




Robust zero-watermarking algorithm for medical images based on SIFT and Bandelet-DCT

Yangxiu Fang¹ · Jing Liu² · Jingbing Li^{1,3}  · Jieren Cheng⁴ · Jiabin Hu¹ · Dan Yi¹ · Xiliang Xiao¹ · Uzair Aslam Bhatti⁵

Received: 15 December 2020 / Revised: 8 April 2021 / Accepted: 31 January 2022 /
Published online: 3 March 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

The gradual improvement of traditional medicare in the cloud has greatly promoted the development of medical enterprise. Meanwhile, problems such as the leakage of patients' personal information, the theft, and tamper of medical images transmitted in the cloud have become increasingly prominent. To solve the above problems, a novel zero-watermarking algorithm for medical images based on bandelet and discrete cosine transform (Bandelet-DCT) is proposed. First, Scale Invariant Feature Transform (SIFT) is performed on the original medical image for extracting the features as the preprocessing step. Second, the chaotic system tent map is used to encrypt the watermark which contained patients' information. Then, Bandelet-DCT is applied to extract the visual feature vectors of medical images. Finally, the watermark embedding and extraction are realized by combining zero-watermarking technology and cryptography related technology. The experimental results show that the proposed algorithm has strong robustness and can effectively solve the problem of information leakage. It has a strong anti-attack ability, good robustness, and certain application prospects.

Keywords Zero-watermarking · Medical images · Bandelet-DCT · Scale invariant feature transform · Robustness

1 Introduction

With the rapid development of information technology, the concept of cloud has gradually become familiar to everyone. Coupled with the arrival and application of 5G technology, it has promoted the rapid development of all walks of life in society. Traditional medical care has gradually become cloud-based, and cloud diagnosis with cloud treatment technologies have become more mature. The new era of smart medical care has arrived, and the intuitive

✉ Jingbing Li
jingbingli2008@hotmail.com

expression ability of images makes medical images (containing private information about the patient's condition) frequently active in the cloud. The convenience of big data in the cloud makes it store more and more private information [5, 20]. However, it is followed by a series of information security problems, such as willfully copying and tampering of medical pictures transmitted in the cloud, disclosure of patient privacy information and so on [3, 24]. Therefore, how to protect the safe transmission of medical image information and protect the patient's privacy, and information is a hot topic for scholars from various countries [4, 24]. And due to the particularity of medical images, any watermark embedding method that causes image changes is unacceptable [9, 19]. Medical image digital watermarking technology is an effective solution. It hides the information that users want to hide in the carrier image so that the image only presents the carrier image information, which has good imperceptibility and robustness. Imperceptibility and robustness are particularly important for the medical image watermarking algorithm [4, 14, 28, 29]. According to the division of the embedding area, digital watermarking can be divided into spatial digital watermarking technology and frequency domain digital watermarking technology. In the process of embedding the watermark, both types of algorithms need to modify the spatial or frequency domain information of the carrier image. At this time, the imperceptibility of the watermark will decrease as the modification intensity increases. If the modification intensity is too small, the robustness of the watermark will decrease [18, 25]. The zero-watermarking technology proposed by Wenquan et al. solved the contradiction between imperceptibility and robustness. Nowadays, commonly used zero-watermarking algorithms are based on discrete cosine transform (DCT) [10, 11, 23], discrete wavelet transform (DWT), scale-invariant feature transform (SIFT), etc. [1, 2, 16, 22] Kabir et al. [7] presents a reliable digital watermarking technique that provides high imperceptibility and robustness for copyright protection using an optimal discrete cosine transform (DCT) psychovisual threshold. The watermark image is constructed by modifying some coefficients according to some rules. Lina Aditi Zear et al. [27] creatively combined three transformations of DCT, DWT and SVD, which greatly improved the robustness of a single algorithm for embedding watermarking. Embedding watermarking with multiple transformation domain methods greatly improved the performance of embedding watermarking algorithms. However, this method changes the pixel matrix of the original image and is not suitable for embedding the medical image watermark. Swaraja K et al. [19] proposed a method to hide the watermark information into the non-interested region of the medical image, which is of great help in detecting whether the medical image has been tampered with, but it is weak in resisting geometric attack in the spatial domain.

The algorithm adopted in this paper is the second-generation bandelet transform. Bandelet algorithm belongs to multi-scale geometric analysis, which is a kind of super-wavelet transform, and can adaptively track image edge features, has a wide range of applications in image feature extraction. Shao Dong et al. [6] proposed a robust watermarking algorithm based on bandelet transform and stable feature point detection. The watermark is embedded in the image stable and robust feature area, which has good imperceptibility and robustness. The disadvantage is that the ability to resist conventional attacks is weak and poor security. Yang Yue Xiang et al. [26] combined the bandelet algorithm and adaptive matrix norm to propose a full-frequency lossless watermarking method, adopting the idea of zero-watermarking. The disadvantage is that there is no corresponding hidden encryption technology, and the ability to resist geometric attack is weak. Liu Xuchong et al. [12] proposed an authentication algorithm based on the bandelet transform, which uses the direction flow between the hidden watermark and the vector generated by the bandelet transform for correlation detection to realize image authentication. The disadvantage is that the algorithm cannot

resist geometric attacks effectively. The above algorithms can't be applied to medical image watermark because they change the visual characteristics of the image to a certain extent.

Therefore, to take into account the invisibility and robustness of the medical image watermarking system, and to improve the ability to resist geometric attacks and conventional attacks, our research is focused on solving these issues. This paper creatively proposed a robust medical image watermarking technology based on Bandelet-DCT and chaotic encryption. It used zero-watermarking technology to extract the features of medical images, and performed watermark embedding and extraction operation on the features. The integrity of the original medical image is perfectly guaranteed, and the preprocessing steps of tent map chaotic encryption and scale-invariant feature rotation transformation on the original image are added, which greatly improved the security of the medical image, the invisibility of watermark and the robustness against conventional attacks and geometric attacks.

