Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH Open Access

A robust encryption watermarking algorithm for medical images based on ridgelet-DCT and THM double chaos

Zilong Liu[1,2], Jingbing Li[1*], Yang Ai[3], Yuancai Zheng[4] and Jing Liu[5]

Abstract

With the help of big data, cloud computing, artificial intelligence and other technologies, the informatization and intelligence of the wisdom medical have been gradually realized. However, with the transmission and storage of massive amounts of medical images in the cloud, information security issues have become increasingly prominent. The privacy of patients is at risk of disclosure, theft and tampering, which has become an important challenge restricting the development of wisdom medical. How to protect the personal information of patients in the cloud environment has become an urgent problem to be solved. Medical image watermarking technology is an effective method to solve this problem. Combining the characteristics of Tent chaos and Henon chaos, this paper designed a Tent-Henon-Map double chaos watermarking encryption method and designed a medical image encryption watermarking algorithm based on ridgelet-DCT transform. The watermark images were encrypted by the Tent-Henon-Map double chaos which had the characteristics of sensitive initial values and large key space. Then, the feature vectors of the medical images were extracted through ridgelet-DCT transform. On the basis of ordinary watermarking technology, combined with zero watermarking, third-party concepts, and cryptographic technology, watermarking had a good ability to resist image processing attacks. The experimental results showed that the key space of the algorithm was 10^{116}, which had better encryption and hard to crack. The time of watermark embedding and extraction were only 0.336 s and 0.439 s, with lower computational cost. And under high-strength conventional attacks and geometric attacks, the NC values of the algorithm were all greater than 0.55, which could effectively extract watermark information. It shown that the algorithm proposed had good robustness against conventional and geometric attacks It shown that the algorithm proposed had good robustness against conventional and geometric attacks, while taking into account the security.

Keywords: Medical image, Watermarking, Ridgelet-DCT, THM

Introduction

With the rapid development of 5G, big data, cloud computing technology, and artificial intelligence, the service model of "Internet + medical imaging" has gradually become popular, and it becomes an important driving force for the construction of the wisdom medical [1]. The "Internet + Medical Imaging" platform can help doctors and patients quickly and conveniently grasp diagnosis and treatment information, and provide a full range of medical services [2]. "Internet + medical imaging" promotes the development of the wisdom medical and realizes online and offline linkages between doctors and patients, while also bringing new challenges to the medical industry. Among them, the personal privacy problem of medical information is particularly prominent. To facilitate diagnosis, doctors often embed the personal information of patients into medical images

*Correspondence: jingbingli2008@hotmail.com

[1] School of Information and Communication Engineering, Hainan University, Haikou 570228, China
Full list of author information is available at the end of the article

directly. These medical images are transmitted and stored in the cloud environment, which will easily cause the leakage and tampering of personal information, and bringing great security risks. How to protect personal privacy information in medical images is an important factor restricting the development of "Internet + Medical Imaging" [3]. Medical image watermarking is an effective method to solve this problem [4]. The medical image watermarking is different from that of general images. In view of the sensitivity of medical images, the diagnosis information contained in the medical images cannot be changed when they are embedded with the watermark information. Therefore, the organic combination of digital watermarking technology and medical images can realize the protection of the "region of interest" information in the original medical images while hiding the personal information in the medical images. The research of medical images encryption watermarking algorithm has good anti-geometric attack and anti-conventional attack ability while taking into account better robustness. It achieves the dual purpose of protecting medical image data and patient privacy information. And it has extremely important theoretical research significance and practical application value [5, 6].

Literature survey

In recent years, there are a lot of research on digital watermarking of medical images, and medical watermarking algorithms had been widely developed and applied. By the spatial domain, Jobin Abraham [7] generated a fragile watermark that could better resist noise attacks, by the least significant bit (LSB) algorithm [8]. Ghassan N. Mohammed [9] proposed watermarking images algorithm based on DISB model, and in this method, two bits were embedded in each pixel of the original image. In the case of high watermark image quality, the proposed model had better robustness and was superior to the LSB algorithm. However, the robustness of this algorithm was poor in strong conventional attacks and geometric attacks. Akram Zeki [10] proposed an intermediate significant bit (ISB) watermark embedding method through pixel replacement. The algorithm had good robustness in compression and noise attacks, but it still could not effectively resist geometric attacks.

By the transform domain, various transformations such as DCT [11, 12], DFT [13, 14], DWT [15, 16] and SVD [17, 18] were mainly used to convert the original images into the frequency domain, and then inverted after embedding watermark. Compared with the spatial domain method, the transform domain methods could embed more information without destroying the value of the original images. However, although one single transform domain method could resist some conventional and geometric attacks, the robustness was still not satisfactory.

In order to improve the resistance of watermarking algorithm to conventional attacks and geometric attacks, and improve the robustness of the algorithm, the methods of hybrid domain [5, 6] were proposed on the basis of transform domain. At present, watermarking methods based on hybrid domains had become the mainstream of current watermarking algorithms. Hybrid transform domain technology could improve the overall anti-attack ability and robustness of the watermarking algorithms. At the same time, they also increased the computational complexity. Based on NSPD-DCT, Rui Wang [19] proposed a zero watermarking scheme against rotation attacks, and it had strong robustness to various attacks. Jing Liu [20] proposed an encrypted watermarking algorithm in the DTCWT-DCT domain combined with Henon Map. The algorithm could embed multiple watermarks at the same time, and has better anti-attack ability while taking into account encryption watermarks. Siming Xing [21] proposed an algorithm to improve the security of watermark information, by scrambling the watermark information with Arnold transform. The algorithm had good robustness against image processing attacks such as clipping attack and rotation attack. The DWT-SVD algorithm was proposed by Zermi Narima [22], applied DWT to retinal images and SVD to LL subbands. It had strong robustness against noise attack, but performed poorly for scaling attacks, rotation attacks. Balasamy K [23] proposed a watermarking method based on fuzzy region of interest (ROI) and DWT to embed encrypted watermark. This algorithm had high security and could resist conventional attacks, but it was less robust to geometric attacks. Kahlessenane Fares [24] proposed two watermarking methods "DCT-Schur" and "DWT-Schur", among which "DCT-Schur" had better robustness against JPGE compression attacks. "DWT-Schur" had stronger anti-attack ability to 0.01 Gaussian noise. These two methods were poor in anti-scaling attacks and anti-average filtering attacks. Based on RSA pseudo-random sequences and Curvelet-DCT, Fengming Qin [25] proposed a robust zero-watermark algorithm, which had better performance in both conventional attacks and geometric attacks. Bandelet-DCT was applied to extract the visual feature vectors of medical images, Yangxiu Fang [26] proposed a novel zero-watermarking algorithm for medical images. It combined Scale Invariant Feature Transform (SIFT) at the preprocessing step on the original medical image extracting the features and had strong robustness. Cheng Zeng [27] proposed a zero watermarking medical image based on KAZE-DCT, and it had good robustness against both common attacks and geometric attacks. Rohit Thanki [28] proposed a hybrid blind watermarking scheme. The scheme was based on DCuT and RDWT, which was robust against noise attacks and JPEG, and the embedded watermark was highly invisible. After that, Rohit Thanki [29] embedded the patient's secret identity into medical images by combining ridgewave transform(FIT) and SVD to realize identity recognition and authentication. And it used Arnold scrambling encryption method to encrypt medical images containing watermarks. This scheme improved the effective load capacity of existing watermarking schemes, and had better robustness to conventional attacks, but the resistance of this algorithm to geometric attack was not ideal. A novel blind Zero code named KeySplitWatermark was proposed by Celestine Iwendi [30]. It was based on watermark detection approach, and used keywords to make segments of the code to produce a key-dependent on the watermark, that could protect software against cyber-attacks. Based fractional-order radial harmonic Fourier moments (FoRHFMs), Zhiqiu Xia [31] proposed a zero-watermarking algorithm to achieve lossless copyright protection of medical images, that had high robustness to geometric attacks and common attacks. Baowei Wang [32] proved the feasibility of combining the zero-watermark algorithm with blockchain technology to improve the security of the zero-watermark algorithm. Using a deep learning-based chaotic logistic map, Ch. Rupa [33] proposed a secure multimedia transformation approach. It used ResNet model to perform classification for identifying the fake medical multimedia data, and could against various cyber-attacks and had high entropy levels.

It could be found that these watermarking algorithms above could protect watermark information well in cloud environment, and they could resist Gaussian attack, median filter attack, JPGE compression and other conventional attacks well. The anti-geometric attack was the research focus and difficulty of watermarking algorithms. Most of these algorithms could resist two or more geometric attacks and had good robustness. Baowei et al. [32] combined blockchain technology with zero watermarking to further improve the security of the watermarking algorithm. Combined with the obfuscated sequence, [33] used ResNet-50 to realize the encryption conversion of information, which provides a new idea for the embedding and extraction of watermarks. But for the encryption of watermarks, [20, 23, 25–27] used chaos theory to encrypt, the algorithms were single and small key spaces, and had a risk of being cracked. Siming et al. [21], Thanki et al. [28], Thanki and Kothari [29] used Arnold transform to encrypt, which kept the image area invariant and had a certain degree of security. However, these methods retained the pixel characteristics of the original images and required a large amount of calculation. The evaluation criteria for measuring the degree of image scrambling were difficult to be unified, and it was periodic. For conventional attacks, [24, 28] had poor robustness to average filter attacks. Wang et al. [19], Siming et al. [21], Balasamy and Suganyadevi [23], Fares et al. [24], Fengming et al. [25], Thanki and Kothari [29], Zhiqiu et al. [31] had better robustness for low noise intensity (such as Gaussian noise intensity lower than 0.1), but when the noise intensity increased after reaching a certain level (such as the Gaussian noise intensity was higher than 0.2), the robustness of the algorithms were decreased. For geometric attacks, [23, 29] had low robustness under geometric attacks. Jing et al. [20], Siming et al. [21] could resist most types of geometric attacks, but they performed poorly on translation attacks. Narima et al. [22] had better robustness to rotation attacks (less than 5 degrees). When the rotation angle was increased, the robustness of the algorithms would decrease a lot. It could be seen that searching for medical watermarking algorithms that could effectively resist geometric attacks and high-intensity noise attacks had always been a puzzle for researchers. KeySplitWatermark [30] was too dependent on the programming language. If the code changed greatly or the programming languages was changed, it would cause great damage to the watermark. And resNet-50 network model [32] requires high computing power and takes a long time, and the robustness of the algorithm was greatly affected by adversarial example.

