

Medical image watermarking encryption algorithm based on spiral transform and shift registers

Yan Liu(刘岩), Kaihua Wang(王凯华), Xianying Xu(徐宪莹), Yinghong Cao(曹颖鸿), Suo Gao(高锁), and Jun Mou(牟俊)

Citation: Chin. Phys. B, 2026, 35 (**8**): 080502. DOI: 10.1088/1674-1056/ae15f8
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

A modular-bias-sin chaotification method for enhanced discrete memristor chaotic maps

Shu Yi(易澍), Huihai Wang(王会海), and Kehui Sun(孙克辉)
Chin. Phys. B, 2026, 35 (**7**): 070504. DOI: 10.1088/1674-1056/ae181e

Modeling of a dual-capacitor neuron without an inductor

Zhen-Hua Yu(于振华), Yu-Chen Zhang(张钰晨), and Fei-Fei Yang(杨飞飞)
Chin. Phys. B, 2026, 35 (**6**): 060513. DOI: 10.1088/1674-1056/ae77d3

Symmetrical Turing instability in Chua corsage memristor siblings-based two-cell network

Zhicheng Tian(田桎成), Peipei Jin(靳培培), Shutong Liu(刘姝彤), Meiyuan Gu(顾梅园), Long Chen(陈龙), and Guangyi Wang(王光义)
Chin. Phys. B, 2026, 35 (**6**): 060511. DOI: 10.1088/1674-1056/ae68f9

Spectral statistics and wave-chaos transition in three-dimensional acoustic cavities

Xiaodong Zhang(张晓东)
Chin. Phys. B, 2026, 35 (**6**): 060510. DOI: 10.1088/1674-1056/ae3555

A chaotic hierarchical encryption/watermark embedding scheme for multi-medical images based on row-column confusion and closed-loop bi-directional diffusion

Zheyi Zhang(张哲祎), Jun Mou(牟俊), Santo Banerjee, and Yinghong Cao(曹颖鸿)
Chin. Phys. B, 2024, 33 (**2**): 020503. DOI: 10.1088/1674-1056/ad0775

Medical image watermarking encryption algorithm based on spiral transform and shift registers

Yan Liu(刘岩)[1], Kaihua Wang(王凯华)[2,†], Xianying Xu(徐宪莹)[1], Yinghong Cao(曹颖鸿)[1,‡], Suo Gao(高锁)[1], and Jun Mou(牟俊)[1]

[1] *School of Information Science and Engineering, Dalian Polytechnic University, Dalian* 116034, *China*
[2] *Department of Basic Education,Liaoning Vocational College of Light Undustry, Dalian* 116100, *China*

(Received 2 September 2025; revised manuscript received 20 October 2025; accepted manuscript online 22 October 2025)

The popularity of telemedicine has opened up the possibility of realizing scenarios such as multi-party online consultations and remote surgical protocols for treating patients. In the process of diagnosing and treating patients, medical image movies containing the patients' physical conditions are transmitted across regions. Given that the security of medical image transmission is directly related to patient safety, this paper aims to address encryption issues in this field. A novel watermark encryption scheme is proposed, which adopts a hybrid architecture of dynamic spiral operations and shift registers. In obtaining the embedded watermark, focusing on the non-visualization and time cost, the edge features of medical images are first extracted by the Canny operator and are used as the watermark information. In the specific embedding implementation, NSCT, DCT, and SVD techniques are combined to realize a good embedding of the watermark. After obtaining the medical watermark image, the multi-size watermark image is merged and converted into a cube of plaintext information. Chaotic sequences generated by coupling discrete memristors with Rulkov neurons are used to define the starting point and direction of spiral operations, thereby disrupting the pixel positions within the cube. The diffusion part utilizes the shift register principle to convert the pixel values into 8-bit strings. This is followed by a dissimilarity operation with the chaotic sequence, thereby altering the pixel values to produce the final ciphertext cube. The scheme successfully passed a series of tests, including key space and key sensitivity, histogram, pixel correlation, noise attack, etc. In terms of watermark extraction and restoration, the reconstruction quality is clear and without obvious distortion. Therefore, it can be proven that the scheme can simultaneously meet the transmission efficiency and copyright protection requirements of medical images.