2 The fundamental theory

2.1 SIFT (scale-invariant feature transform) preprocessing

Scale-invariant feature transform(SIFT) was proposed by Lowe [15] and proved that it has ideal robustness to the rotation, translation, scaling, and projection transformation. The algorithm is a local feature description operator that uses local image features to extract key points. These key points are the maximum value of the image gray value, which contains information such as the location, size, and direction. Therefore, SIFT is often used for the detection and matching of image feature points. Details as follows:

(a) Extreme values detection in scale-space

The first stage of calculation is to search for image positions on all scales. The Gaussian differential function is used to identify potential points of interest that are invariant to scale and rotation. Suppose $I(x, y)$ represents the input image, and its scale space function $L(x, y, \delta)$ is obtained by convolution of the original image $I(x, y)$ and the variable-scale Gaussian kernel function $G(x, y, \delta)$. The specific formula is:

$$L(x, y, \delta) = G(x, y, \delta) * I(x, y) \quad (1)$$

In order to find the extreme points of the image, by subtracting the adjacent image matrices in the same scale space, the Gaussian difference scale space can be obtained as follows:

$$D(x, y, \delta) = (G(x, y, k\delta) - G(x, y, \delta)) * I(x, y) = L(x, y, k\delta) - L(x, y, \delta) \quad (2)$$

Two adjacent scales are separated by a constant k .

(b) Extract stable feature points

In order to find the extreme point of the DOG function, each pixel has to be compared with all its neighbors to see if it is larger or smaller than all its neighbors [1]. The Gaussian scale space to the Gaussian difference scale space is shown in Fig. 1. The adjacent point is composed of 8 adjacent points of the same scale and 9×2 points of adjacent scales up and down, a total of 26 points [13].

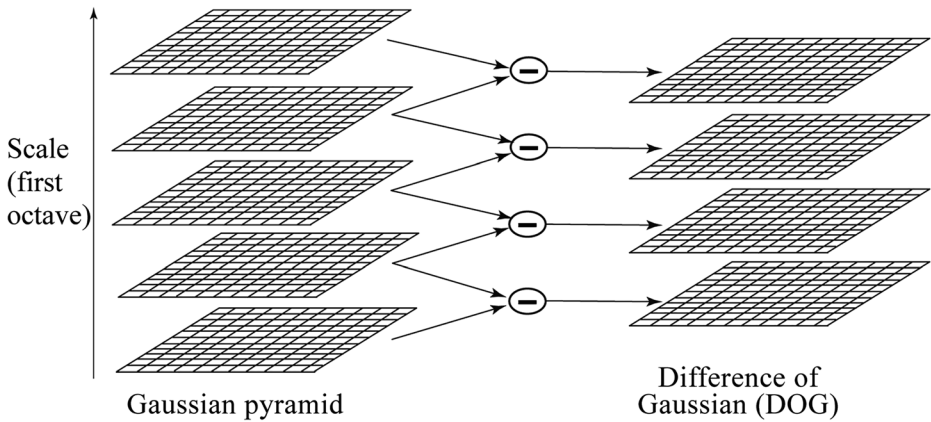


Fig. 1 Gaussian scale space to Gaussian difference scale space

(c) Direction determination

Based on the local gradient direction of the image, one or more directions are assigned to each key point position. All subsequent operations on the image data are transformed relative to the direction, scale and position of the key points, thereby providing invariance to these transformations.

(d) Key point description

In the neighborhood around each key point, the local gradient of the image is measured on the selected scale. These gradients are transformed into a representation that allows relatively large local shape deformation and illumination changes (see Fig. 2).

2.2 Bandelet transformation

The second-generation Bandelet transform was proposed by Peyer and Mallat [17] in 2005. It effectively simplifies the first-generation algorithm and is a multi-scale geometric analysis method. The algorithm is to perform bandelet transform again based on wavelet transform, which can better extract geometric features such as complex textures and edges of the image. There is no edge effect when reconstructing the image, and the algorithm process is simple. It

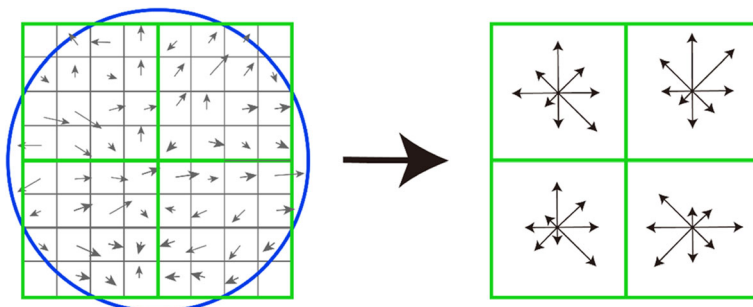


Fig. 2 SIFT feature vector generation

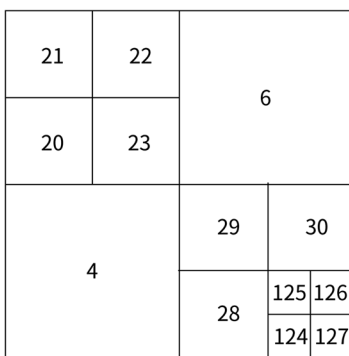
first divides the wavelet coefficients into blocks, and then approximates the geometric flow with a straight line in each sub-block, and realizes the control of the geometric flow with a parameter. This parameter is called the geometric vector line direction flow. The principal flow of the algorithm is as follows:

- (a) Perform two-dimensional discrete orthogonal wavelet multi-scale transform on the image.
- (b) Obtain the Bandelet blocks via divide each sub-band after wavelet transform quadtree divisions (the quadtree segmentation diagram is shown in Fig. 3) to establish the best quad-tree decomposition.
- (c) Bandelet the obtained Bandelet block to obtain the bandelet coefficient. Bandeletization is a reversible transformation of high-frequency sub-band coefficients generated by two-dimensional wavelet transform.
- (d) Arrange the Bandelet coefficients according to the best geometric flow direction to obtain a matrix.

