	0.21	0.14	-0.32	0.04	-0.06	110011010
Gaussian noise (10%)	2.93	0.01	-0.76	-0.13	0.17	0.10	-0.24	0.03	-0.03	110011010
JPEG attack (4%)	1.86	0.01	-1.00	-0.18	0.21	0.13	-0.32	0.05	-0.06	110011010
Median filter [5×5]	1.70	0.01	-1.02	-0.19	0.24	0.15	-0.35	0.04	-0.06	110011010
Rotation (clockwise 10°)	1.77	0.08	-1.03	-0.26	0.21	0.12	-0.40	0.07	-0.02	110011010
Movement (left 8%)	1.77	0.15	-1.01	-0.24	0.15	0.25	-0.28	0.00	-0.04	110011010

DCT coefficient unit: 1.0e+003

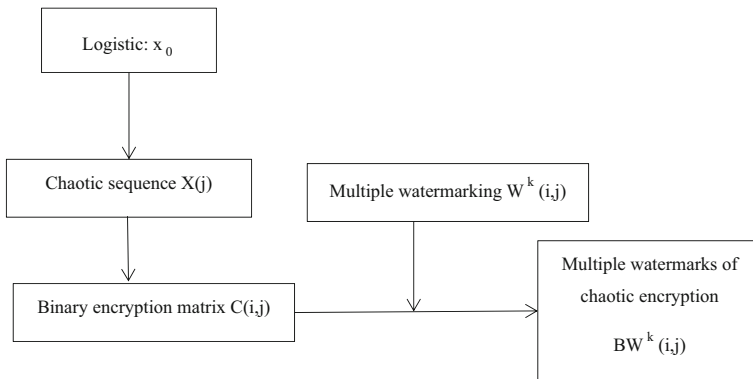


Fig. 4 The encryption algorithm flow

2 The fundamental theory

2.1 Contourlet transform

The contourlet transform is a new two-dimensional image sparse representation method proposed by Do and Vetterli in 2002 [7]. It can analyze the direction and scale of each image at the same time, and can effectively represent the texture and contour of the image. This transformation is mainly to complete two parts of about the Laplacian Pyramid (LP) decomposition [4] and the Direction Filter Bank (DFB) filter [14]. Figure 1 shows the decomposition used in the contourlet filter bank. Bandpass images from LP are fed into a DFB to capture the directional information. By iterating this scheme on the coarse image, the image decomposes into directional subbands at multiple scales. This means that a multidirectional and multiscale resolution decomposition of the original images can be achieved.

Compared with the commonly used wavelet transform, contourlet transform has the advantage of describing the edge of the image contour [7]. When approaching a singular curve, the two-dimensional separable wavelet is implemented on the basic function of the square support domains of different sizes [17], but the direction is limited, so that the wavelet transform cannot capture the information from the two aspects [1]. Meanwhile, contourlet transform is implemented by using rectangles with different length and width dimension as basic functions. It can be clearly seen from Fig. 2a and b that the number of

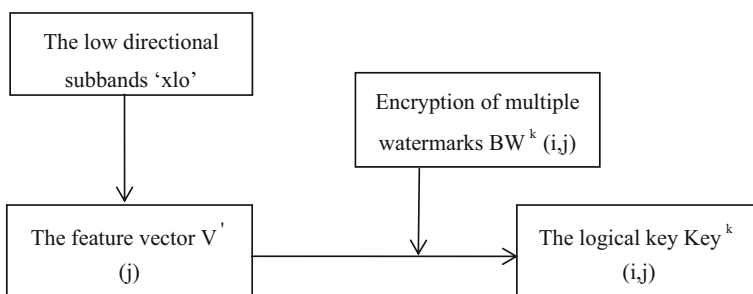


Fig. 5 The watermark embedding process

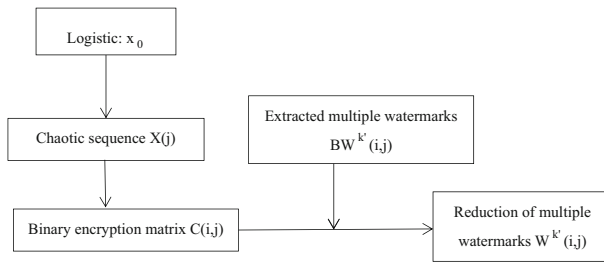


Fig. 6 Watermark decryption process

rectangles used by the contourlet transform is significantly less than the number of wavelet transform squares under the same conditions. Therefore, the contourlet transform is better than the wavelet transform terms of in contour details.