Keywords: medical image encryption, cube watermarking, canny operator, spiral transform, shift register

PACS: 05.45.–a, 05.45.Gg

DOI: 10.1088/1674-1056/ae15f8 **CSTR:** 32038.14.CPB.ae15f8

1. Introduction

In recent years, with the rapid development of artificial intelligence and the internet, the digital storage and remote sharing of medical images have become an integral part of modern medical diagnosis.[1–3] Due to their significant advantages in visualization performance, data carrying capacity, and data redundancy, digital images have gradually become the mainstream method for medical information exchange.[4–6] However, security issues such as data leakage, malicious tampering, and unauthorized access during the transmission of medical images have further fueled the increased exploitation of internet technology by criminals, who seek to gain personal benefits by accessing medical information.[7–10] Additionally, patients have an inviolable right to ownership of their personal treatment information. Any erroneous transmission of diagnostic materials to consulting physicians during treatment can deal a severe blow to the treatment process.[11,12] In this context, the use of digital watermarking technology is considered to better protect the copyright of transmitted medical images and mitigate transmission risks. Therefore, this paper combines encryption technology and digital watermarking technology to design a brand-new medical image watermark encryption scheme. The reliability of the scheme and the stability of the watermark embedding are verified through simulation testing.[13–16]

Chaotic systems have become the focal direction of modern cryptography research because of their initial value sensitivity, unpredictability, non-periodicity, and a series of other excellent properties that fit the field of cryptography.[17,18] The classification of chaotic systems can be divided into continuous chaotic systems and discrete chaotic systems in terms of type, and further divided into low-dimensional chaotic systems and high-dimensional chaotic systems in terms of dimension.[19,20] In this paper, a discrete memristor-coupled Rulkov neuron system (DMCNR) is selected as a scheme carrier, which combines the complexity and stability of high-dimensional systems with the iteration speed and low computational complexity of discrete systems.[21,22] Memristor-

†Corresponding author. E-mail: jcb@lnli.edu.cn
‡Corresponding author. E-mail: caoyinghong@dlpu.edu.cn

© 2026 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

coupled neurons simulate the electrophysiological characteristics of biological organisms to construct a bio-inspired encryption system. This design can generate more complex hyperchaotic attractors, further confirming that the chaotic sequences generated by the system have better randomness and can achieve more ideal encryption effects.[23–25]

At the same time, given that a single encryption technique cannot safeguard the transmission of image information over insecure channels, and considering the unique nature of medical images that renders their ownership highly sensitive, a watermarking-based implementation approach has been designed. As a core method in copyright protection, watermarking technology primarily focuses on evaluating three key aspects: robustness, invisibility, and information capacity.[26,27] Due to the complexity of medical images in clinical and telemedicine, such as CT, x-ray, and MRI, different devices generate different resolutions and sizes of medical image data. Therefore, the designed algorithm is centered around the encryption of medical images of multiple sizes, which can make up for the lack of encryption of a single type of image. In order to realize this idea, this design introduces the combination of watermarking technology and image encryption, which not only provides a larger key space for watermarked image encryption but also improves the anti-attack ability of watermarked images.[28,29]

So far, a lot of research results have been achieved in the field of image encryption and watermarking technology. Qiu *et al*. proposed an encryption operation utilizing the hyperchaotic system 2D-CSCM. Their approach decomposes a color image into three grayscale images to encrypt its three-dimensional bit-level matrix, thereby enhancing security during transmission.[30] Wang *et al*. proposed a new self-embedded watermarking encryption scheme for holographic images. The corresponding phase hologram is obtained by using holographic technology, and the encryption algorithm adopts the Hilbert transform principle and the law of genetic center.[31] Alexan *et al*. proposed to combine multiple two-dimensional images together to form an image cube, and six new S-boxes in the hyperchaotic four-dimensional Chen system are used as the chaotic system for the subsequent encryption and decryption operations.[32] Gao *et al*. proposed a multi-image encryption scheme based on hyper-chaotic mapping and a three-dimensional cube. This scheme realizes encryption by first segmenting the multi-image and then performing DNA coding along different angles.[33] Ma *et al*. proposed a color watermark image encryption algorithm based on memory cell neural network and Arnold transform, where a memristor is introduced into the cellular neural network, and the Arnold transform is used for the disruption of the image to enhance the security of the watermarked image.[34]