Based on these researches, and in order to balance encryption and attack resistance, this paper proposed a robust algorithm of tent-Henon-Map (THM) double chaotic cryptographic watermarking based on ridgelet-DCT. Based on the common watermarking technology, the algorithm combined the third party concept, chaos encryption technology to achieve the "zero watermarking" embedding of medical images and blind extraction of watermarking information. And it could effectively resist conventional attacks and geometric attacks while taking into account confidentiality, invisibility and robustness.

The main contributions in this paper were:

1. Based on ridgelet-DCT, it proposed a new feature extraction method of medical images which did not require any modification to the original image. The algorithm had better invisibility and robustness, and at the same time it could resist conventional attacks and geometric attacks.
2. It had low requirements on the quality of the original image, and had a high embedding rate and good

payload. And the embedding of the watermark could be achieved by using a key stored in a third party, without selecting the region of interest, which could effectively protect patient privacy. It did not need the original image to extract the watermarks, only to use the key and the embedded watermark image to extract the watermark and decrypt it.

3. Combined the advantages of Tent Map and Henon Map, a THM double chaotic encryption system was proposed. The encryption system was sensitive to the initial values, easy to implement, and had a large key space, which enhanced the security of the watermark.

The fundamental theory

Ridgelet transform theory

The radon transform

Radon transform was proposed by Radon in 1917. It has good anti-noise performance and is widely used in medical image processing. The function $g(x, y)$ represents the pixel of the point (x, y) in image I, and map a certain straight line $t = x\cos\theta + y\sin\theta$ in the space to a point (t, θ) in Radon space, then the two-dimensional Radon transform of the image is shown as Eq. (1).

$$R(t,\theta) = \iint\limits_{I} g(x,y)\eta(x\cos\theta + y\sin\theta - t)dxdy \quad (1)$$

Among them,$\eta(\cdot)$ is the Dirac function, t is the distance (x, y) to the origin, and θ is the angle between X-axis and the line which perpendicular to the line t from the origin. It can be understood that Radon transform is the projection of image I in $t - \theta$ space, and each point in the $t - \theta$ space corresponds to a straight line in the image space. And it can also be understood as the projection on the horizontal axis after the image is rotated θ clockwise, as shown in Fig. 1.

Ridgelet transform

Ridgelet transform performs Randon transform on the image firstly, maps one-dimensional odd-specificity in the image into a point in the Randon domain, and then detects the singularity with one-dimensional wavelets. That can more effectively represent the singular features in the image with orientation. Ridgelet transform is more suitable for analyzing signals with straight line or hyperplane singularity. It can sparsely express image features and achieve high approximation accuracy while taking into account anti-noise ability. Its mathematical model is:

$$RT_g(a,b,\theta) = \int_{R^2} \psi_{a,b,\theta}(w)g(w)dw \quad (2)$$

Among them, $\psi(w) = a^{-\frac{1}{2}}\psi\left(\frac{x\cos\theta + y\sin\theta - b}{a}\right)$ is called the ridge function, $RT_f(a,b,\theta) = \int_{R^2}\psi(w)g(w)dw$ is the continuous Ridgelet transformation of $g(w)$ on R^2. In the two-dimensional case, the two can be connected through the radon transform. The inverse transformation of ridgelet transform is expressed as:

$$g(w) = \int_0^{2\pi}\int_{-\infty}^{\infty}\int_0^{\infty} RT_g(a,b,\theta)\psi(w)\frac{da}{a^3}db\frac{d\theta}{4\pi} \quad (3)$$

The chaos theory

Tent chaos

Tent chaos is an 1D chaos with linear mapping. It is suitable for image data encryption design due to that it has large secret key space, sensitivity to initial values, unrepeatability, uncertainty and unpredictability. The mathematical model is:

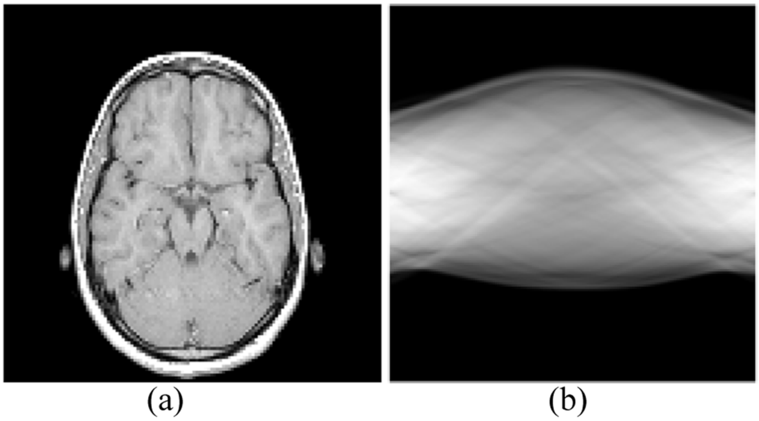


Fig. 1 Radon transformation of medical images ((**a**) original image; (**b**) the result after Radon transformation)

$$x_{n+1} = \begin{cases} \dfrac{x_n}{\alpha}, 0 < x_n \leq \alpha \\ \dfrac{1-x_n}{1-\alpha}, \alpha \leq x_n < 1 \end{cases} \tag{4}$$

When a ϵ (0,1) and x_n ϵ (0,1), tent map is in a state of chaos. The initial value x_0 will be different from the system parameter a to avoid the formation of the system cycle Usually.

Henon map

Henon Map is a discrete nonlinear dynamic 2D chaotic system generated by variables x and y simultaneous iteration. Its mathematical model is:

$$\begin{cases} x_{n+1} &= 1 - \alpha x_n^2 + y_n \\ y_{n+1} &= \beta x_{n+1} \end{cases} \tag{5}$$

Among them, a and β are the system parameters. When $a = 1.4$ and $\beta = 0.3$, the system is in a chaos. Henon mapping is easy to implement and more complex chaotic structure. And it has the characteristics of pseudo-randomness and initial value sensitivity, which is suitable for encrypting images. However, the existence of "blank area" and "stable area" are two problems faced when using Henon mapping for image encryption, as shown in Fig. 2.

Design of THM dual chaotic systems

In order to make up for the shortage of henon chaos and tent chaos, a tent-henon map (THM) dual chaotic system is designed in this paper. THM double chaos system has the characteristics of easy to implement, fast calculation speed, large key space, sensitive initial values, etc. It can produce chaotic sequences that are difficult to predict, and the application is more flexible. Tent chaotic matrix T_1 and Henon chaotic matrix H_1 are transformed into binary matrices T_2 and H_2 by Eq. (6) and Eq. (7).

$$T_2(i,j) = \begin{cases} T_1(i,j) = 0 \ , \ T_1(i,j) < T_{average} \\ T_1(i,j) = 1 \ , \ T_1(i,j) \geq T_{average} \end{cases} \tag{6}$$

$$H_2(i,j) = \begin{cases} H_1(i,j) = 0 \ , \ H_1(i,j) < H_{average} \\ H_1(i,j) = 1 \ , \ H_1(i,j) \geq H_{average} \end{cases} \tag{7}$$

Then T_2 and H_2 are obtained by XOR operation. The encryption key key_{THM} is obtained by Eq. (8).

$$Key_{THM} = T_2 \oplus H_2 \tag{8}$$

The proposed algorithm

The main steps of the algorithm

The algorithm was a watermarking algorithm based on ridgelet-DCT transform domain and THM double chaotic encryption system. In the feature extraction stage, based on human visual features, in the ridgelet-DCT domain, a new perceptual hash feature sequence that could represent image features was determined by setting a threshold parameter and participated in the watermarking operation. The algorithm organically combined watermarking technology with chaotic encryption,

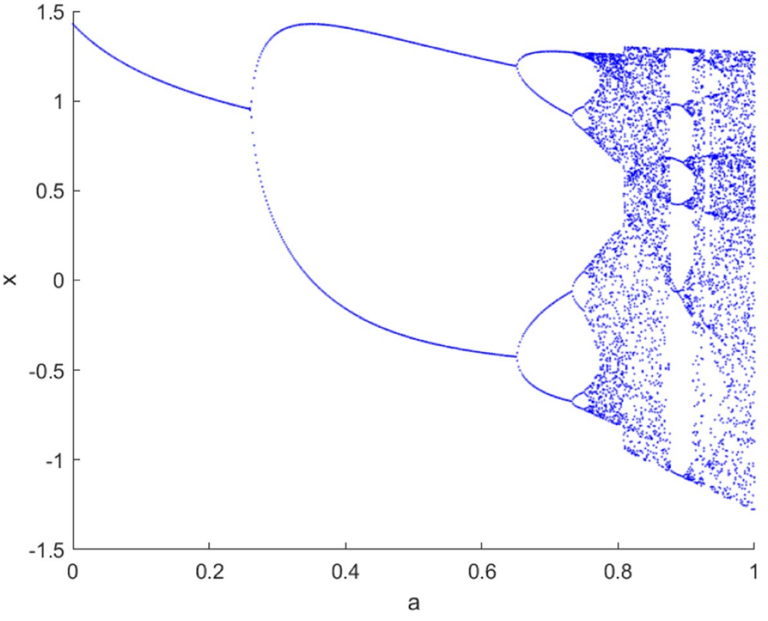


Fig. 2 The bifurcation diagram of Henon Map

third-party concepts and cryptography, for improving the security of medical image transmission and better protection of patient privacy. While it made the watermark resistant to conventional attacks and geometric attacks, and had strong robustness.

Step 1: ridgelet-DCT transform was performed on the original medical images I. And then in the transformed domain, it obtained the feature vector V_{img} of the medical image. V_{img} was converted into a binary hash feature sequence V_h, by setting the threshold parameter k.

Step 2: A binary matrix W_b was obtained by the transform of watermark image W. By setting the initial values of the tent diagram and Henon diagram, two chaotic sequences were generated. After binarization, the encryption matrix key_{THM} was obtained by logical XOR calculation of them.

Step 3: The encrypted watermark W_e was obtained by the matrix W_b and key_{THM}.