2.2 Discrete cosine transform

Discrete cosine transform is widely used in the signal and image processing for lossy data compression of signals and images. This is because most of the signal energy can be concentrated in the low-frequency part after DCT [11], and Suboptimal Orthogonal Transformations take only seconds with K-L transformation obtained under the minimum Mean Square Error Conditions. It is fast, accurate and highly capable of extracting the feature components. So this experiment uses DCT to extract the feature vectors of the medical images. The two-dimensional discrete cosine transform (2D-DCT) formula is shown as follows:

$$\begin{aligned}
 F(u, v) &= c(u)c(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \cos \frac{\pi(2x+1)u}{2M} \cos \frac{\pi(2y+1)v}{2N} \\
 & \quad u = 0, 1, \dots, M-1; v = 0, 1, \dots, N-1; \\
 c(u) &= \begin{cases} \sqrt{1/M} & u = 0 \\ \sqrt{2/M} & u = 1, 2, \dots, M-1 \end{cases} \quad c(v) = \begin{cases} \sqrt{1/N} & v = 0 \\ \sqrt{2/N} & v = 1, 2, \dots, N-1 \end{cases}
 \end{aligned}
 \tag{1}$$

The two-dimensional discrete cosine inverse transform (2D-IDCT) formula is carried out by using:

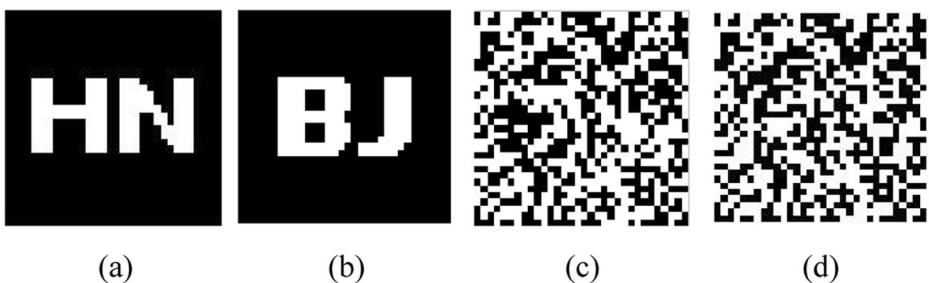


Fig. 7 Watermarks and their chaotic encrypted images: a Watermark 1, b Watermark 2, c Watermark 1 of chaotic encryption, d Watermark 2 of chaotic encryption

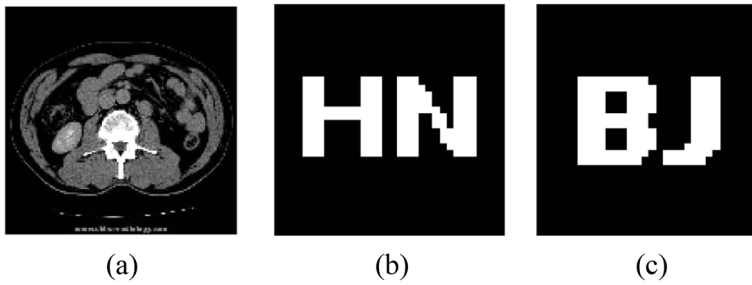


Fig. 8 Image without attack and the extracted watermarking: **a** Original medical image under no attacks, **b** Extracted watermarking 1, **c** Extracted watermarking 2

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

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

Where, x, y represent the spatial sampling frequency domain; u, v frequency presents the domain sampling value, and they are generally represented by a pixel square matrix in digital image processing, i.e. $M = N$.

2.3 Logistic map

The iteration of the chaotic system generates a factor sequence for the transformation when it is encrypted. The main theoretical basis of chaos encryption lies in the self-similarity of the chaos [6, 15]. The one-dimensional discrete-time nonlinear dynamic system Logistic map is defined as follows:

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

Among these values, $x_k \in (0, 1)$ and $0 \leq \mu \leq 4$ are the growth parameters. At the time of $3.5699456... < \mu \leq 4$, the Logistic map is in a chaotic state. In the initial state x_0 , the sequence generated under the Logistic map state is very sensitive to the initial value as well as is non-cyclic and non-convergent. Therefore, this sequence was chosen as the ideal key sequence. The value $\mu = 4$ is taken in this studies.