However, in existing schemes, it is difficult to maintain a balance between the application of watermarking technology and encryption technology. When faced with higher security standards, many shortcomings gradually become apparent (high encryption costs, difficulty in extracting and reconstructing watermarks, low robustness, etc.). In order to make up for the still-existing problems, a new watermark image encryption scheme is proposed. First, the edge features of medical images are obtained as watermarks embedded in plaintext images by the method of Canny operator, and the watermarks are embedded by applying the combined method of non-subsampled contourlet transform (NSCT), discrete cosine transform (DCT), and singular value decomposition (SVD). Because the three have different transformation characteristics, the watermarked images obtained by applying the combined method can resist different types of attacks, and also can maintain the visual quality of the medical images in a better way, which is vital for both the doctors and the patients.[35] In terms of image encryption, the disambiguation part adopts the method of dynamic spiral transformation, which is based on the two-dimensional spiral transformation to carry out a similar transformation on the cube, so that the dynamic spiral disambiguation algorithm can change the position of all the pixel values on the cube at one time. The diffusion part uses a combination of shift registers and XOR operations to change the values of the image pixel points because shift registers have the characteristics of parallel input and output, which makes them capable of processing a large amount of medical image data in a short period of time to meet the requirements of real-time encryption. The XOR operation is a bit-level operation that can achieve the ability to process high-resolution images. Therefore, combining the two for diffusion algorithms can save encryption time to improve efficiency and process high-resolution images. The main contributions of this paper are as follows:

1. For medical images of various sizes, we have designed a more convenient and efficient watermark encryption protection solution.

2. Using dynamic coordination technology, an encryption-watermark protection framework is constructed, combining spiral algorithms and shift register principles to achieve secure transmission.

3. Robust watermark embedding is achieved using a combination of frequency domain technology, which has the advantages of good invisibility and high reconstruction quality.

4. Simulation results and performance tests have proven that the proposed solution is widely applicable and offers superior performance.

The rest of the article is structured as follows. The second part describes the selected chaotic system and presents the dynamics analysis and a brief description of the watermarking implementation application techniques. The fourth and fifth

parts present the decryption scheme as well as the simulation test results. The sixth part analyzes the performance test results. Finally, the conclusion of this article is given.

2. Related methods

2.1. Chaotic system model

In this paper, a DMCNR is selected as a vehicle for cryptographic schemes.[36] The system is constructed and implemented by simulating the synaptic function between neurons, introducing two discrete quadratic flux controllers in Rulkov neurons to model the synapses, and obtaining a chaotic system with high complexity and stability. Compared to traditional continuous-form neural models, discrete systems offer faster computation speeds, making them suitable for large-scale image simulation testing and dynamic analysis. The integration of memristors aims to endow the system with intrinsic memory characteristics, enabling individual neurons to exhibit complex multimodal behaviors difficult to achieve with conventional models. This memristor-coupled chaotic system possesses heightened complexity and unpredictability, demonstrating significant practical application value and promising prospects in the field of information security. The equations are given as follows:

$$\begin{cases} x_{n+1} = a/(1+x_n^2) + b + c(y_n - x_n)\tanh(z_n^2), \\ y_{n+1} = a/(1+y_n^2) + b + c(y_n - x_n)\tanh(z_n^2), \\ z_{n+1} = z_n + d(y_n - x_n), \end{cases} \tag{1}$$

where x, y, and z are the state variables of the system, and a, b, c, and d are the system parameters. In order to better analyze the dynamics of the chosen DMCRN chaotic system, this section discusses it in terms of the Lyapunov exponent and phase diagram.

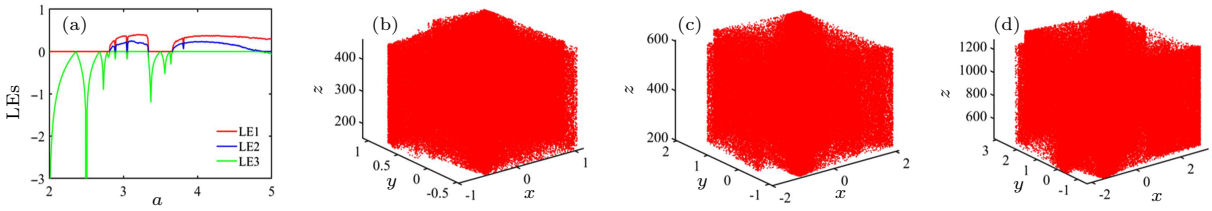


Fig. 1. Chaos system dynamics analysis. (a) LEs of parameter a. (b)–(d) Phase diagram for $a = 3$, $a = 3.8$, $a = 4.8$.