Step 4: Through the encrypted watermark W_e of the image and the binary feature V_h of the medical image, the binary logic sequence *key* was calculated and stored on the third-party platform.

Step 5: The feature sequence V_h' of medical image I' required to extract watermark was extracted by using the method of Step 1. The encrypted watermark matrix W_e' was obtained by logical operation with *key* stored in the third party.

Step 6: The final watermarking result was obtained by decrypting $W_e^{'}$ with the encryption key key_{THM}.

Feature extraction based on ridgelet-DCT transform domain

The medical image feature extraction algorithm based on the ridgelet-DCT transform domain was proposed in this paper. It takes into account the advantages of Ridgelet algorithm with better sparse expression ability, high approximation accuracy, and DCT transform with robustness, ergodicity, and strong anti-conventional

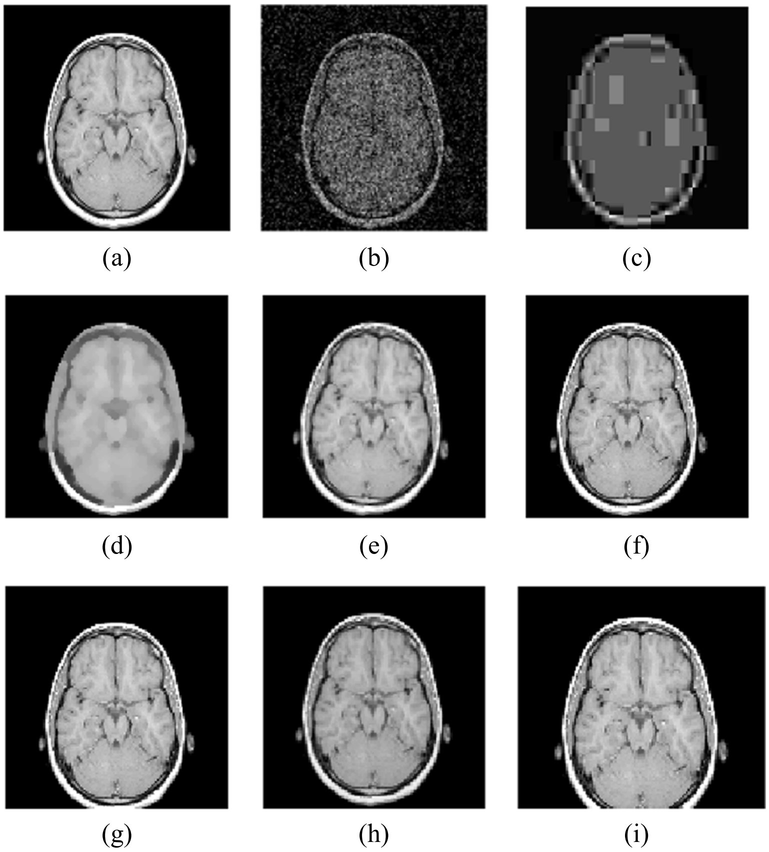


Fig. 3 The results under different attacks: (**a**) The brain image; (**b**) Gaussian noise attack with 1%; (**c**) JPEG compression attack with 4%; (**d**) Median filter attack with [3 × 3] and 10 times; (**e**) Rotation attack with clockwise 5○; (**f**) Translation attack with left 5% (**g**) Translation attack with down 7%; (**h**) Scaling attack with 95%; (**i**) Cropping attack with Y direction 10%

Table 1 The ridgelet-DCT coefficients under different attacks

Image Processing	PSNR (dB)	O (1,1)	O (1,2)	O (1,3)	O (1,4)	O (1,5)	O (1,6)	O (1,7)	O (1,8)	O (1,9)	O (1,10)	Sequence of Coefficient Signs	NC
The brain image	\	3.9960	0.4723	0.0000	0.000	0.0055	-3.8745	-0.5619	-0.0064	-0.217	0.0000	1100100000	1
Gaussian noise attack with 1%	12.36	4.9354	0.4014	0.0000	0.0000	0.0023	-4.1378	-0.4790	-0.0042	-0.1832	0.0000	1100100000	1
JPEG compression attack with 4%	17.61	4.0269	0.5057	0.0000	0.0000	0.0025	-3.9131	-0.6088	-0.0063	-0.2324	0.0000	1100100000	1
Median filter attack with [3 × 3] and 10 times	21.85	3.6915	0.4240	0.0000	0.0000	0.0162	-3.6004	-0.5122	-0.0041	-0.1952	0.0000	1100100000	1
Rotation attack with clockwise 5∘	12.38	3.9962	0.4678	0.0000	0.0000	0.0481	-3.8752	-0.5556	-0.0514	-0.2154	0.0000	1100100000	1
Translation attack with left 5%	11.75	3.9960	0.4743	0.0000	0.0000	0.3200	-3.8427	-0.5595	0.0520	-0.2186	0.0000	1100100100	0.99
Translation attack with down 7%	12.59	3.9514	0.7080	0.0000	0.0000	0.0025	-3.7529	-0.8425	-0.0069	-0.3255	0.0000	1100100000	1
Scaling attack with 95%	\	4.1322	0.4069	0.0000	0.0000	0.0252	-0.4489	-3.7705	-0.0049	-0.1870	0.0000	1100100000	1
Cropping attack with Y direction 10%	\	3.8646	0.6490	0.0000	0.0000	0.0054	-0.7432	-3.6219	-0.0032	-0.3026	0.0000	1100100000	1

attack ability. And ridgelet-DCT transform was used to find visual features suitable for medical images. A human brain image (128 × 128) was randomly selected for conventional attack and geometric attack, as shown in Fig. 3.

These images were transformed by ridgelet-DCT, and the coefficient data were extracted. It could be found that although these data had certain changes, their symbols were basically guaranteed to remain unchanged, as shown in Table 1. Based on the threshold, and set the values greater than the threshold to 1, others into 0. And it obtained the feature sequence of the brain image in the ridgelet-DCT transform domain, as "11,001,000,000". By Table 1 it could be found that, after transformation, symbol sequences of all attacked images were basically consistent with the original image.

According to the conclusions drawn in Table 1, this paper randomly selected a large number of medical images for the same test, and calculated the correlation coefficients between the 32-bit feature hash sequences of these images. Figure 4 showed 8 medical images selected randomly and Table 2 showed the correlation coefficient values between them. It could be found that the correlation coefficients between different medical images were all less than 0.5. Therefore, we could take the feature hash sequence transformed by ridgelet-DCT as the feature vector of medical image, and associated it with watermarking, so as to realize the zero-watermarking algorithm.

Watermark encryption and embedding

Before embedding the watermark, the THM double chaos system was used to encrypt the watermark and the encrypted watermark was obtained. The watermarking encryption scheme was shown in Fig. 5, and the watermarking embedding algorithm was shown in Fig. 6.

Step 1: Selecting the initial values, It selected the initial values of Tent chaos as $x_0 = 0.36$ and $\alpha = 0.98$, and iterated 300 times to generate the Tent Map chaotic sequence and converted it into a 300 × 300 matrix T_1. It set the initial values of Henon chaos as $\alpha = 1.4$ and $\beta = 0.314$ to iterate 300 times, and generates the Henon Map chaotic matrix H^1.
Step 2: It transformed T_1 and H_1 into binary matrices T_2 and H_2, by Eq. (6) and Eq. (7).
Step 3: It done logical XOR of T_2 and H_2 to get the encryption key key_{THM}, by Eq. (8).
Step 4: The binary watermark matrix W_b and the encryption key key_{THM} were logically XORed to obtain the encrypted watermark , by Eq. (9).

$$W_e = W_b \oplus key_{THM} \tag{9}$$

Step 5: Used the feature extraction method to perform ridgelet-DCT transformation on the original image I and extracted the feature vector $V_{img}(i)$, $i = 1, 2, \cdots, 32$, by Eq. (10).

$$V_h(i) = \begin{cases} 1 & , V_{img}(i) \geq k \times mean(V_{img}) \\ 0 & , V_{img}(i) < k \times mean(V_{img}) \end{cases} \tag{10}$$

Here, k was the threshold parameter, which transformed the feature vector V_{img} into a binary feature hash V_h.
Step 6: With binary feature hash V_h and the encrypted watermark W_e, it generated binary henon sequences *key* by Eq. (11), the algorithm flow was shown in Fig. 6.

$$key = V_h \oplus W_e \tag{11}$$

Watermark extraction and decryption

The algorithm proposed realizes the embedding of zero watermark and the blind extraction of watermark. The specific steps were shown in Fig. 7.

Step 7: To obtain binary feature vector V_h', it performed the operation on the image I' as **Step 5.**
Step 8: It obtained the encrypted watermark W_e' by Eq. (12).

$$W_e' = key \oplus V_h' \tag{12}$$

Step 9: It obtained the watermark decryption key key_{THM} in steps 1–3, and performed the following operations with the extracted encrypted watermark W_e' to obtain the decrypted watermark by Eq. (13).

$$W' = key_{THM} \oplus W_e' \tag{13}$$

Finally, it accorded to the degree of correlation between W and W' to determine the patient's personal information.