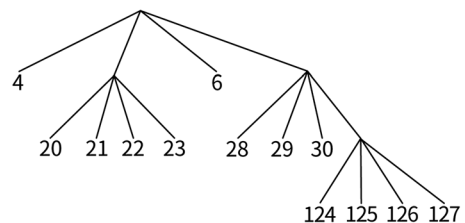
The output result of the algorithm has three items, namely: quadtree, optimal geometric flow direction, and Bandelet coefficient. Among them, the bottom-up global optimization algorithm is adopted, that is, a quadtree optimization segmentation algorithm. The algorithm optimization process is as follows:

Firstly, the optimal geometric flow direction was searched for each $L \times L$ square block S , and the optimal geometric flow direction and the minimum Lagrange function value $L_0(S)$ were obtained; Secondly, Let $L = 2L$, and perform the first step for each square to obtain the corresponding optimal geometric flow direction and the value of Lagrange function $L(S)$; Finally, mark the child nodes of each sub-block as (S_1, S_2, S_3, S_4) . Then:

$$L(S) = L_0(S_1) + L_0(S_2) + L_0(S_3) + L_0(S_4) + L_0(S) + \lambda * T^2 \tag{3}$$



(a)



(b)

Fig. 3 The quadtree segmentation diagram: **a** Binary division; **b** Quadtree segmentation and Leaf node corresponds to the small square label in (a)

The sum of the Lagrange values of the four child nodes is taken as the Lagrange value of the leaf node, and let $L_0(S) = \min \{L_0(S), L(S)\}$, $L_0(S)$ is the result of the quadtree split. On this basis, the best geometric flow direction of the Bandelet block can also be obtained. The geometric flow is optimized by the function of Lagrange. The specific method is as follows: for $L \times L$ small square, the rounded corners $[0, \pi]$ are discretized into $L^2 - 1$. That is, the possible values of θ are $\theta = \frac{k\pi}{L^2-1} (k = 0, 1, \dots, L^2-2)$, The geometric flow direction that makes the Lagrange function value minimum is the optimal geometric flow direction. The schematic diagram of the geometric flow direction in the sub-block is shown in Fig. 4.

Bandelet transform has two advantages compared with wavelet transform: (1) Taking full advantage of geometric regularity, high-frequency sub-band energy is more concentrated, and non-zero coefficients are relatively reduced under the same quantization step; (2) Due to the quadtree structure and geometric flow information, the Bandelet coefficients can be rearranged, and the coefficient scanning mode is more flexible when encoding.

2.3 Discrete cosine transform

Discrete Cosine Transform (DCT) is a special form of Discrete Fourier Transform (DFT). The two-dimensional DCT transform (2D-DCT) formula is shown as follows:

$$\sum_{x=0}^{M-1} \sum_{y=0}^{M-1} f(x,y) \cos \frac{\pi(2x+1)u}{2M} \cos \frac{\pi(2y+1)v}{2N} \quad u = 0, 1, \dots, M-1; v = 0, 1, \dots, N-1; c(u) = \begin{cases} \sqrt{1/M} & u = 0 \\ \sqrt{2/M} & u = 1, 2, \dots, M-1 \end{cases} \quad (4)$$

Through the DCT transformation, the picture pixel matrix is divided into DC (low frequency components) components and AC (medium and high frequency) components. The DC component concentrates more energy, mostly texture and background parts, while the AC component concentrates less energy, mostly sudden changes or details.

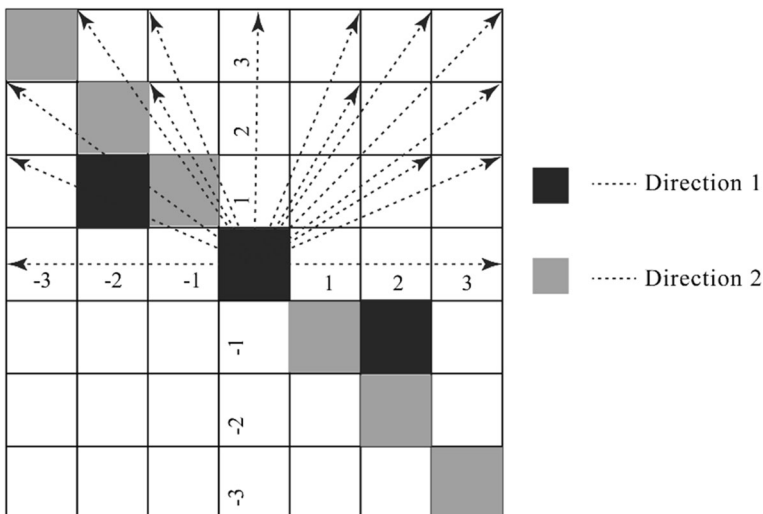


Fig. 4 Schematic diagram of geometric flow direction in sub-block

3 The proposed algorithm

In this paper, Bandelet and DCT transform are combined to propose a medical zero-watermark robustness algorithm based on Bandelet-DCT transform. This algorithm is more robust than simple use of DCT transform in resisting various conventional and geometric image attacks. The whole algorithm includes five parts: image preprocessing, extract visual feature vector of medical image, embed watermark, extract watermark, and restore watermark.

3.1 Image preprocessing

3.1.1 Watermark image preprocessing

To ensure the security of the watermark image and generate an encrypted watermark signal with higher security, we need to construct a higher security information encryption system before embedding the watermark. The chaotic system can be used to preprocess the original watermark image. Commonly used chaotic systems include Logistic mapping, Arnold transform, Tent mapping [8], etc. Among them, Tent mapping has faster iteration speed and better uniformity than Arnold transform and Logistic mapping. The chaotic sequence generated by this chaos has good statistical characteristics. Therefore, the Tent chaotic map is used in this paper. It is defined as follows:

$$x_{n+1} = \begin{cases} \frac{x_n}{\alpha}, & 0 \leq x_n < \alpha \\ \frac{1-x_n}{1-\alpha}, & \alpha \leq x_n < 1 \end{cases} \quad (5)$$

The initial parameters are set to generate the Tent chaotic map sequence $X(j)$. The binary encryption matrix $C(i, j)$ is obtained through the sign function. Then, the hash function is used to process $C(i, j)$ and the binary watermark $W(i, j)$ to obtain the encrypted watermark $CW(i, j)$. Figure 5 described the encryption process of the watermark.

$$CW(i, j) = W(i, j) \oplus C(i, j) \quad (6)$$

3.1.2 Medical image preprocessing

To improve the robustness of the algorithm against attacks, the SIFT preprocessing transformation is performed on the medical image before the feature extraction of the medical image, and the local feature invariant region $IR(i, j)$ of the original medical image is established.