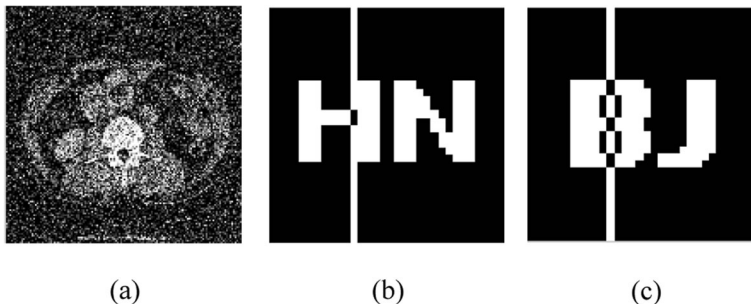


Fig. 9 Attacked medical image and extracted watermarks **a** the Gauss noise intensity 10%, **b** Extracted watermarking 1, **c** Extracted watermarking 2

Table 2 The PSNR and NC values under Gaussian noise

Noise intensity/%	3	5	10	15	20
PSNR/dB	17.25	15.16	12.46	10.94	9.99
NC1	1.00	0.95	0.95	0.86	0.90
NC2	1.00	0.93	0.93	0.90	0.81

3 Watermarking algorithm

3.1 Acquire the feature vector of medical images

As shown in Fig. 3a, we selected a 512×512 Gy medical image as an the original image to test. As shown in Fig. 3b, a contourlet transform was used to perform a Laplacian pyramid transformation of 2 levels and 8 subdivision of the finest sub-band in the medical image, and then we extracted the low directional subbands [3, 23] 'xlo'.

Although the contourlet transform can extract low frequency subgraphs that concentrate most the energy of the original image, the coefficients with larger amplitudes in the coefficient matrix are not concentrated and have no regularity. This brings difficulties to extract feature values. Then we focused image energy and eliminate correlation between eigenvalues by DCT.

Then the low directional subbands 'xlo' was extracted from the contourlet transform and subjected to full-map DCT to obtain the coefficient matrix $FD(i, j)$. The coefficient matrix was obtained from the first 32 values after sorting by size, and the feature vector $V(j) = \{v(j) | v(j) = 0, 1; 1 \leq j \leq 32\}$ of the original image was obtained by symbolic operations.

$$FD(i, j) = DCT2(F(i, j)) \quad (4)$$

$$V(j) = \text{sign}(FD(i, j)) \quad (5)$$

We regarded the value of low-frequency coefficient ($F(1,1) \sim F(1,9)$) to construct a symbol sequence (see Table 1). Considering the DCT coefficient value is 1, if it is greater than or equal to zero; otherwise it is 0. After a large number of experiments, we found that although the selected low frequency coefficient values changed after the encrypted medical image were attacked, the symbol sequence of the low frequency coefficient remained basically unchanged.

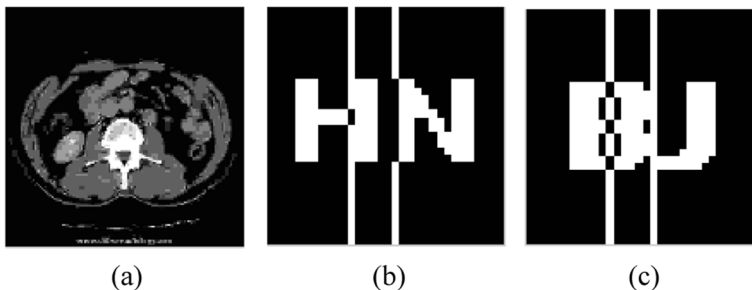


Fig. 10 Attacked medical image and extracted watermarks: **a** JPEG compression quality 2%, **b** Extracted watermarking 1, **c** Extracted watermarking 2

Table 3 PSNR and NC values under JPEG compression attack

Compression quality/%	2	4	8	10	20	40
PSNR/dB	24.62	26.39	28.81	29.79	32.32	34.72
NC1	0.86	1.00	1.00	1.00	1.00	1.00
NC2	0.90	1.00	1.00	1.00	1.00	1.00

3.2 Watermark encryption and embedding

Chaotic encryption The Fig. 4 represents the flow chart in which the Logistic Map used to encrypt the watermark that needs to be embedded. Since the chaotic sequence $X(j)$ generated by the initial value x_0 of the Logistic Map was one-dimensional, but the embedded watermark was a two-dimensional image, the one-dimensional sequence was converted into the required two-dimensional matrix by the dimensionality formula. Subsequently, the binary matrix $C(i, j)$ was obtained by the symbolic operation, which was combined with the original watermark $W^k(i, j)$, and then lastly the encrypted watermark $BW^k(i, j)$ was obtained by using the Hash function.

Encryption watermark embedding The Fig. 5 described the process of the watermark embedding. The logical key formula is as follows:

$$Key^k(i, j) = BW^k(i, j) \oplus V(j) \quad (6)$$

The key $Key^k(i, j)$ was saved to extract the watermark. And the \oplus means exclusive OR. The feature vectors extracted from medical images and the encrypted watermark are used to obtain the binary logic key by the \oplus . Then the feature vectors of medical images are extracted after attack, and use this key to get embedded watermark. We used the important features of the image to construct the watermark information. This method did not change the pixel value of the original image. So as to the method achieved a zero watermark embedding. The zero watermarking technology can well solve the contradiction between the perceptibility and robustness of invisible digital watermarks.