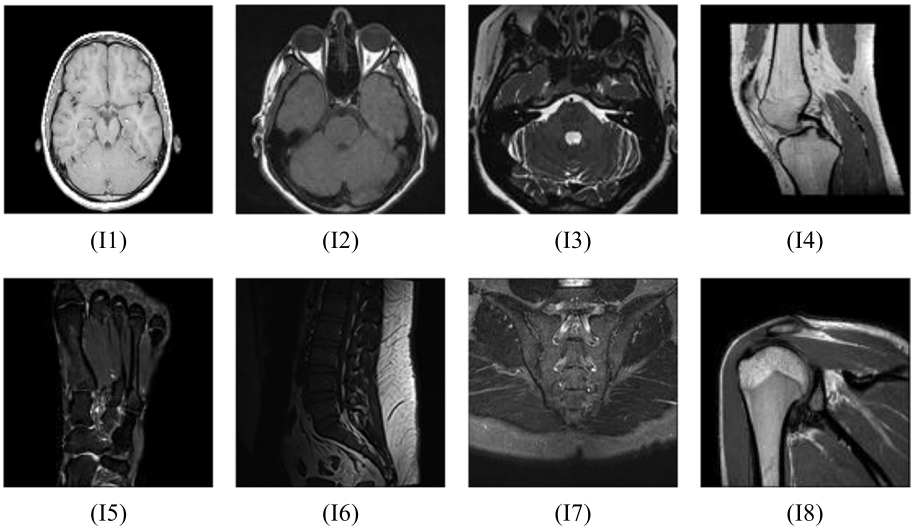


Fig. 4 Tested images ((I1) Brain; (I2) Orbit; (I3) Internal auditory canal; (I4) Knee; (I5) Foot; (I6) Spine; (I7) Coccygeal vertebra; (I8) Shoulder)

Table 2 The correlation coefficients between different medical images

Images	Brain	Orbit	Internal auditory canal	Knee	Foot	Spine	Coccygeal vertebra	Shoulder
Brain	1	0.0710	-0.2698	0.2966	-0.1972	0.2520	-0.3780	0.2520
Orbit	0.0710	1	0.1972	0.1395	0.0039	0.3131	-0.1879	0.3131
Internal auditory canal	-0.2698	0.1972	1	-0.2164	0.1815	0.2520	0	0.3780
Knee	0.2966	0.1395	-0.2164	1	-0.0120	0.1909	-0.1909	-0.1909
Foot	-0.1972	0.0039	0.1815	-0.0120	1	-0.3131	0.1879	0.0626
Spine	0.2520	0.3131	0.2520	0.1909	-0.3131	1	-0.3750	0.2500
Coccygeal vertebra	-0.3780	-0.1879	0	-0.1909	0.1879	-0.3750	1	-0.1250
Shoulder	0.2520	0.3131	0.3780	-0.1909	0.0626	0.2500	-0.1250	1

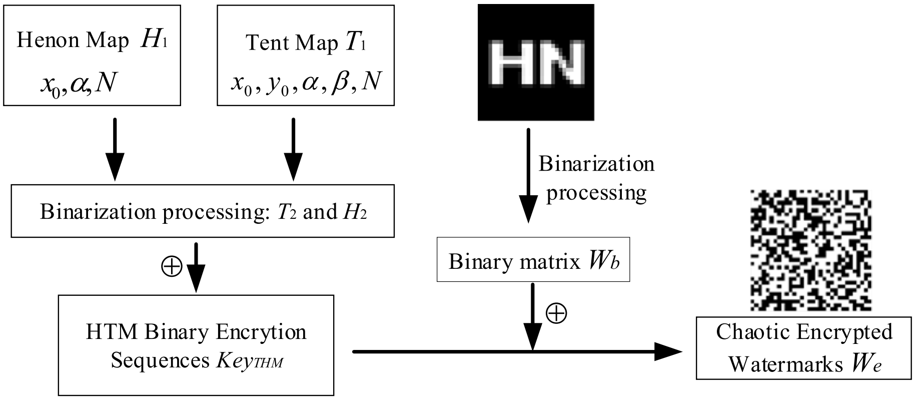

Henon Map H_1
x_0, α, N
Tent Map T_1
$x_0, y_0, \alpha, \beta, N$
HN
Binarization processing
Binarization processing: T_2 and H_2
$\oplus$
Binary matrix W_b
HTM Binary Encrytion Sequences Key_{THM}
$\oplus$
Chaotic Encrypted Watermarks W_e

Fig. 5 The watermarking encryption scheme

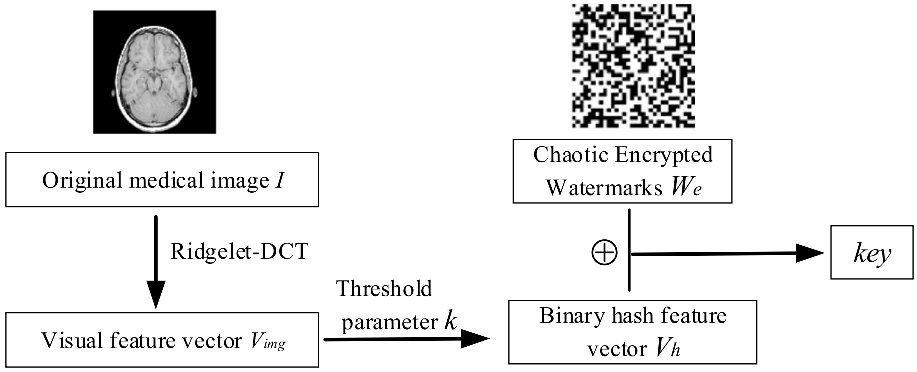

Original medical image I
Ridgelet-DCT
Visual feature vector V_{img}
Threshold parameter k
Chaotic Encrypted Watermarks W_e
$\oplus$
key
Binary hash feature vector V_h

Fig. 6 The watermarking embedding algorithm

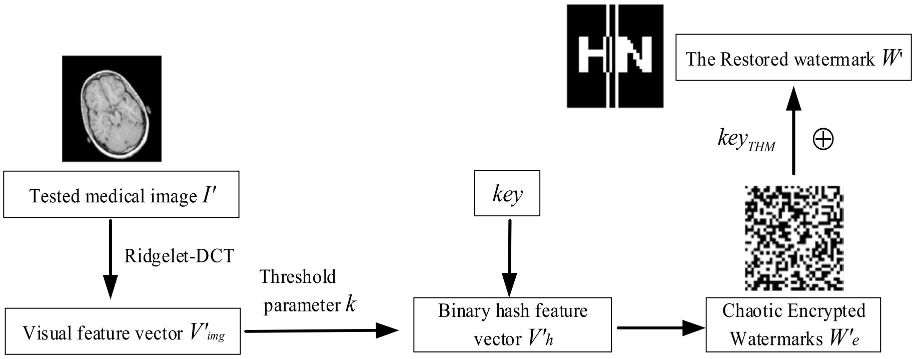

Tested medical image I'
Ridgelet-DCT
Visual feature vector V'_{img}
Threshold parameter k
key
Binary hash feature vector V'_h
Chaotic Encrypted Watermarks W'_e
key_{THM}
$\oplus$
The Restored watermark W'

Fig. 7 The watermarking extraction and decryption algorithm

Experiment and analysis

In this paper, Matlab 2021a was used as the software platform, and the original image was the "brain" image and a meaningful image as the original watermark. By slightly changing the initial values of the THM chaotic system, the sensitivity and security of the algorithm were verified. (a) (b) (c) in Fig. 9 were the embedded watermarked image, the watermark image, and the encrypted watermark image.

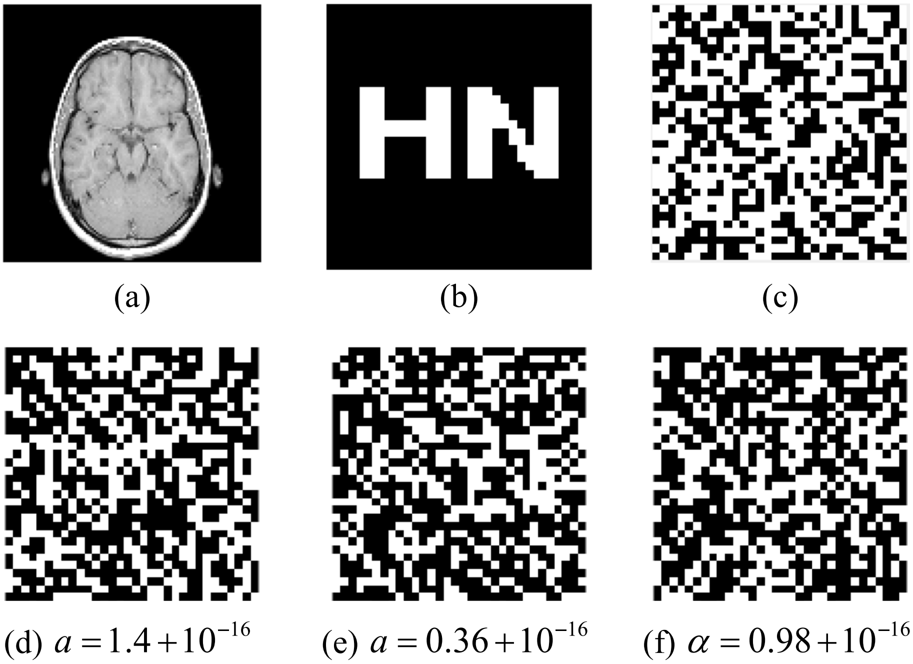
The sensitivity analysis

In this paper, the THM double chaos system was designed based on the characteristics of Tent Map's large secret key space and Henon Map's high complexity and suitable for two-dimensional images. The chaotic system could generate chaotic sequences that were difficult to predict, simple, flexible, sensitive to initial values, fast calculation speed, and large key space. The key space of THM was 10^{116} which was much larger than that of low-dimensional chaotic systems and other double chaotic algorithms, as shown in Table 3. The THM double chaotic system changed the dynamic behavior of a single chaotic system, made up for the deficiency of the blank window in the chaotic region. And it avoided periodic degradation of low chaotic system, and effectively resisted model exhaustive attacks and reconstruction attacks.

THM double chaotic system was highly sensitive and highly dependent on the key. Even minor change in the key could not get the correct decryption result, and the resulting images encryption would fall into chaos. In this paper, the initial values of Tent chaos were set as $x_0 = 0.36$, $\alpha = 0.98$ and $N = 300$, and the initial values

Table 3 The comparison of key space

	The algorithm proposed	Wang R [19]	Jing L [20]	Balasamy K [23]	Yangxiu F [26]	Ceng X [27]	Hegui Z [34]	Congxu Z [35]
Key space	10^{116}	10^{48}	10^{64}	10^{32}	10^{32}	10^{32}	2^{256}	10^{100}


(a) (b) (c)

(d) $a = 1.4 + 10^{-16}$ (e) $a = 0.36 + 10^{-16}$ (f) $\alpha = 0.98 + 10^{-16}$

Fig. 8 Sensitivity analysis of encryption algorithm ((**a**) the medical image of the watermark; (**b**) the correctly decrypted watermark; (**c**) the encrypted image; (**d**) the error decryption result with $a = 1.4 + 10^{-16}$; (**e**) the error decryption result with $a = 0.36 + 10^{-16}$; (f) the error decryption result with $\boldsymbol{\alpha} = 0.98 + 10^{-16}$)

of Henon chaos were set as $x_0 = 0$, $y_0 = 0$ and the initial parameters were $\alpha = 1.4$ and $\beta = 0.314$. While keeping other parameters unchanged, the initial parameter of henon map was changed to $\alpha = 1.4 + 10^{-16}$, the initial parameter of tent map was changed to $x_0 = 0.36 + 10^{-16}$ or $\alpha = 0.98 + 10^{-16}$. They all could not get the correct watermark image, as shown in Fig. 8. It showed that the THM double chaos encryption system proposed in this paper had high security and could protect the security of watermark image data better.