3.2 Extract visual feature vector of medical image

As its particularity, the medical image cannot change any information. Therefore, zero-watermarking technology is used to embed the watermark, and Bandelet-DCT is performed on the original medical image. In the low-frequency coefficient matrix, 32-bit data is selected to form a symbol sequence, which is quantized (more than the symbol sequence average value is “1”, otherwise, it is “0”) as the medical image feature vector $HV(j)$. As shown in Table 1, to verify the effectiveness of the proposed visual characteristic sequence of the original image

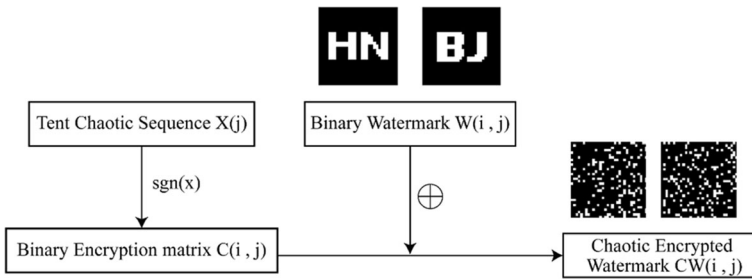


Fig. 5 The encryption scheme for the watermark

recognition, various attacks are performed on these vectors, and the normalization coefficient NC values are all equal to 1.0. We can see that the vector of the images proposed in this paper will not change with the attacks. To further verify the proposed visual feature sequences can well distinguish the different medical images, we perform a cross-validation test on different medical images (see Fig. 6). As shown in Table 2, the NC values are all less than 0.5 which mean that the proposed vector can distinguish different images. Hence, the symbol sequence proposed by this algorithm can be the visual feature of medical images (For better presentation in the table, only 9 digits of the coefficient matrix are shown).

3.3 Embed watermark

Do XOR operation on the obtained medical image feature vector $HV(j)$ and the encrypted watermark $CW(j)$ sequence to complete the watermark embedding process. The key $Wkey(i, j)$ generated after embedding can be stored in IPR (Intellectual Property Rights) database for the authentication and protection of medical images. Figure 7 described the process of feature extraction and watermark embedding.

3.4 Extract watermark AND restore watermark

After attacked, the tested medical image $I' (i, j)$ is obtained. The watermark extraction process is opposite to the embedding process. Figure 8 shows the watermark extraction process. To restore the watermark, the same initial parameters must be obtained and set to generate the same Tent map chaotic mapping sequence $X(j)$, the binary encryption matrix

Table 1 Bandelet-DCT coefficient changes of original medical images under various attacks

Image Manipulation	Sequence of coefficient signs	NC
Original image	0 1 1 0 0 0 0 0	1.00
Gaussian noise (5%)	0 1 1 0 0 0 0 0	1.00
JPEG compression (10%)	0 1 1 0 0 0 0 0	1.00
Median filter [5×5](10 times)	0 1 1 0 0 0 0 0	1.00
Translation (15%, right)	0 1 1 0 0 0 0 0	1.00
Translation (15%, up)	0 1 1 0 0 0 0 0	1.00
Block cropping (upper left, 1/8)	0 1 1 0 0 0 0 0	1.00
Rotation (clockwise, 20%)	0 1 1 0 0 0 0 0	1.00

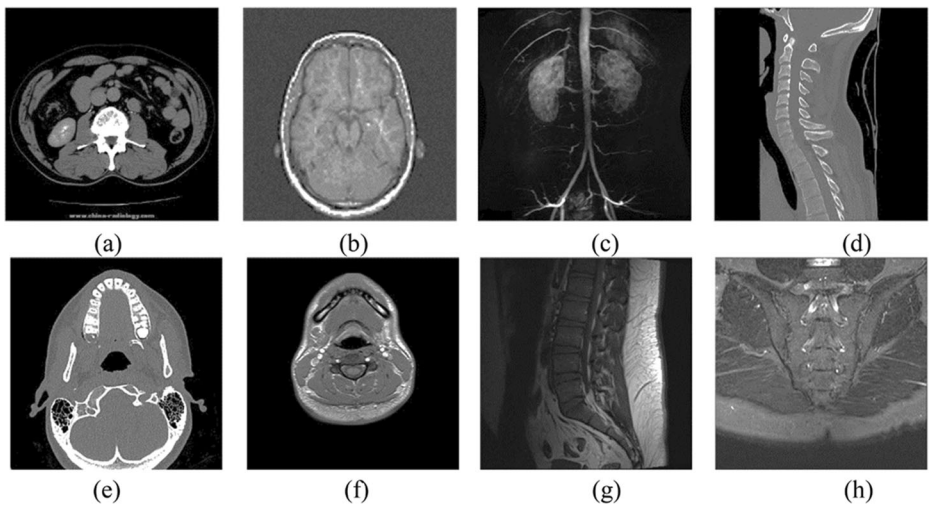


Fig. 6 Medical images for watermarking: **a** Abdomen; **b** Brain; **c** Lung; **d** Cervical Spine; **e** head MRI; **f** Neck; **g** Lumbar spine; **h** Sacroiliac

$C(i, j)$ is obtained through the sign function, and then the hash function is used to process $C(i, j)$ and the extracted binary watermark $CW'(i, j)$ to obtain the restored watermark $W'(i, j)$. Figure 9 shows the restoration of the watermark.

$$W'(i, j) = C(i, j) \oplus CW'(i, j) \tag{7}$$

4 Experiments and results

To verify the effectiveness of the algorithm, a 512×512 pixel medical image (see Fig. 10a) and a $32 \text{ pixel} \times 32 \text{ pixel}$ binary watermark image (see Fig. 10b) is selected for experiments, and use peak signal-to-noise ratio (PSNR) [21] and normalized correlation coefficient (NC) [21] to evaluate the robustness of the algorithm against attacks, the simulation platform is MATLAB R2016a. In the experiment, we carried out various common attacks and geometric attacks on images embedded with watermarks. Figure 10c shows the chaotic encrypted watermark image, the initial value of the chaotic encryption $a = 0.8, x(1)=0.34$, and Fig. 10d shows the embedded watermarked medical image in the state of no attacks.