3.3 The extraction and decryption of watermark

Feature vector extraction Let the medical image to be measured and denoted by $F(i, j)$. $FD(i, j)$ which is a coefficient matrix obtained by discrete cosine transformation. Then the

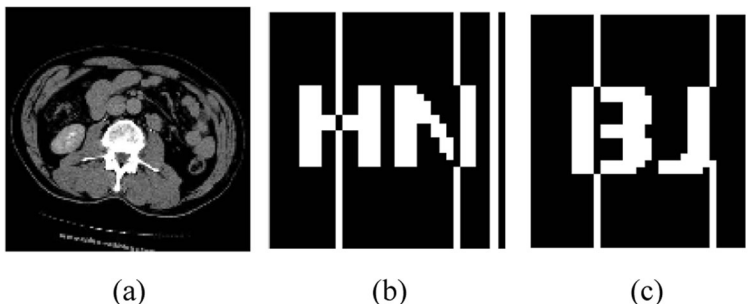


Fig. 11 Attacked medical image and extracted watermarks: **a** Median filtering [5×5], **b** Extracted watermarking 1, **c** Extracted watermarking 2

Table 4 PSNR and NC values under median filtering attack

Parameter	[3×3]			[5×5]			[7×7]		
	1	10	20	1	10	20	1	10	20
PSNR/dB	30.91	28.07	27.71	27.05	24.37	23.61	25.50	22.31	21.25
NC1	1.00	0.91	0.91	0.91	0.86	0.90	0.91	0.86	0.77
NC2	1.00	0.96	0.96	0.96	0.90	0.96	0.95	0.89	0.86

extraction formula for feature vector $V(j)$ is as follows:

$$FD'(i, j) = DCT2(F'(i, j)) \tag{7}$$

$$V'(j) = sign(FD'(i, j)) \tag{8}$$

Watermark extraction The feature value vector $V(j)$ of the image to be tested was extracted according to the feature extraction method of the original image, then the watermark information $BW(i, j)$ in the test image was obtained by the Hash function and the logic key $Key^k(i, j)$ was stored during the watermark embedding and the feature vector $V(j)$ of the test image. The formula of $BW(i, j)$ is as follows:

$$BW'(i, j) = Key^k(i, j) \oplus V'(j) \tag{9}$$

Watermark decryption The Fig. 6 was the process of the watermark decryption. The original watermark $W^k(i, j)$ was restored by the Hash function by using the binary encryption matrix $C(i, j)$ and the extracted watermark $BW(i, j)$. This can be shown as follows:

$$W^{k'}(i, j) = C(i, j) \oplus BW^k(i, j) \tag{10}$$

The entire algorithm did not require the original medical image when extracting the encrypted watermark. This effectively protected the image information and improved the security of the image.

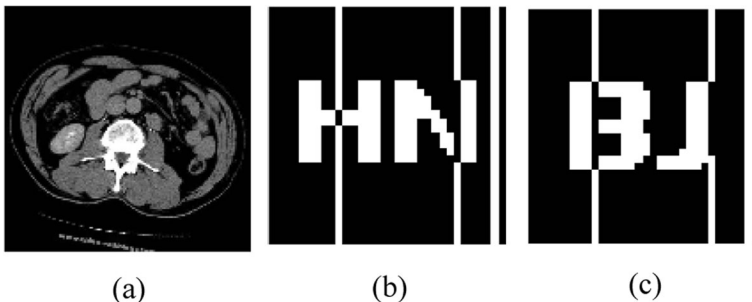


Fig. 12 Attacked medical image and extracted watermarks: **a** rotation (clockwise 10°), **b** Extracted watermarking 1, **c** Extracted watermarking 2

Table 5 The NC value under rotation attack (clockwise)

Parameter/ $^{\circ}$	5	10	15	20
PSNR/dB	16.80	14.99	14.17	13.66
NC1	0.95	0.82	0.60	0.60
NC2	0.90	0.78	0.54	0.55

4 Experiments and results

Using the MATLAB 2014a we selected as the simulation platform and two different letter pictures as the watermark embedded in the original image. Shown in Fig. 7a and b, denoted as $W^k = \{w^k(i, j) | w^k(i, j) = 0, 1; 1 \leq i \leq 3, 1 \leq j \leq 32, 1 \leq k \leq 2\}$. Afterwards, a huge change was applied in the watermark image after the chaos and the security of its information was guaranteed, as shown in Fig. 7c and d and used the original image is a 512×512 gray medical image. In this experiment, the initial value of the chaotic coefficient was set to 0.2, the growth parameter was 4, and the iteration number was 32.

The NC1 and NC2 values were used to represent the correlation coefficients of the two watermarks. When the NC value was closer to 1.0, the correlation between the original watermark and the extracted watermark was higher, and it was also used to measure the robustness of the attacked algorithm.