Conventional attacks

Gaussian noise attacks

Under the attacks of Gaussian noise, this paper added different intensity noises to the "human brain" medical image, as shown in Fig. 9.

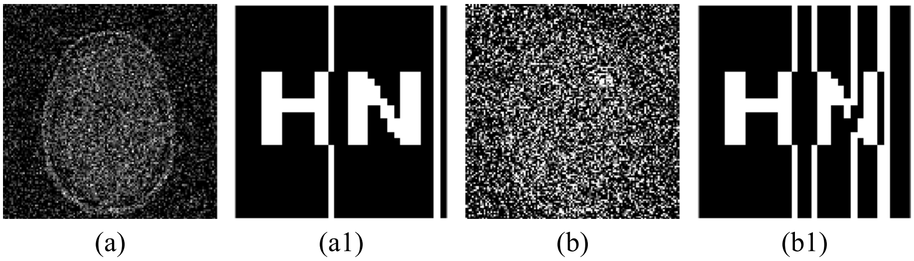

(a) (a1) (b) (b1)

Fig. 9 The images and watermark results under different Gaussian noise attacks ((**a**) 5% noise intensity; (a1) the watermark result of (**a**); (**b**) 50% noise intensity; (b1) the watermark result of (**b**))

Table 4 Results of Gaussian noise attacks

Gaussian Noise(%)	1	5	15	20	30	40	50
PSNR	12.33	5.93	1.80	0.78	0.58	-1.22	-1.70
NC	1.00	0.91	0.82	0.76	0.66	0.65	0.62

When the threshold coefficient was set $k = 1$, the NC value results of watermark extracted under Gaussian noise attacks were obtained, as shown in Table 4. When the noise intensity was less than 1%, the NC values were 1, and it was less than 5%, the NC values were higher than 90%. Even though the noise intensity reached 50%, the images had been severely distorted and difficult to be accurately recognized by the naked eye. The NC values were still higher than 0.6. It indicated that the algorithm proposed was robust against Gaussian noise.

Median filter attacks

In this paper, median filtering attacks of [3,3], [5,5], [7,7] and [9,9], and 1, 10 and 20 times were carried out on the original image respectively. Parts of the attack results and extracted watermark were shown in Fig. 10. It set the threshold parameter as k = 1, the NC values calculated by the algorithm proposed are all 1, as shown in Table 5. That shows that the algorithm had good resistance to median filtering attacks.

JPEG attacks

Due to the large data volume of medical images, they must be compressed for storage in order to save the limited storage space, reduce storage costs, improve image transmission speed and reduce communication costs. As an international compression standard, JPEG compression was a common method of medical image compression. It set the threshold parameter as k = 1, in this paper. 4%, 8%, 15%, 20% and 40% JPEG compression of the original image were carried out respectively, as shown in Fig. 11. The values of NC were always set to 1, when the original image was compressed to 40%. It showed that the algorithm had a better ability with anti-JPEG attacks and robustness, as shown in Table 6.

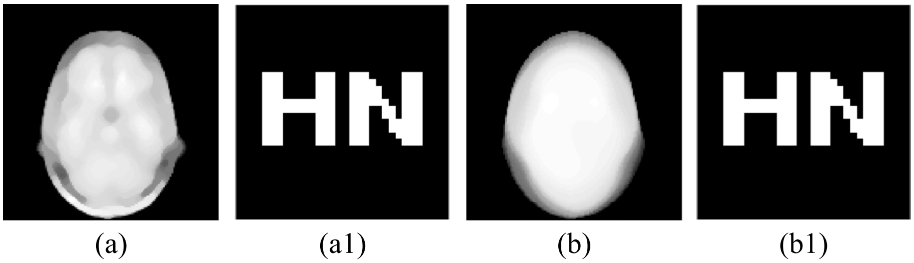


Fig. 10 The images and watermark results under different median filtering attacks ((**a**) 10 times of [5,5]; (a1) the watermark result of (**a**); (**b**) 20 times of[9,9]; (b1) the watermark result of (b))

Table 5 Results of median filtering attacks

Median Filter	[3, 3]			[5,5]			[7,7]			[9,9]		
Repeat Times	**1**	**10**	**20**	**1**	**10**	**20**	**1**	**10**	**20**	**1**	**10**	**20**
PSNR	24.52	21.85	21.30	20.44	18.28	17.73	18.41	16.99	16.91	16.90	15.94	15.71
NC	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

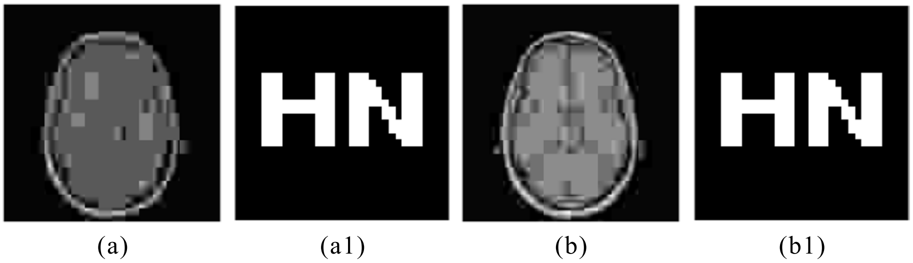


Fig. 11 The images and watermark results under different JPEG compression attacks ((**a**) 4% JPEG compression; (a1) the watermark result of (**a**); (**b**) 8% JPEG compression; (b1) the watermark result of (**b**))

Table 6 Results of JPEG compression attacks

JPEG compression	4%	8%	15%	25%	30%	40%
PSNR	17.61	19.99	22.01	23.67	24.29	25.06
NC	1.00	1.00	1.00	1.00	1.00	1.00

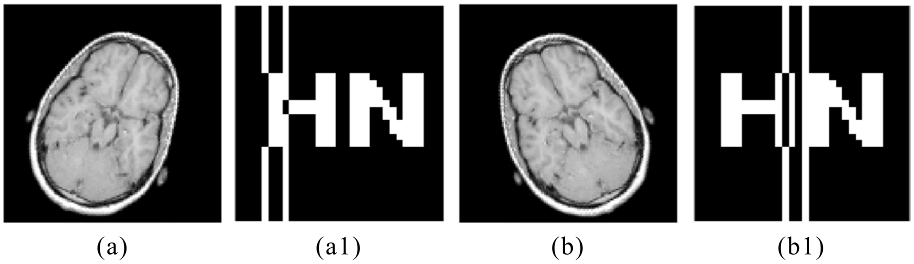


Fig. 12 The images and watermark results under rotation attacks ((**a**) Clockwise rotation 25°; (a1) the watermark result of (**a**); (**b**) Contrarotate 25°; (b1) the watermark result of (**b**))

Table 7 Results of rotation attacks

Sense of rotation	Clockwise		Contrarotate	
Rotation angles	PSNR	NC	PSNR	NC
5	16.19	1.00	16.19	1.00
10	13.49	1.00	13.49	0.91
15	12.70	0.91	12.70	0.91
20	12.38	0.77	12.38	0.83
25	12.16	0.77	12.16	0.83
30	11.90	0.77	11.90	0.83
35	11.58	0.77	11.58	0.75
40	11.25	0.77	11.25	0.67
45	10.95	0.69	10.95	0.60

Geometrical attacks

Rotation attacks

It rotated clockwise and counterclockwise by 5° each time on the original image, and partial results were shown in Fig. 12. When the threshold parameter $k = 3$ was set, the NC values were shown in Table 7. It could be found that the algorithm had better robustness when the rotation angles were less than 10°. When the rotation angles were between 10° and 30°, the NC values were greater than 0.76 and 082. When it was rotated to 45°, the NC values could still be above 0.6. It showed that the algorithm had good ability on anti-rotation attack and robustness, and it had a better effect on counterclockwise rotation attacks than clockwise rotation attacks.

Table 8 Results of left and right translation attacks

Distance (%)	Left		Right	
	PSNR	NC	PSNR	NC
3	13.00	0.9029	14.22	0.90
5	11.75	0.9029	12.28	0.90
7	11.38	0.8121	11.51	0.90
8	11.27	0.7441	11.38	0.90
9	11.14	0.7441	11.27	0.76
10	11.00	0.7441	11.14	0.76
15	10.05	0.7441	10.31	0.76
18	9.35	0.7441	9.56	0.67
20	8.95	0.6925	9.15	0.67

Table 9 Results of up and down translation attacks

Dstance (%)	Up		Down	
	PSNR	NC	PSNR	NC
2	13.79	0.91	15.33	1.00
4	12.40	0.83	13.04	1.00
8	11.54	0.72	12.20	1.00
12	10.62	0.62	11.55	1.00
13	10.46	0.62	11.41	0.90
15	10.16	0.58	11.20	0.90
18	9.60	0.58	10.68	0.90
22	9.16	0.53	10.25	0.90

Translation attacks

Translation attacks on the original image were selected to verify the robustness of the algorithm, and the threshold parameter was set as $k = 2$. Left–right translation attacks and up-down translation attacks were carried out on the original image, then the watermark information was extracted, and the results were shown in Tables 8 and 9. They showed that the effect of the algorithm on the right translation attacks was better than that on the left. Among them, the NC values were all higher than 0.9 when left and right distance were within 5%. When the distance of left and right translation reached 20%, the NC values could still be higher than 0.67. It showed that the algorithm could resist translation attack better and had good robustness. (a), (b), (a1) and (b1) in Fig. 13 showed the attack results and watermarking results with 10% translation on the left and right.