Table 2 Medical image cross-validation NC value

NC	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
(a)	1.0000	0.1260	0.0000	0.0159	0.0552	-0.0882	0.0401	0.0976
(b)	0.1260	1.0000	0.1250	-0.1260	-0.0626	-0.1909	-0.0636	0.0000
(c)	0.0000	0.1250	1.0000	0.1260	-0.0626	0.1909	0.1909	0.1291
(d)	0.0159	-0.1260	0.1260	1.0000	0.3235	0.3447	0.2164	0.1627
(e)	0.0552	-0.0626	-0.0626	0.3235	1.0000	0.1156	0.3706	0.0485
(f)	-0.0882	-0.1909	0.1909	0.3447	0.1156	1.0000	-0.0364	0.2793
(g)	0.0401	-0.0636	0.1909	0.2164	0.3706	-0.0364	1.0000	0.0164
(h)	0.0976	0.0000	0.1291	0.1627	0.0485	0.2793	0.0164	1.0000

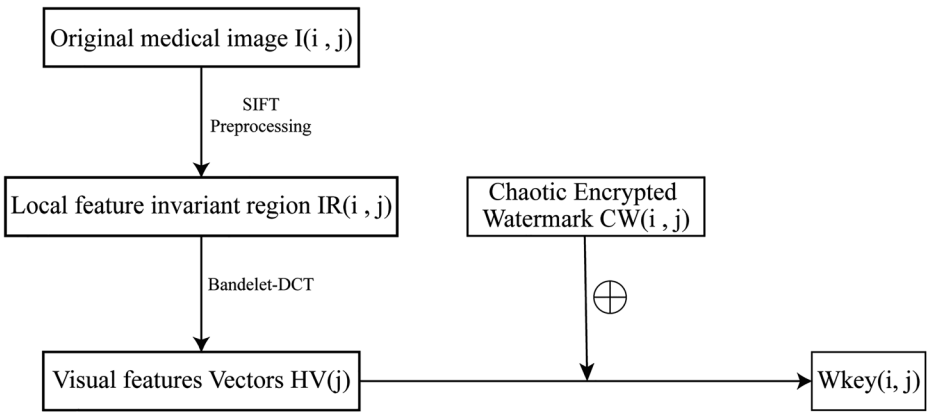


Fig. 7 Feature extraction and watermark embedding

$$PSNR = 10 \log_{10} \frac{MN \max_{i,j} (I_{(i, j)})^2}{\sum_i \sum_j (I_{(i, j)} - I'_{(i, j)})^2} \tag{8}$$

$$NC = \frac{\sum_i \sum_j W_{(i, j)} W'_{(i, j)}}{\sum_i \sum_j W_{(i, j)}^2} \tag{9}$$

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 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.

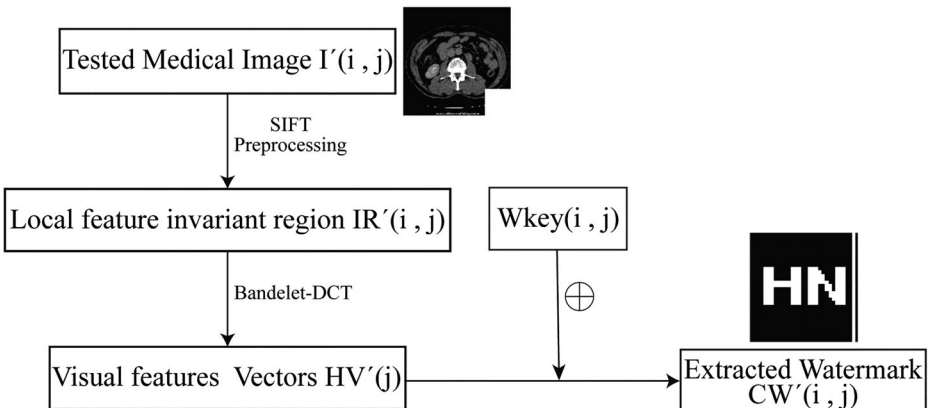


Fig. 8 The extraction process of the watermark

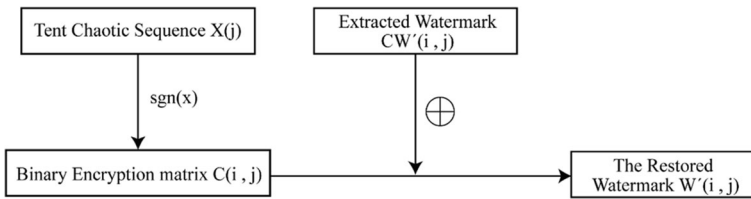


Fig. 9 Watermark restoration algorithm

4.1 Common attacks

To test the robustness of the algorithm, we perform common attacks on the test watermarked medical images, the specific performance of the algorithm is shown in Table 3. When the Gaussian noise intensity reaches 30%, the NC value is still greater than 0.5 to 0.78, and the extracted watermark can still be distinguished; Even if the JPEG compression quality reaches only 1% of the original image, the NC value is still 1.00; When the median filter of $[7 \times 7]$ is repeated 10 times on the test image, the NC value can also reach 0.88, which shows that the algorithm has strong robustness against common attacks. In Fig. 11, some test watermarked medical images and corresponding extracted watermarked images under common attacks are given.

4.2 Geometrical attacks

Geometric attacks on medical images are easier to do than common attacks, so the robustness of the algorithm against geometric attacks is crucial. In Table 4, we show the performance of test images under common geometric attacks. From the data in the table, we can see the significant advantages of this algorithm. When the image is subjected to a high-intensity geometric attack, such as the rotation degree reaches 24 degrees, the downward translation reaches 24%, and the square cropping reaches 1/4, the value of NC can still be maintained above 0.5, and the extracted watermark image features are distinguishable (see Fig. 12). Therefore, the algorithm is also very robust to geometric attacks.