The formula for the normalized correlation coefficient NC is as follows:

$$NC = \frac{\sum_i \sum_j W_{(i,j)} W'_{(i,j)}}{\sum_i \sum_j W_{(i,j)}^2} \quad (11)$$

The peak signal-to-noise ratio formula is as follows:

$$PSNR = 10 \lg \left[\frac{MN \max_{i,j} (I_{(i,j)})^2}{\sum_i \sum_j (I_{(i,j)} - I'_{(i,j)})^2} \right] \quad (12)$$

In the above formula, $I_{(i,j)}$ and $I'_{(i,j)}$ represent the gray values of the original medical images and the coordinates of the embedded watermark images (i, j) , respectively, M and N represent

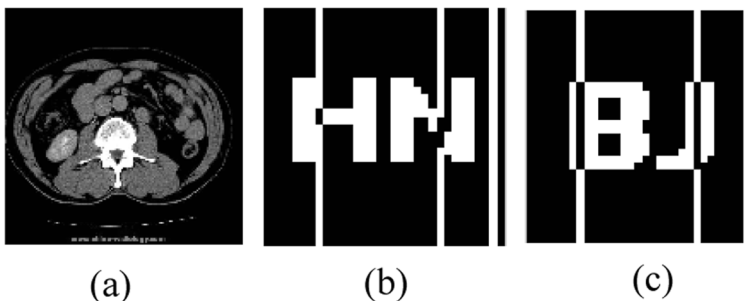


Fig. 13 Attacked medical image and extracted watermarks: **a** Movement (left) 10%, **b** Extracted watermarking 1, **c** Extracted watermarking 2

Table 6 The PSNR and NC values under moving attack

Movement (left)/%	4	6	8	10	15
PSNR/dB	17.66	16.61	15.67	15.25	14.04
NC1	1.00	0.96	0.86	0.85	0.76
NC2	1.00	0.96	0.77	0.77	0.67

the pixel values of image rows and columns. The PSNR value indicates the degree of distortion, and the larger the PSNR value, the smaller was the distortion of the image.

In Fig. 8a it can be seen when the original medical image was not attacked, the image did not changed, and from the extracted watermark, and is shown in Fig. 8b and c, the NC value was 1.0. Subsequently, the conventional attack and geometric attacks were used to test the robustness of the algorithm.

4.1 General attack

Gaussian noise It can be seen from Fig. 9a that when the gaussian noise was 10%, the PSNR = 12.63 dB value of the image was indistinct when compared with the non-attack scenario. From Fig. 9b and c, the original watermark can be clearly seen and identified. We found NC1 = 0.95, NC2 = 0.93. When Gaussian noise was as high as 20%, the watermark could still be extracted accurately, which indicates that the method exhibited a strong robustness against the interference of Gaussian noise (see Table 2).

JPEG attack JPEG compression was performed on medical images containing watermarks, as shown in Fig. 10a. When the compression quality was 2%, the image experienced an obvious blurred “squares” effect. However, from Fig. 10b and c, it can be seen that the algorithm extracted a high definition of the watermark, which was consistent with the original watermark NC1 = 0.86, NC2 = 0.90. Therefore, from Table 3, we can reach the conclusion that there is a good robustness against JPEG attacks.

Median filtering attack To contain the watermark image median filtering (parameters [5×5], filtering repeat time 10), the outline of the image was blurred, as shown in Fig. 11a, we observed a high degree of NC value, as shown in Fig. 11b and c, NC1 = 0.86, NC2 = 0.90. We extracted the watermark successfully. Therefore, this method was found to be robust against the median filtering (Table 4).

4.2 Geometry attack

Rotation attack As shown in Fig. 12, the image clockwise turned 10 degrees, and the NC values were 0.82 and 0.78 respectively. The watermark was also extracted accurately. The extraction of watermarks had differences at different rotation angles. The watermark extraction

Table 7 The NC value under scaling attack

Parameter	×0.1	×0.25	×0.6	×0.85	×1.5
NC1	0.67	0.91	0.95	1.00	1.00
NC2	0.66	0.84	0.93	1.00	1.00

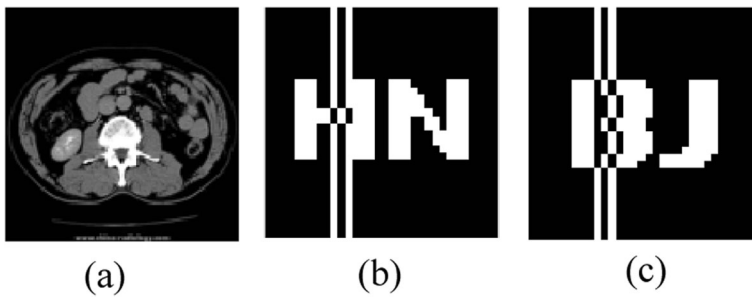


Fig. 14 Attacked medical image and extracted watermarks: **a** Scaling factor 0.25, **b** Extracted watermarking 1, **c** Extracted watermarking 2

quality was reduced with an increase in the degree of rotation. When rotation was as high as 20 degrees (see Table 5), still the watermark was extracted accurately. So, the method exhibited robustness against rotation attack.