It could be found from Table 9 that when down distance 12%, the NC values were still 1. And when down distance 22%, the NC values were greater than 0.9. With up distance 8%, the NC values had dropped to 0.72. When up distance 22%, the NC values were greater than 0.5. It indicated that the algorithm had good resistance to up and down translation attacks and good robustness. And the algorithm was resistant to downward translation attacks far better than resisting upward translation attacks. (c), (d), (c1) and (d1)

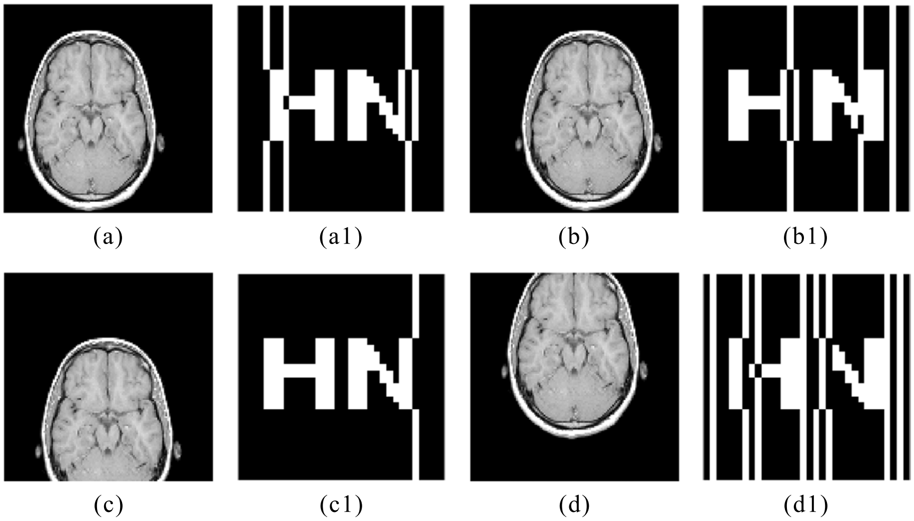


Fig. 13 The images and watermark results under translation attacks ((**a**) left distance 10%; (a1) the watermark result of (**a**); (**b**) right distance 10%; (b1) the watermark result of (**b**); (**c**) down distance 22%; (c1) the watermark result of (**c**); (**d**) up distance 18%; (d1) the watermark result of (**d**))

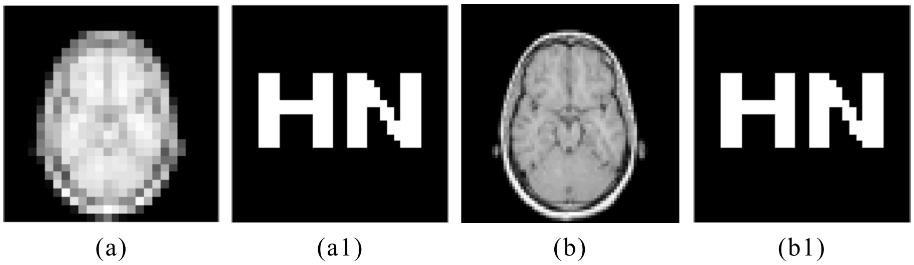


Fig. 14 The results under scaling attacks ((**a**) scaling factor 0.2; (a1) the result of (**a**); (**b**) scaling factor 8.0; (b1) the result of (**b**))

Table 10 Results of scaling attacks

Scaling Factor	0.2	0.4	0.8	1.2	4.0	6.0	8.0
NC	1.00	1.00	1.00	1.00	1.00	1.00	1.00

in Fig. 13 showed the attack results and watermarking results with down distance 22% and up distance 18%.

Scaling attacks

The scaling attacks were carried out on the original image, and the threshold parameter was settd as $k = 1.5$. The partial results were shown in Fig. 14. According to Table 10, the scaling parameters ranged from 0.2 to 8.0, and the NC values were still 1. It showed that the algorithm was very robust to scaling attacks.

Cropping attacks

The original image was sheared in the Y-axis direction and the X-axis direction respectively, and part of the results were shown in Fig. 15. It could be found that the algorithm had better anti-attack effect for Y-axis cropping when the threshold parameter was $k = 12$ as shown Table 11. When the original image was cropped less than 12%, the NC values were 1. When it was cropped 35%, the NC value was bigger than 0.9, and cropped 40%, the NC could still reach 0.7689.

When the X-axis was cropped, the threshold parameter was $k = 2.5$, and the anti-attack effect of the algorithm was the best. Then the original image was cropped less than 12%, the NC values were greater than 0.9. When it was cropped 23%, the NC value could be greater than 0.6. And, when it was cropped 40%, the NC could still reach 0.5531. This indicated that the algorithm proposed in this paper had good robustness to cropping attack, and the results in the Y-axis direction were better than those in the X-axis direction.

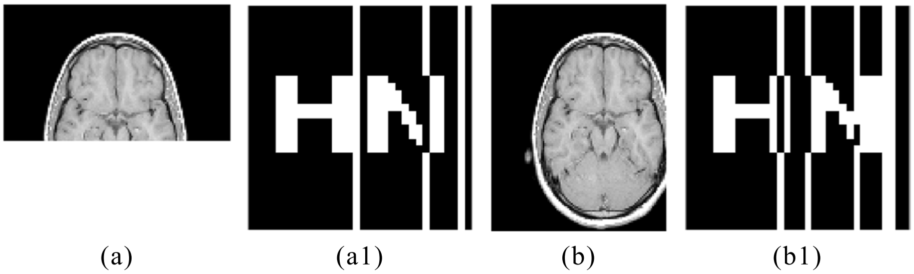


Fig. 15 The images and watermark results under scaling attacks ((**a**) Y Direction 40%; (a1) the watermark result of (**a**); (**b**) X Direction 23%; (b1) the watermark result of (**b**))

Table 11 Results of cropping attacks

Cropping (%)	2	8	12	15	23	30	35	40
NC of Y Direction	1.00	1.00	1.00	0.91	0.91	0.91	0.91	0.77
NC of X Direction	1.00	0.90	0.90	0.71	0.65	0.58	0.55	0.55

Table 12 Different algorithms comparison

Conventional attacks	Intensity	Proposed Algorithm NC1	Jing L [20] NC2	Fengming Q [25] NC3	Yangxiu F [26] NC4	Ceng X [27] NC5	Zea A [36] NC6	Xiaochen Y [37] NC7
Gaussian Noise	1%	1.00	1.00	1.00	1.00	0.52	0.88	0.92
	10%	0.82	0.79	0.80	1.00	0.68	0.79	0.88
	25%	0.74	0.79	0.80	0.77	0.51	0.63	0.81
JPEG Compression	4%	1.00	0.81	1.00	1.00	0.63	0.11	0.51
	8%	1.00	0.97	0.89	1.00	0.59	0.31	0.77
	25%	1.00	0.95	1.00	1.00	0.72	0.91	0.85
Median Filter (10 times)	[3,3]	1.00	0.97	1.00	1.00	0.27	0.15	0.89
	[5,5]	1.00	0.88	1.00	0.87	0.44	0.04	0.77
	[9,9]	1.00	0.81	0.89	0.50	0.18	0.01	0.69

Table 13 Different algorithms comparison

Geometric attacks	Intensity	Proposed Algorithm NC1	Jing L [20] NC2	Fengming Q [25] NC3	Yangxiu F [26] NC4	Ceng X [27] NC5	Zea A [36] NC6	Xiaochen Y [37] NC7
Rotation (clockwise)	10°	1.00	0.90	0.63	1.00	0.81	0.21	0.86
	20°	0.77	0.90	0.63	1.00	0.89	0.17	0.84
	40°	0.77	0.86	0.32	1.00	0.74	0.10	0.80
Scaling	0.4	1.00	0.93	1.00	1.00	0.25	0.39	0.59
	0.8	1.00	0.93	1.00	1.00	0.68	0.54	0.63
	2.0	1.00	1.00	1.00	1.00	0.31	0.92	0.74
Down Translation	8%	1.00	0.91	0.89	1.00	0.61	0.73	0.86
	15%	0.90	0.80	0.50	1.00	0.56	0.66	0.77
	20%	0.90	0.71	0.45	0.86	0.56	0.54	0.61
Left Translation	3%	0.90	0.97	0.72	1.00	1.00	0.77	0.90
	5%	0.90	0.97	0.52	0.86	1.00	0.74	0.83
	8%	0.74	0.81	0.52	0.86	1.00	0.70	0.66
Cropping	12%	1.00	1.00	1.00	1.00	0.55	0.76	0.97
	23%	0.91	1.00	0.89	0.87	0.41	0.21	0.92
	35%	0.91	0.61	0.78	0.62	0.33	0.03	0.02

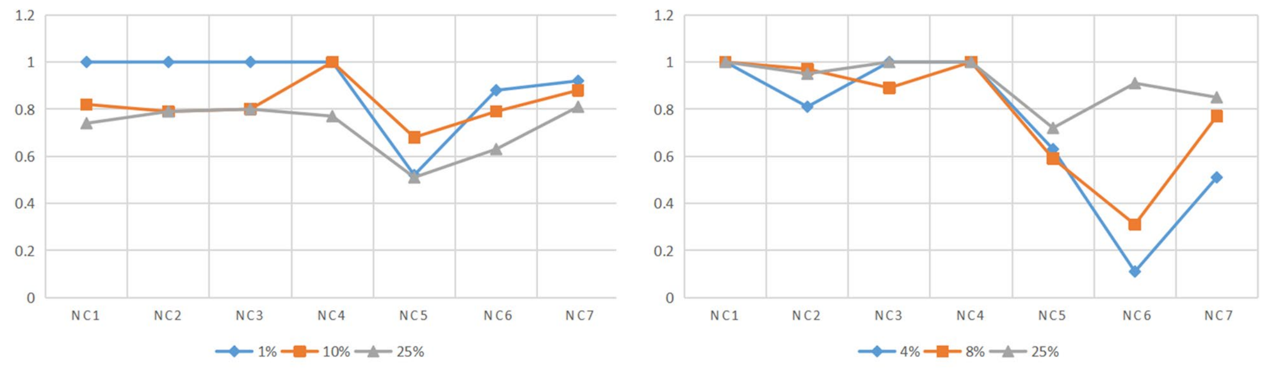
Algorithms comparison

This paper compared the NC values of [20, 25–27, 36, 37] under different attacks. The results under conventional attacks were shown in Table 12, and the results under geometric attacks were shown in Table 13.