4.3 Comparison with other algorithms

In this paper, we compared this algorithm with the other two algorithms, respectively comparing the single DCT zero-watermarking algorithm and Bandelet zero-

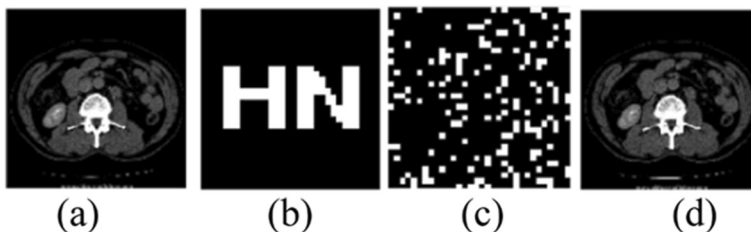


Fig. 10 Medical pictures and watermarks: **a** original medical image; **b** original binary watermark; **c** encrypted watermark; **d** watermarked medical image

Table 3 The data under common attacks

Common attacks	Intensity of attacks	PSNR/dB	NC
Gaussian noise	1%	21.99	1.00
	15%	11.08	1.00
	30%	8.78	0.78
JPEG compression	1%	25.64	1.00
	4%	27.18	1.00
	30%	34.53	1.00
Median filter (10 times)	[3×3]	29.17	1.00
	[5×5]	25.79	0.89
	[7×7]	23.61	0.88

watermarking algorithm. Detailed comparison results are given in Tables 5 and 6. In the two tables, we can clearly see that the Bandelet-DCT algorithm in this paper is more robust against JPEG compression and geometric attacks than the Bandelet algorithm alone. In terms of translation attack, square cropping, and rotation attack, the robustness of the algorithm in this paper is far stronger than that of the independent DCT zero-watermarking algorithm. On the whole, the robustness of the algorithm in this paper is better than the independent Bandelet zero-watermarking algorithm and DCT zero-watermarking algorithm.

To further verified the superiority of the algorithm, it was compared with the algorithm in Ref. [24] and Ref. [13]. For ease of comparison, we used the images consistent with the references as the original images. We used the algorithms proposed in the literature to extract the features of the images that have experienced the same attacks. From Fig. 13, we can saw

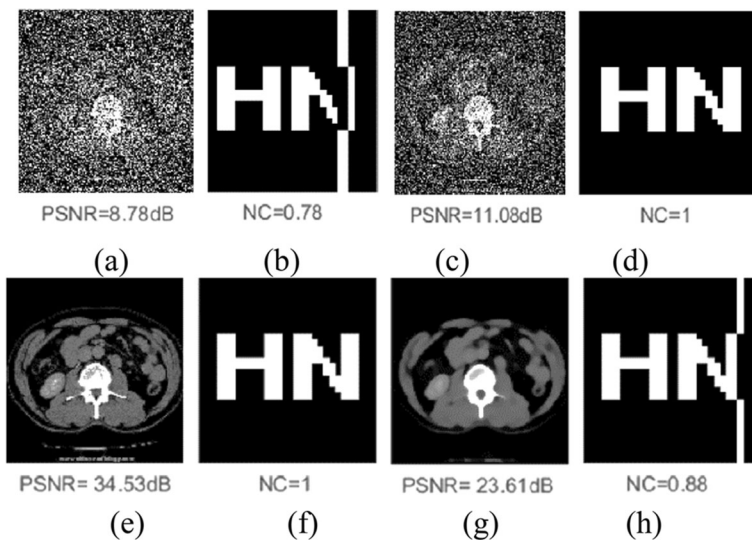


Fig. 11 Medical Images under common attacks: **a** Gaussian noise level of 30%; **b** the extracted watermark under Gaussian noise level of 30%; **c** Gaussian noise level of 15%; **d** the extracted watermark under Gaussian noise level of 15%; **e** JPEG compression quality 30%; **f** the extracted watermark under compression quality 30%; **g** median filter [7 × 7], 10 times; **h** the extracted watermark under median filter [7 × 7], 10 times

Table 4 The data under geometrical attacks

Geometrical attacks	Intensity of attacks	PSNR/dB	NC
Rotation (clockwise)	6°	17.95	1.00
	16°	15.86	1.00
	24°	15.08	1.00
Scaling	×0.2	-	1.00
	×0.8	-	1.00
	×1.8	-	1.00
Down translation	4%	15.67	1.00
	14%	13.18	1.00
	24%	12.01	0.88
Left translation	7%	14.53	1.00
	14%	13.16	0.88
	23%	12.5	0.88
Cropping attacks	Upper left (1/16)	-	1.00
	Upper left (1/4)	-	0.89
	Center (1/4)	-	0.52