Moving attack When the medical image containing the watermark was moved (left) 10%, $NC1 = 0.85$, $NC2 = 0.77$, as shown in Fig. 13a ~ c, the original watermark was extracted. However, Table 6 shows that the algorithm was robust against the movement attack.

Scaling attack As shown in Fig. 14a ~ c, when the medical image containing the watermark was reduced to 0.25 times the original, $NC1 = 0.91$, $NC2 = 0.84$. The content information of the watermark was still completely presented, namely, the watermark that embedded in the medical image was accurately obtained at this time. We implemented a scaling attack experiment on the medical image, Table 7 shows the extraction quality of the watermark. When scaling factor was 0.1, $NC1 = 0.67$, $NC2 = 0.66$. And we were still able to get valid information from the watermark. The algorithm was robust against the scaling attack.

Cropping attack The Fig. 15a was the medical image subjected to cropping attack in the upper left corner. $NC1 = 0.85$, $NC2 = 0.80$. From the Fig. 15b and c, we clearly saw that the watermark had some distortion, but they did not affect the content information of the watermark. However the cropping attack in other locations, the effect was relatively poor (see Table 8). So The algorithm was generally robust against the cropping attack.

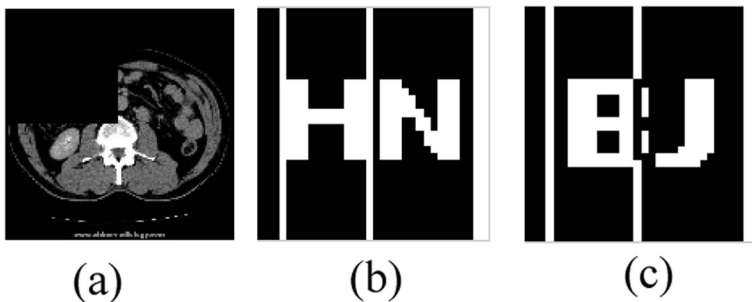


Fig. 15 Attacked medical image and extracted watermarks: **a** cropping attack (upper left corner 1/4), **b** Extracted watermarking 1, **c** Extracted watermarking 2

Table 8 The NC value under cropping attack

Parameter	Upper left corner 1/16	Upper left corner 1/4	Center 1/4	Bottom right 1/4
NC1	1.00	0.85	0.48	0.51
NC2	1.00	0.80	0.63	0.38

4.3 Comparison with other algorithms

On comparing the simulation results of the two algorithms (see Table 9). We can get conclusions from the data. First, according to NC values, The zero-watermark scheme of the two transform domains was robust to attack methods. As the attack intensity was increased, the quality of the extracted watermark image was decreased. The NC value was also decreased. But the proposed algorithms in this paper could reduce the NC value to a lesser extent. So the algorithm was more robust. Second, in the Gaussian noise attack, rotation attack and translation attack, the NC value was significantly higher. When the medical image was cropped, the center-cropping was slightly worse, and the proposed algorithm was better than the wavelet domain in other locations. But when using JPEG attack, median filtering attack and scaling attack, the proposed algorithm has a slightly smaller NC value than the wavelet domain.

In order to further verified the superiority of the algorithm, it was compared with the Ref. [13, 16]. We replaced the ‘Lena’ as the original image, which was consistent with the comparative literature. From Table 10, the NC values of the proposed algorithm were higher than those of the comparative literature. And the comparative literature used a small degree of attack. There was no movement attack in the literature, so we had no comparison. The proposed algorithm has very strong robustness in Gaussian noise attack, rotation attack and median filtering attack.