The parameter a is selected for validation with fixed parameters $b = -2$, $c = 0.15$, $d = 0.02$ and initial values $x_0 = 0.2$, $y_0 = 0.5$, $z_0 = \pi$. When $a \in [2,5]$, the Lyapunov exponent diagrams are shown in Fig. 1(a), which can clearly distinguish the regions of chaos as well as hyperchaotic states with different parameters. Figures 1(b)–1(d) give the attractor phase diagrams for different values of a. It can be seen that the selected system has good dynamics.

2.2. Image edge detection

In this paper, the Canny operator is selected to obtain the edge information of the plaintext image, thereby embedding the received data as a watermark into the plaintext image. The edges are usually the most stable and information-rich parts of an image. Watermarks extracted from these areas have strong anti-interference ability, can better resist external attacks, have good robustness, and can effectively reduce the amount of transmitted data to save time and costs. The image edge extraction using the Canny operator and the comparison results with other operators are presented in Figs. 2 and 3.

The Canny operator adopts the double-threshold technique to determine the edge. In the field of medical research, medical images usually contain complex tissue structures and details. In medical images with a lot of noise, this operator can accurately locate the position of the edge and avoid misjudgment. This high-precision edge detection is crucial for the further processing of medical images.

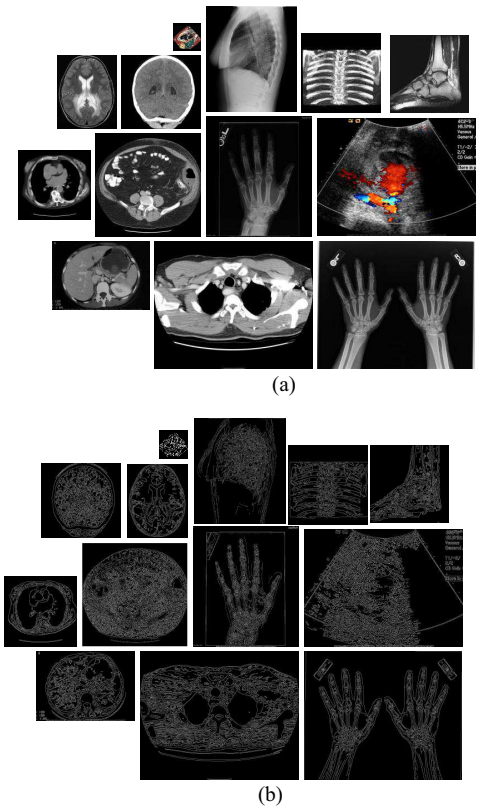


Fig. 2. Image edge extraction based on Canny operator. (a) Plaintext image. (b) Embedded watermark.

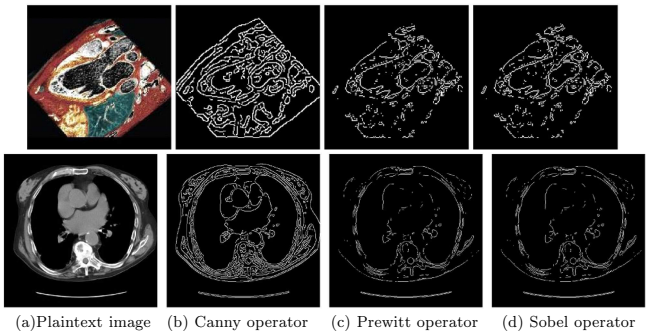


Fig. 3. The comparison results with other operators. (a) Plaintext image, (b) Canny, (c) Prewitt, (d) Sobel.

2.3. Non-subsampled contourlet transform

The NSCT is a multi-scale and multi-directional image decomposition technique, built upon a nonsubsampled pyramid (NSP) structure combined with a nonsubsampled directional filter bank (NSDFB). Compared with other conventional methods such as DWT and DCT, it can better capture the edge information in all directions of the image and avoid distortion problems. The detailed NSCT decomposition diagram is presented in Fig. 4.