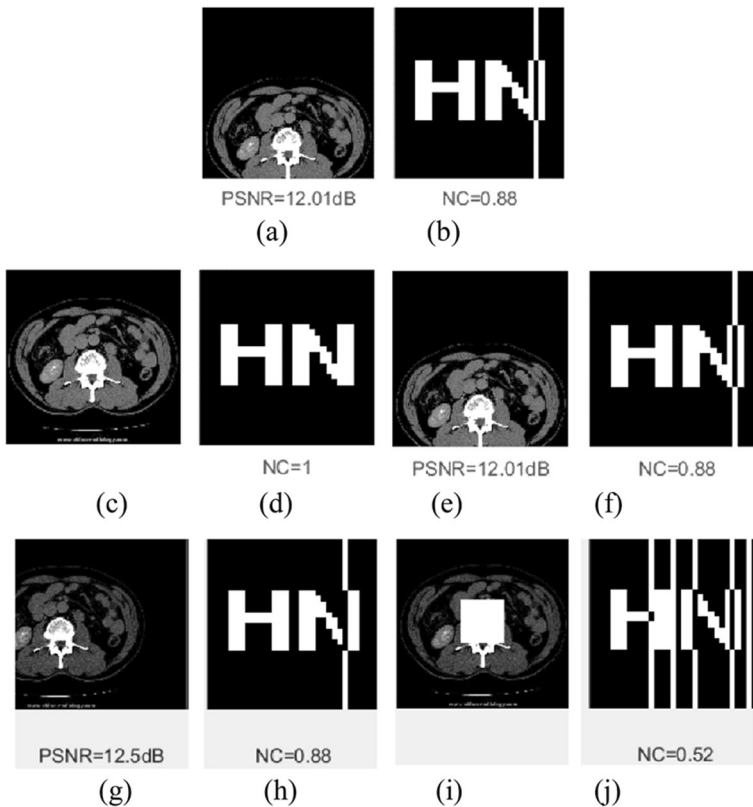


Fig. 12 Images under geometrical attacks: **a** Rotation (clockwise) 24°; **b** the extracted watermark under rotation (clockwise) 24°; **c** Scaling factor 2.0; **d** the extracted watermark under scaling factor 2.0; **e** down distance 24%; **f** the extracted watermark under down distance 24%; **g** left distance 23%; **h** the extracted watermark under left distance 23%; **i** Center square cropping 25%; **j** the extracted watermark under center square cropping 25%

Table 5 The comparison values of PSNR and NC under common attacks

Common attacks	Intensity of attacks	PSNR/dB	Bandelet NC1	DCT NC2	Bandelet-DCT NC3
Gaussian noise	5%	15.36	0.88	0.80	1.00
	10%	12.62	0.66	0.80	1.00
	30%	8.78	0.69	0.73	0.78
JPEG compression	2%	25.64	0.66	0.81	1.00
	10%	30.58	0.48	1.00	1.00
	30%	34.53	0.48	1.00	1.00
Median filter (10 times)	[3×3]	29.17	1.00	1.00	0.89
	[5×5]	25.79	0.79	1.00	0.89
	[7×7]	23.61	0.79	0.89	0.88

Table 6 The comparison values of PSNR and NC under geometrical attacks

Geometrical attacks	Intensity of attacks	PSNR/dB	Bandelet NC1	DCT NC2	Bandelet-DCT NC3
Rotation(clockwise)	10°	16.68	0.57	0.68	1.00
	20°	15.34	1.00	0.32	1.00
	40°	14.64	0.48	0.21	1.00
Scaling	×0.4	-	0.74	1.00	1.00
	×1.4	-	0.72	1.00	0.70
	×2.0	-	1.00	1.00	1.00
Down translation	5%	15.32	0.52	0.71	1.00
	15%	13.07	0.60	0.27	1.00
	25%	11.98	0.47	0.23	0.69
Left translation	6%	14.66	0.54	0.50	1.00
	15%	13.06	0.54	-0.10	0.88
	30%	12.25	0.90	-0.11	0.78
Cropping (Square)	Upper left (1/8)	-	1.00	0.19	1.00
	Middle (1/8)	-	0.38	0.67	0.78
	Bottom right (1/4)	-	1.00	0.35	0.90

that the NC values of the proposed algorithm were higher than those of the comparative literature. We take the average value of all kinds of attacks and get an average NC value, which can better reflect the superiority of the proposed algorithm.

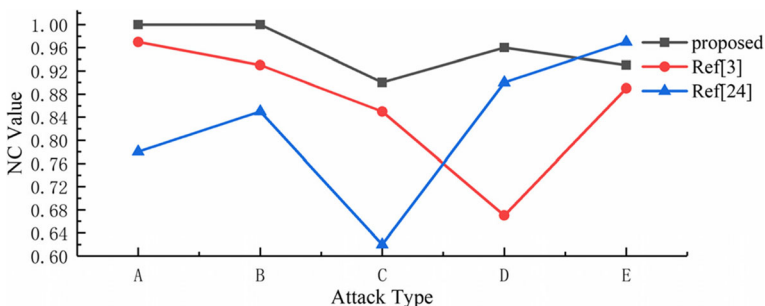


Fig. 13 The NC value of comparative analysis results under the different attacks: A to E respectively represent the attacks: Gaussian noise, JPEG compression, Median filter (10 times), Rotation (clockwise), Translation (left)

5 Conclusion

This paper proposed a robust watermarking algorithm for medical images based on Bandelet-DCT, which combined cryptographic algorithms, tent map chaotic sequences, and third-party database authentication protection. It greatly improved the security performance of the algorithm. Moreover, the scale-invariant feature transformation preprocessing process was creatively added in terms of feature extraction, and the optimized bandelet transform and discrete cosine transform were used to extract the visual features of the original image. The experimental results show that the algorithm is robust to both common attacks and geometric attacks, and achieves the requirement of zero-watermarking in extracting watermarks, that is, no original medical images are required. Therefore, the algorithm can be used on special occasions such as medical images that have strict requirements on image quality. In the next step of research, the algorithm will improve its robustness to other cropping attacks except square cropping.

Acknowledgments This work was supported in part by the Natural Science Foundation of China under Grant 62063004 and 61762033, in part by the Hainan Provincial Natural Science Foundation of China under Grant 2019RC018 and 619QN246, by the Postdoctoral Science Foundation under Grant 2020TQ0293, by the Science and Technology Research Project of Chongqing Education Commission Under Grant KJQN201800442, and by the General Project of Chongqing Natural Science Foundation Under Grant cstc2020jcyj-msxmX0422.