Table 9 Comparison of the two algorithms

Attacks	Parameter	DWT-DCT		Contourlet-DCT	
		NC1	NC2	NC1	NC2
Movement (left)/%	6	0.87	0.92	0.96	0.96
	8	0.76	0.73	0.86	0.77
	10	0.76	0.73	0.85	0.77
Rotation (clockwise)/°	5	0.86	0.87	0.95	0.90
	10	0.73	0.74	0.82	0.78
	15	0.50	0.51	0.60	0.54
Gaussian noise/%	5	0.86	0.89	0.95	0.93
	10	0.90	0.92	0.95	0.93
	15	0.82	0.86	0.86	0.90
JPEG attack/%	4	1.00	1.00	1.00	1.00
	8	0.91	0.96	1.00	1.00
	10	1.00	1.00	1.00	1.00
Median filtering/10 times	[3,3]	1.00	1.00	0.91	0.96
	[5,5]	0.95	0.93	0.86	0.90
	[7,7]	0.95	0.93	0.86	0.89
Scaling attack	×0.25	0.92	0.89	0.91	0.84
	×0.6	1.00	1.00	0.95	0.93
	×1.5	1.00	1.00	1.00	1.00
Cropping attack	Upper left corner 1/4	0.81	0.75	0.85	0.80
	center 1/4	0.54	0.41	0.51	0.38
	bottom right 1/4	0.44	0.60	0.48	0.63

Table 10 The comparison results with NC for Lena image using the schemes in this paper and Ref. [13, 16]

Attacks	Ref [13]	Ref [16]	Proposed	
Gaussian noise/1%	0.9978	0.97	1.00	1.00
Gaussian noise/2%	–	0.86	1.00	1.00
Median filtering/[3,3]	0.9889	0.95	1.00	1.00
Rotation/1°	0.7713	0.8594	1.00	1.00
Rotation/2°	–	0.45	1.00	1.00

In a word, the contourlet transform decomposed more directional sub-bands with more directional information, so it exhibited a better feature of the image texture. And we combined DCT to extract feature vectors more conveniently. We used zero-watermarking concept, this method did not change the pixel value of the original image. We selected the appropriate parameters to effectively express the image. The proposed algorithm was very robust to common image processing and geometric attacks.

5 Conclusion

In this paper, we proposed a multiple robust watermarking algorithm based on contourlet-DCT for medical images. According to the experimental data, the algorithm demonstrated a strong robustness against the Gaussian noise interference, JPEG attacks, median filtering, scaling, rotation and translation. Initially, the proposed scheme used a contourlet transform to extract the multidirectional and multiscale texture information. Subsequently, we obtained the feature vector from the low directional sub-band by the DCT. The feature vector extraction algorithm was very robust to geometric attacks and common image processing such as noise. Furthermore, from the studies using Logistic Map, multiple watermarks were scrambled to strengthen their security. Finally, we adopted the zero-watermarking technique which did not modify the image pixel value. Thus it can be used in special conditions like medical images etc. that strictly demand image quality. Therefore, this algorithm showed a good practicability in medical and other related fields.

Acknowledgements This work is supported by the Key Research Project of Hainan Province [ZDYF2018129], and by the National Natural Science Foundation of China [61762033] and the Natural Science Foundation of Hainan [617048, 2018CXTD333].

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Akhaee MA, Bartolini SME, Sankur B, Marvasti F (2009) Robust scaling-based image watermarking using maximum-likelihood decoder with optimum strength factor. *IEEE Trans Multimedia* 11(5):822–833
2. Akhaee MA, Sahraeian ME, Marvasti F (2010) Contourlet-based image watermarking using optimum detector in a noisy environment. *IEEE Trans Image Process* 19(4):967–980
3. Asmare MH, Asirvadam VS, Hani AFM (2015) Image enhancement based on contourlet transform. *SIViP* 9(7):1679–1690
4. Burt PJ, Adelson EH (1983) The Laplacian pyramid as a compact image code. *IEEE Trans Commun* 31(4): 532–540