It could be seen from Fig. 16(a) that under Gaussian noise attacks, when noise intensity was 1%, the anti-Gaussian noise ability of the algorithm, [20] and [25, 26] were higher than that of [27] and [36, 37]. When the noise intensity was 10%, the ability of our algorithm was slightly lower than [26] and [37] and better than other algorithms. When the noise intensity was 25%, our NC value was still greater than 0.7, the anti-Gaussian noise ability of the algorithm decreased, and it was better than [27] and [36].

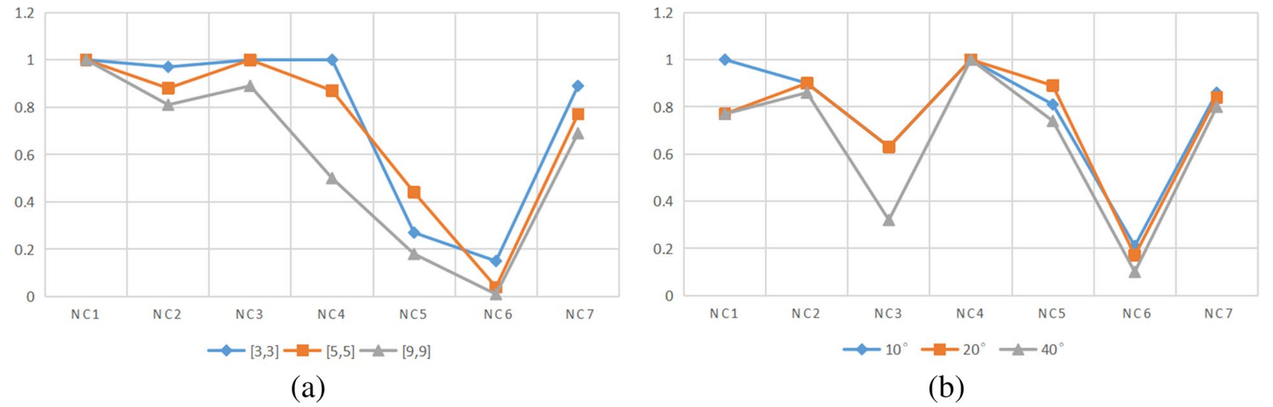
For JPEG attacks, it could be found that other algorithms change to a certain extent with the increase of attacks, but for our algorithm and [26], the NC values were still 1, which was superior to other algorithms, as shown in Fig. 16(b). And for mean filtering attacks, it could be found that our algorithm was superior to other algorithms, as shown in Fig. 17(a).

It was a difficult problem for watermark algorithm to resist geometric attack. This paper used rotation (clockwise), scaling, down translation, left translation and cropping to compare the robustness of the algorithm with other methods, and their NC values were shown in Table 13. From Fig. 17(b), it could be found that when the rotation angle was less than 10°, the NC values of our algorithm and [26] were 1, greater than



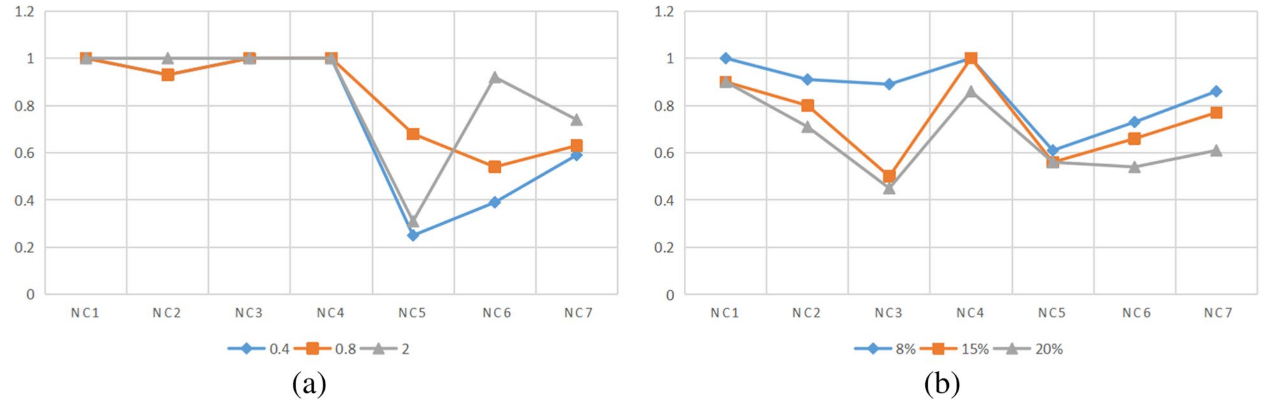
(a) (a)

Fig. 16 Comparison of NC values under Gaussian noise attacks and JPEG compression attacks ((**a**) median filter attacks (**b**) JPEG compression attacks)



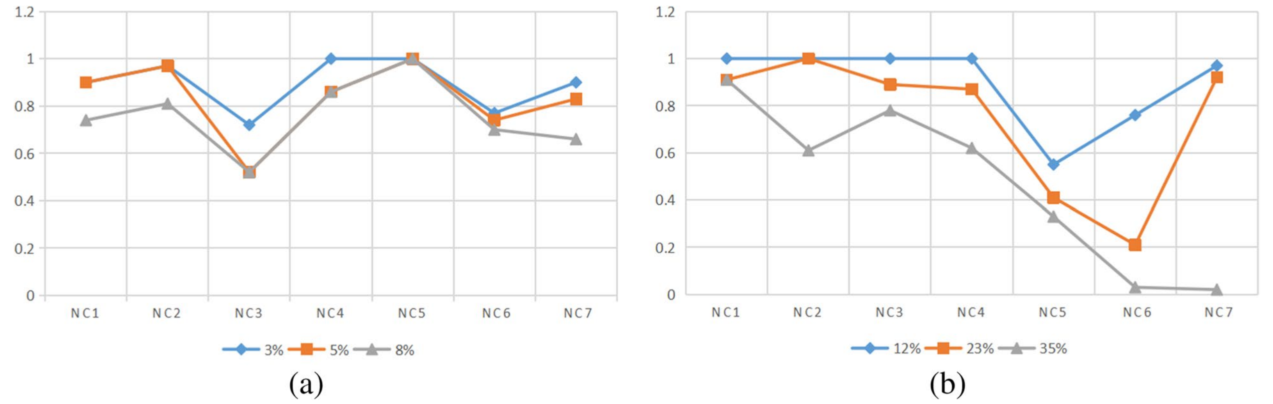
(a) (b)

Fig. 17 Comparison of NC values under median filter attacks attacks and rotation(clockwise) attacks ((**a**) Gaussian noise attacks (**b**) rotation(clockwise) attacks)



(a) (b)

Fig. 18 Comparison of NC values under scaling attacks and down translation attacks ((**a**) scaling (**b**) down translation)



(a) (b)

Fig. 19 Comparison of NC values under left translation attacks and cropping attacks ((**a**) left translation (**b**) cropping)

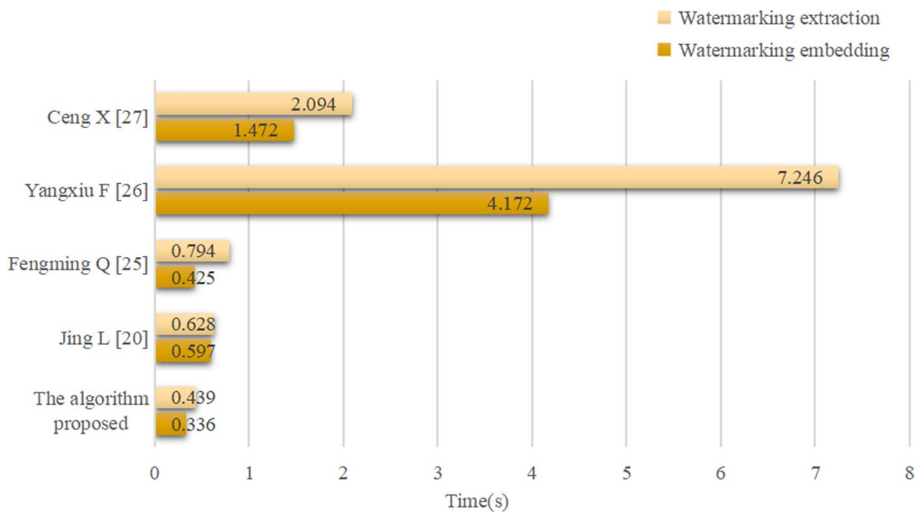


Fig. 20 Comparison of computation cost

others. When the rotation angle reached 40°, it was better than [25, 27] and [36].

For scaling attacks, the anti-attack ability of our algorithm and [25, 26] were significantly better than other algorithms, as shown in Fig. 18(a). For down translation attacks, when the attack strength reached 20%, NC value of us was still 0.9, greater than others, as shown in Fig. 18(b). For left translation attacks, the anti-attack ability of our algorithm was better than [25] and [36, 37], as shown in Fig. 19(a). And as the cropping attacks strength increased at 35%, anti-attack ability of our algorithm was better than other algorithms, as shown in Fig. 19(b).

It selectd 5 algorithms with better performance, and compared the computational cost of the time required by the algorithms for embedding and extracting watermarks under the same conditions, as shown in Fig. 20. It could be found that the computational cost of our algorithm was lower than other algorithms.

Therefore, through the above comparison, it could be found that the algorithm proposed in this paper was significantly better than other algorithms in median filtering, JPEG and cropping attacks. And its performance in rotation attack and left translation attack were in the middle level of all. When the NC values of other algorithms decreases as the attack increases, the NC values of our algorithm were all greater than 0.7. This shown that the anti-attack capability of the algorithm was more comprehensive and balanced, and it could better resist high-intensity conventional attacks and geometric attacks, and the algorithm had good robustness while taking into account the low computational cost.