References

1. Ahmad RM, Yao X, Nawaz SA, Bhatti UA, Mehmood A, Bhatti MA, Shaukat MU (2020) Robust image watermarking method in wavelet domain based on SIFT features. In: Proceedings of the 2020 3rd International Conference on Artificial Intelligence and Pattern Recognition. pp. 180–185. Association for Computing Machinery, New York, NY, USA
2. Ambadekar SP, Jain J, Khanapuri J (2019) Digital image watermarking through encryption and DWT for copyright protection. In: Bhattacharyya S, Mukherjee A, Bhaumik H, Das S, Yoshida K (eds) Recent trends in signal and image processing. Springer, Singapore, pp 187–195
3. Aparna P, Kishore PVV (2020) A blind medical image watermarking for secure E-healthcare application using crypto-watermarking system. *J Intell Syst* 29:1558–1575
4. Balasamy K, Shamia D (2021) Feature extraction-based medical image watermarking using fuzzy-based median filter. *IETE J Res*:1–9
5. Balasamy K, Suganyadevi S (2021) A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD. *Multimed Tools Appl* 80:7167–7186
6. Dong S (2019) Robust image watermarking algorithm based on the second generation Bandelet transform and stable feature detection. *Comput Appl Softw* 36:302–310
7. Ernawan F, Kabir MN (2018) A robust image watermarking technique with an optimal DCT-Psychovisual threshold. *IEEE Access* 6:20464–20480
8. Hu Y-C, Lo C-C, Chen W-L, Wen C-H (2013) Joint image coding and image authentication based on absolute moment block truncation coding. *JEI* 22:013012
9. Khare P, Srivastava VK (2021) A secured and robust medical image watermarking approach for protecting integrity of medical images. *Trans Emerg Telecommun Technol* 32:e3918
10. Leng L, Zhang J, Xu J, Khan MK, Alghathbar K (2010) Dynamic weighted discrimination power analysis in DCT domain for face and palmprint recognition, (pp. 467–471). *IEEE*
11. Leng L, Li M, Kim C, Bi X (2017) Dual-source discrimination power analysis for multi-instance contactless palmprint recognition. *Multimed Tools Appl* 76:333–354
12. Liu X-C, Luo Y, Wang J-X, Wang J (2010) Watermarking algorithm for image authentication based on second generation Bandelet. *J Commun* 31:123–130

13. Liu J, Li J, Chen J, Zou X, Cheng J, Liu J (2018) Medical image watermarking based on SIFT-DCT perceptual hashing. In: Sun X, Pan Z, Bertino E (eds) *Cloud computing and security*. Springer International Publishing, Cham, pp 334–345
14. Liu J, Li J, Cheng J, Ma J, Sadiq N, Han B, Geng Q, Ai Y (2019) A novel robust watermarking algorithm for encrypted medical image based on DTCWT-DCT and chaotic map. *Comput Mater Continua* 61:889–910
15. Lowe DG (2004) Distinctive image features from scale-invariant Keypoints. *Int J Comput Vis* 60:91–110
16. Luo H, Sun X, Yang H, Xia Z (2011) A robust image watermarking based on image restoration using SIFT. *Radioengineering* 20:8
17. Peyre G, Mallat S (2005) Discrete bandelets with geometric orthogonal filters. In: *IEEE International Conference on Image Processing 2005*. p. 1–65
18. Su Q, Liu D, Yuan Z, Wang G, Zhang X, Chen B, Yao T (2019) New rapid and robust color image watermarking technique in spatial domain. *IEEE Access* 7:30398–30409. <https://doi.org/10.1109/ACCESS.2019.2895062>
19. Swaraja K, Kollati M, Kora P (2019) An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. *Biomed Signal Process Control* 55: 101665
20. Swaraja K, Meenakshi K, Kora P (2020) An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. *Biomed Signal Process Control* 55:101665
21. Thakur S, Singh AK, Ghrera SP, Dave M (2018) Watermarking techniques and its applications in telehealth: A technical survey. In: *Cryptographic and Information Security Approaches for Images and Videos* by S. Ramakrishnan Chapter –17, pp. 467–511
22. Vishwakarma VP, Sisaudia V (2018) Gray-scale image watermarking based on DE-KELM in DCT domain. *Procedia Comput Sci* 132:1012–1020
23. Wen Q, Sun T-F, Wang S-X (2003) Concept and application of zero-watermark. *ACTA Electron Sin* 214–216
24. Wu X, Li J, Tu R, Cheng J, Bhatti UA, Ma J (2019) Contourlet-DCT based multiple robust watermarks for medical images. *Multimed Tools Appl* 78:8463–8480
25. Wu D, Tang Y, Zhao W, Wan Y, Qu C (2020) Zero-watermarking algorithm based on Curvelet-DWT-SVD. *J Yanshan Univ* 44:38–48
26. Yang Y, Luo Y, Ye Z, Cheng L (2007) A complete frequency lossless watermarking method via bandelet and adaptive matrix norm. *J Comput Res Dev* 44(12):1996
27. Zear A, Singh AK, Kumar P (2018) A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimed Tools Appl* 77:4863–4882
28. Zhang L, Wei D (2019) Dual DCT-DWT-SVD digital watermarking algorithm based on particle swarm optimization. *Multimed Tools Appl* 78:28003–28023
29. Zou B, Du J, Liu X, Wang Y (2018) Distinguishable zero-watermarking scheme with similarity-based retrieval for digital rights Management of Fundus Image. *Multimed Tools Appl* 77:28685–28708

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

Affiliations

Yangxiu Fang¹ · Jing Liu² · Jingbing Li^{1,3}  · Jieren Cheng⁴ · Jiabin Hu¹ · Dan Yi¹ · Xiliang Xiao¹ · Uzair Aslam Bhatti⁵

Yangxiu Fang
FangYangXiu@hainanu.edu.cn

Jing Liu
liujinglj@zhejianglab.edu.cn

Jieren Cheng
cjr22@163.com

Jiabin Hu
18085208210009@hainanu.edu.cn

Dan Yi
Yidan@hainanu.edu.cn

Xiliang Xiao
xiaoxiliang1997@163.com

Uzair Aslam Bhatti
uzairaslambhatti@hotmail.com

¹ School of Information and Communication Engineering, Hainan University, Haikou, Hainan, People's Republic of China

² Research Center for Healthcare Data Science, Zhejiang Lab, Hangzhou, Zhejiang, People's Republic of China

³ State Key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou, Hainan, People's Republic of China

⁴ School of Computer Science and Cyberspace Security, Hainan University, Haikou, Hainan, People's Republic of China

⁵ School of Geography (Remote sensing and GIS Lab), Nanjing Normal University, Nanjing, Jiangsu, People's Republic of China