5. Cao Y, Zhou Z, Sun X, Gao C (2018) Coverless information hiding based on the molecular structure images of material. *Comput Mater Con* 54(2):197–207
6. Deng ZJ, Xiao D, Tu FH (2004) Design and implementation of chaotic encryption algorithm based on logistic map. *JCU* 27(4):61–63
7. Do MN, Vetterli M (2005) The contourlet transform: an efficient directional multiresolution image representation. *IEEE Trans Image Process* 14(12):2091–2106
8. Dzwonkowski M, Papaj M, Rykaczewski R (2015) A new quaternion-based encryption method for DICOM images. *IEEE Trans Image Process* 24(11):4614–4622
9. Feng HY, Gu YS, Li YC (2012) Research on digital watermarking based on wavelet theory. *J Converg Inf Technol* 7(13):292–299
10. Hu DH, Wang L, Jiang WJ, Zheng SL, Li B (2018) A novel image steganography method via deep convolutional generative adversarial networks. *IEEE Access* (9):1–1
11. Jin C (2008) Digital watermarking technology and theory. Bei Jing, China
12. Kevin RE, Eduardo FN, Clara CR, Rogelio RR, Mariko NM (2017) Adaptive removable visible watermarking technique using dual watermarking for digital color images. *Multimed Tool Appl*:1–28
13. Liu Y, Wang JX, Hu HH, Zhu YH (2016) Robust blind digital watermarking scheme based on contourlet transform and QR decomposition. *J Optoelectronics Laser* 27(3):317–324
14. Roberto HB, Smith MJT (1992) A filter bank for the directional decomposition of image: theory and design. *IEEE Trans Signal Process* 40(4):882–893
15. Sun X, Yi KY, Sun YX (2002) Image encryption algorithm based on chaotic system. *J Comput Aided Des Comput Graph* 14(2):1–4
16. Verma VS, Jha RK, Ojha A (2015) Significant region based robust watermarking scheme in lifting wavelet transform domain. *Expert Syst Appl* 42:8184–8197
17. Wang JW, Li T, Shi YQ, Lian SG, Ye JY (2017) Forensics feature analysis in quaternion wavelet domain for distinguishing photographic images and computer graphics. *Multimed Tools Appl* 76(22):23721–23737
18. Zhan YF, Feng X, Fu C, Bai GT, Ma HF (2012) An efficient medical image cryptosystem based on chaotic maps. *J Digit Content Technol Appl* 6(13):265–274
19. Zhang Y, Qin C, Zhang WM, Liu FL, Luo XY (2018) On the fault-tolerant performance for a class of robust image steganography. *Signal Process* 146:99–111
20. Zheng SL, Wang L, Ling BH, Hu DH (2017). Coverless information hiding based on robust image hashing. 13th International Conference Intelligent Computing (ICIC 2017), Liverpool, UK, August 7-10, p 536-547
21. Zhou YS, Jin W (2011) A novel image zero-watermarking scheme based on DWT-SVD. *IEEE International Conference on Multimedia Technology (ICMT 2011)*:2873–2876
22. Zhou QL, Qiu YB, Li L, Lu JF, Yuan WQ, Feng XQ, Mao XY (2018) Steganography using reversible texture synthesis based on seeded region growing and LSB. *Comput Mater Con* 55(1):151–163
23. Zhu TT, Hu DH, Wang LN (2009) Perceptual hash functions based on contourlet transform and singular value decomposition, 2009 International Conference on Multimedia Information Networking and Security, p 87-90



Xiaoqi Wu was born in 1995. She received the B. D. from Bengbu College. Now she is studying at Hainan University. Her research interests include image processing and medical image watermarking.



Jingbing Li was born in 1966. He received B.S. from Wuhan University of Technology, Wuhan, China, in 1989, the M.S. Beijing Institute of Technology, in 1996, and the Ph.D. degree from Chongqing University, in 2007. In 2006, he joined Zurich University, Switzerland, as a visiting scholar. In 2011, he went to Intelligent Laboratory of Ritsumeikan, Japan, as a visiting scholar. From 2013 to 2014, he was a visiting scholar at Troy University, USA. Now he is a full professor at Hainan University. His research interests include artificial intelligence, network security, image processing, medical image watermarking.



Rong Tu radiology professor in First Affiliated Hospital of Hainan Medical University. Chief physician, Ph.D., Master advisor, expert with State Council special allowance, outstanding teacher in Hainan Province, famous Doctor, Former director of Hainan Province Radiology Committee. Published more than 90 papers, focusing on abdominal imaging diagnosis and molecular imaging.



Jieren Cheng was born in 1974. He received the Ph.D. degree from School of Computer, National University of Defense Technology in 2010. Now he is a professor and graduate supervisor at Hainan University, and the member of CCF. His research interests include cloud computing, artificial intelligence, network security and intelligent transportation, etc.



Uzair Aslam Bhatti received his engineering degree in computer systems in Pakistan. Did Masters in computer science and telecommunication in 2013. Currently pursuing Phd in Hainan University. His area of interest are Health information, Big Data and Artificial intelligence.



Jixin Ma, Henan, China, 1963 He received a PhD degree in Computer Science from the University of Greenwich, London, UK. His research interests include Artificial Intelligence and Graph Matching. He is a member of: the American Association of Artificial Intelligence; the China-Britain Technology and Trade Association (committee member); the World Scientific and Engineering Society; and the UK Temporal Reasoning, Artificial Intelligence and Logic Group.

Affiliations

Xiaoqi Wu¹ · Jingbing Li^{1,2} · Rong Tu³ · Jieren Cheng¹ · Uzair Aslam Bhatti¹ · Jixin Ma⁴

Xiaoqi Wu
xiaoqiwu567@163.com

Jieren Cheng
cjr22@163.com

Uzair Aslam Bhatti
uzairslambhatti@hotmail.com

Jixin Ma
J.Ma@greenwich.ac.uk

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 The First Affiliated Hospital of Hainan Medical University, Haikou 570102, China

⁴ School of Computing & Mathematical Sciences, University of Greenwich, London, UK