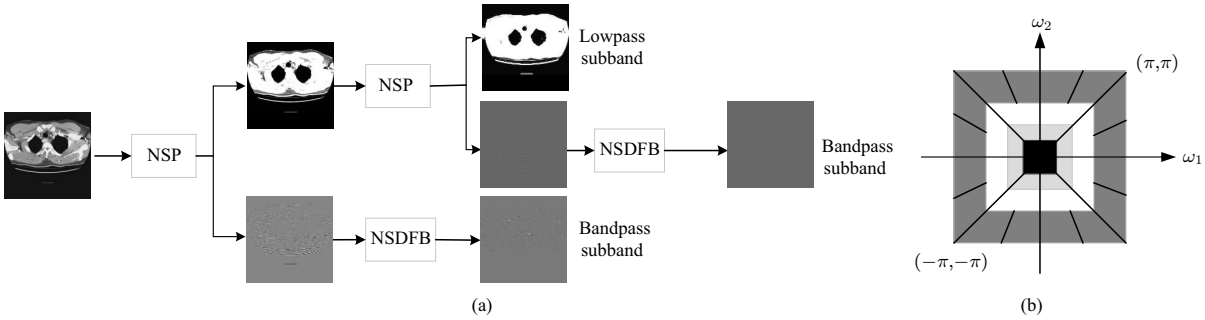


Fig. 4. NSDFB structural decomposition diagram. (a) Decomposition structure diagram. (b) Frequency-domain decomposition structure diagram.

First, the NSCT of the image can obtain the low-pass sub-band image and the bandpass sub-band image. Second, the NSP decomposition is performed on the low-pass sub-band, and the NSDFB decomposition is carried out on the bandpass sub-band simultaneously. After the bandpass decomposition, high-frequency information in different directions is obtained, and the resulting image is more detailed.

3. Digital watermarking encryption scheme

To ensure that medical images can be transmitted securely over the internet and to protect personal information, such as patient privacy, this section proposes a method that combines NSCT, DCT, and SVD to embed watermarks in the frequency domain of medical images. Then, it fuses multiple watermarked images into a cube. In image encryption, the disruption part generates chaotic random numbers through chaotic sequences, and utilizes the dynamic helical transform principle as well as translation operations to realize the change of pixel positions. The diffusion part accomplishes the change of pixel values through a shift register and the XOR principle, and the ciphertext image cube can then be obtained. An encryption flowchart is shown in Fig. 5.

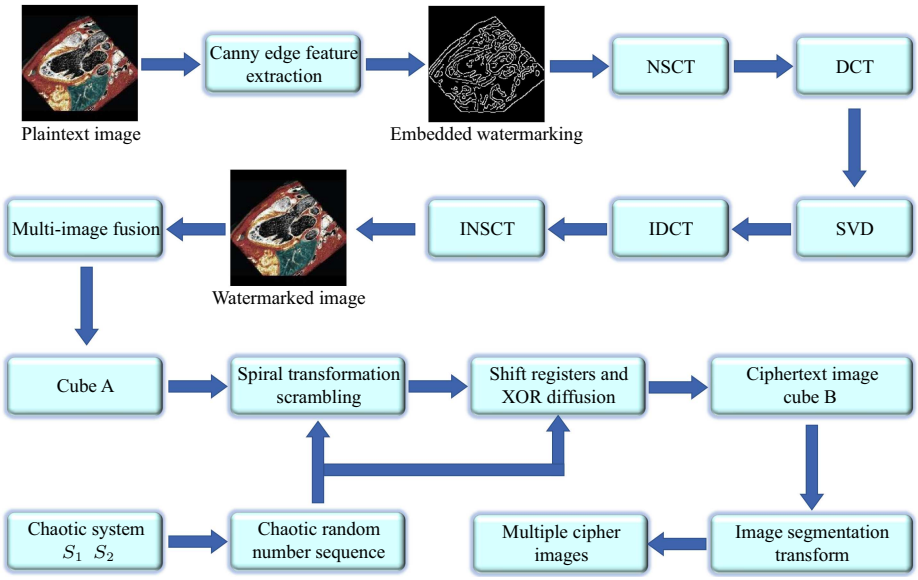


Fig. 5. Flowchart of the encryption scheme.

3.1. Watermark embedding process

For the algorithm proposed in this paper, the detailed steps of watermark embedding are introduced below. Figure 6 shows the watermarked image after embedding the watermark.