Conclusions

In this paper, a new medical image watermarking algorithm based on ridgelet-DCT transform domain and THM double chaos encryption was proposed. The algorithm combined double chaos encryption, zero watermarking and coefficient invariance in transform domain. The watermark could be extracted and embedded without selecting the region of interest. The algorithm was based on image encryption in the ridgelet-DCT transform domain, and considering that the ridgelet transform had good sparse expression ability, high approximation accuracy, and DCT transform had good robustness and anti-traditional attack ability. The algorithm has taken advantage of THM double chaos system, which had the characteristics of high complexity, sensitive initial values, large secret key space and it was difficult to crack. While improving the security of watermark information, it had good robustness against conventional attacks and geometric attacks. And the algorithm also had low computational cost and good balance. The algorithm also had some limitations. Under the attacks of rotation attacks and left translation attacks, the robustness of the algorithm was not good enough. And it had poor robustness for complex geometric attacks (such as ripple attack, squeeze attack, etc.). That need to be further improved and perfected.

Abbreviations

THM: Tent-Henon-Map; DCT: Discrete Cosine Transform; DFT: Discrete Fourier Transform; DWT: Discrete Wavelet Transform; SVD: Singular Value Decomposition; LSB: Least Significant Bit.

Acknowledgements

The authors would like to thank the editor and the anonymous reviewers for helpful and constructive comments that greatly contributed to improving this article.

Authors' contributions

Jingbing Li: Conceptualization (lead); Funding Acquisition; Writing—Review & Editing. Zilong Liu: Conceptualization; Formal Analysis; Writing—Original Draft Preparation; Visualization (lead); Methodology (lead); Writing—Review & Editing. Ai Yang: Software; Visualization (equal); Methodology (equal). Yuancai Zheng: Investigation; Project Administration. Jing Liu: Supervision; Data Curation. The authors read and approved the final manuscript.

Funding

This work was supported by Hainan Provincial Natural Science Foundation of China under Grant 620QN286. And project supported by the Education Department of Hainan Province under Grant Hnkyzc2022-13.

Availability of data and materials

The authors confirm that the data supporting the findings of this study are available within the article or its supplementary materials.

Declarations

Competing interests

The authors declare that they have no conflicts of interest to report regarding the present study.

Author details

[1]School of Information and Communication Engineering, Hainan University, Haikou 570228, China. [2]Haikou University of Economics, Haikou 571127, Hainan, China. [3]College of Information Science and Engineering, Ritsumeikan University, Shiga, Japan. [4]School of Mathematics and Statistics, Hainan Normal University, Haikou 571158, China. [5]Research Center for Healthcare Data Science, Zhejiang Lab, Hangzhou 311121, China.

Received: 16 August 2022 Accepted: 15 September 2022
Published online: 01 October 2022

References

1. Borovska P, Ivanova D, Kadurin V (2018) Experimental Framework for the Investigations in Internet of Medical Imaging Things Ecosystem. in QED'17 UNESCO International Workshop, Sofia, Bulgaria.
2. Chandy A (2019) A review on iot based medical imaging technology for healthcare applications. JIIP 1:51–60. https://doi.org/10.36548/JIIP.2019.1.006
3. Yufeng W, Liwei W, Changao X (2018) Medical information security in the era of artificial intelligence. Med Hypotheses 7(115):1–6. https://doi.org/10.1016/j.mehy.2018.03.023
4. Ashima A, Amit Kumar S (2020) An improved DWT-SVD domain watermarking for medical information security. Comput Commun 152:72–80. https://doi.org/10.1016/j.comcom.2020.01.038
5. Begum M, Uddin M S (2020) Digital image watermarking techniques: a review. information 11(2): 1–38 https://doi.org/10.3390/info11020110.
6. Arkadip R, Somaditya R (2020) Recent trends in image watermarking techniques for copyright protection: a survey. IJMIR 9(4):249–270. https://doi.org/10.1007/s13735-020-00197-9
7. Jobin A, Varghese P (2019) An imperceptible spatial domain color image watermarking scheme. J King Saud Univ-Com 31:125–133. https://doi.org/10.1016/j.jksuci.2016.12.004
8. Celik MU, Sharma G, Tekalp AM (2005) Lossless generalized-LSB data embedding. IEEE Trans Image Process 14(2):253–266. https://doi.org/10.1109/TIP.2004.840686
9. Mohammed G N, Yasin A, Zeki A Z (2014) Robust Image Watermarking Based on Dual Intermediate Significant Bit (DISB). In 2014 6th International Conference on Computer Science and Information Technology, Amman, Jordan, pp.18–22 https://doi.org/10.1109/CSIT.2014.6805973.
10. Zeki A, Abubakar A, Chiroma H (2016) An intermediate significant bit (ISB) watermarking technique using neural networks. Springerplus 5(2):1–25. https://doi.org/10.1186/s40064-016-2371-6
11. Pun C M (2009) High Capacity and Robust Digital Image Watermarking. In: Proceedings Of The 5th International Joint Conference on INC, IMS and IDC, Seoul, South Korea 1457–1461 https://doi.org/10.1109/NCM.2009.85
12. Zhen Z, Shuyu C, Guiping W (2015) A Robust Digital Image watermarking algorithm based on DCT domain for copyright protection. in: smart graphics 2015: International Symposium on Smart Graphics, Chengdu, China 132–142 https://doi.org/10.1007/978-3-319-53838-9_11.
13. Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M (2015) Robust watermarking method in DFT domain for effective management of medical imaging. Signal Image Video 9:1163–1178. https://doi.org/10.1007/s11760-013-0555-x
14. Gaata MT (2016) An Efficient Image Watermarking Approach based on Fourier Transform. IJCA 136:8–11. https://doi.org/10.5120/ijca2016908559
15. Zhiyun C, Ya C, Wenxin H, Dongming Q (2015) Wavelet Domain Digital Watermarking Algorithm Based on Threshold Classification. In: 6th International Conference on Swarm Intelligence, Beijing, China, 129–136 https://doi.org/10.1007/978-3-319-20469-7_15.
16. Yifeng Z, Yingying L, Yibo S (2019) Digital Watermarking Based on Joint DWT-DCT and OMP Reconstruction. Circ Syst Singal Pr 38:5135–5148. https://doi.org/10.1007/s00034-019-01112-2
17. ChinChen C, Piyu T, ChiaChen L (2005) SVD-based digital image watermarking scheme. Pattern Recogn Lett 60:1577–1586. https://doi.org/10.1016/j.patrec.2005.01.004
18. Vaishnavi D, Subashini TS (2015) Robust and Invisible Image Watermarking in RGB Color Space Using SVD. Procedia Computer Science 46:1770–1777. https://doi.org/10.1016/j.procs.2015.02.130
19. Wang R, Shaocheng H, Zhang P (2020) A Novel zero-watermarking scheme based on variable parameter chaotic mapping in NSPD-DCT domain. IEEE Access 8:182391–182411
20. Jing L, Jingbing L, Jixin M et al (2019) A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and Henon Map. Appl Sci 9:701–723. https://doi.org/10.3390/app9040700
21. Siming X, Tongyi L, Jing L (2021) A zero-watermark hybrid algorithm for remote sensing images based on DCT and DFT. JPCS 1952:1–12. https://doi.org/10.1088/1742-6596/1952/2/022049
22. Narima Z, Amine K, Redouane K,et al, (2021) A DWT-SVD based robust digital watermarking for medical image security. Forensic Sci Int 320:1–9. https://doi.org/10.1016/j.forsciint.2021.110691
23. 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. https://doi.org/10.1007/s11042-020-09981-5
24. Fares K, Khaldi A, Redouaneet K et al (2021) DCT & DWT based watermarking scheme for medical information security. Bopmed Signal Proces 66:1–9. https://doi.org/10.1016/j.bspc.2020.102403
25. Fengming Q, Jingbing L, Hui L, .et al (2020) A Robust Zero-Watermarking Algorithm for Medical Images Using Curvelet-Dct and RSA Pseudo-random Sequences. In: International Conference on Artificial Intelligence and Security, Dublin, Ireland 179–190 https://doi.org/10.1007/978-3-030-57881-7_16.
26. Yangxiu F, Jing L, Jingbing L,et al, (2022) Robust zero-watermarking algorithm for medical images based on SIFT and Bandelet-DCT. Multimedia Tools and Applications 81:16863–16879. https://doi.org/10.1007/s11042-022-12592-x
27. Cheng Z, Jing L, Jingbing L,et al, (2022) Multi-watermarking algorithm for medical image based on KAZE-DCT. J AMB INTEL HUM COMP 4:1–9. https://doi.org/10.1007/s12652-021-03539-5
28. Thanki R, Kothari A, Trivedi D (2019) Hybrid and blind watermarking scheme in DCuT-RDWT domain. JISA 46:231–249. https://doi.org/10.1016/j.jisa.2019.03.017
29. Thanki R, Kothari A (2021) Multi-level security of medical images based on encryption and watermarking for telemedicine applications. Multimed Tools Appl 80:4307–4325. https://doi.org/10.1007/s11042-020-09941-z
30. Celestine I, Zunera J, Abdul RJ et al (2020) KeySplitWatermark: zero watermarking algorithm for software protection against cyber-attacks. Journals & Magazines 8:72650–72660. https://doi.org/10.1109/ACCESS.2020.2988160
31. Zhiqiu X, Xingyuan W, Chunpeng W et al (2022) A robust zero-watermarking algorithm for lossless copyright protection of medical images. APPL INTELL 52(1):607–621. https://doi.org/10.1007/s10489-021-02476-2

32. Baowei W, Jiawei S, Weishen W et al (2022) Image copyright protection based on Blockchain and zero-watermark. Trans Netw Sci Eng 4(9):2188–2199
33. Rupa C, Harshitha M, Gautam S et al (2022) Securing Multimedia using a Deep Learning based Chaotic Logistic Map. IEEE J BIOMED HEALTH. https://doi.org/10.1109/JBHI.2022.3178629
34. Hegui Z, Baoming P, Zhiliang Zhu.et al, (2019) Two-dimensional sine-tent-based hyper chaotic map and its application in image encryption. J Chin Comput Syst 7:1510–1518 (1000-1220(2019) 07-1510-09)
35. Congxu Z, Guojun W, Kehui S (2018) Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box. Symmetry 10:1–15. https://doi.org/10.3390/sym10090399
36. Zea 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. https://doi.org/10.1007/s11042-016-3862-8
37. Xiaochen Y, Mianjie L (2018) Local multi-watermarking method based on robust and adaptive feature extraction. Signal Process 149:103–117. https://doi.org/10.1016/j.sigpro.2018.03.007

Publisher's Note

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