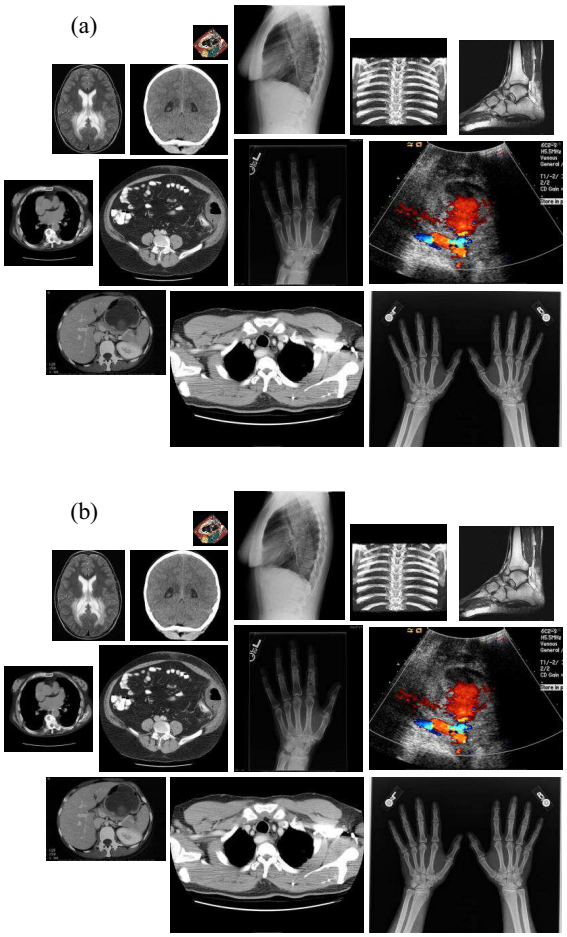


Fig. 6. Watermark embedded in image. (a) Plaintext image. (b) Watermarked image.

Step 1: The direction filter is used to perform NSCT decomposition on the plaintext image P and the watermark image into low-pass sub-bands and bandpass sub-bands in different directions.

Step 2: The low-pass sub-bands after NSCT decomposition were selected for DCT decomposition, and the DCT coefficients were obtained. A transformation from the spatial domain to the frequency domain of an image is achieved through the DCT, which makes the embedding of watermarks more convenient.

Step 3: By performing SVD decomposition on the DCT coefficients of the watermark image and the plaintext image, the coefficient matrices can be obtained as $[S_{\mathrm{w}},\Sigma_{\mathrm{w}},V_{\mathrm{w}}^{\mathrm{T}}]$ and $[S_{\mathrm{p}},\Sigma_{\mathrm{p}},V_{\mathrm{p}}^{\mathrm{T}}]$ respectively.

Step 4: The new diagonal matrix "$\Sigma_{\mathrm{p}'}$" is obtained by using the following formula, and then the new SVD is obtained. Among them, μ is the gain factor, which is used to completely embed the watermark into the image.

$$\Sigma_{\mathrm{p}'} = \Sigma_{\mathrm{p}} + \mu\Sigma_{\mathrm{w}}. \tag{2}$$

Step 5: Next, the inverse DCT and inverse NSCT operations are performed on the new NSCT coefficients, and finally the watermarked image P_{l} is obtained.

3.2. Three-dimensional spiral scrambling

Although the two-dimensional spiral transform is simpler in operation as well as understanding, the pixel correlation of a single image is stronger. Therefore, this paper proposes a new three-dimensional spiral transform, based on the two-dimensional basis of the pixel values on the cube of the position transformation operation. As shown in Fig. 7, taking a three-dimensional image matrix of size $7\times7\times3$ as an example. The detailed procedure for implementing the three-dimensional spiral transformation is outlined as follows:

Step 1: Merge multiple watermark images into a cube A.

Step 2: Divide the cube into L small rectangles of $H\times W\times1$ by layer, i.e., each small rectangle is a layer of the cube A. If neither the length nor the width of the cube is an odd integer, then perform the pixel value filling operation by adding a column or a row of zero matrices to the right column or the bottom row of the cube.

$$\mathrm{Layers} = \mathrm{cell}(L,1), \tag{3}$$

$$\begin{cases} P_{11} = \left[P, \mathrm{zeros}(M,1)\right], \\ P_{12} = \left[P, \mathrm{zeros}(1,N)\right]. \end{cases} \tag{4}$$

Step 3: Select the centers of each layer and place them sequentially in the empty one-dimensional matrix.

$$\begin{cases} x = \mathrm{floor}\left(\dfrac{H}{2}\right)+1, \\ y = \mathrm{floor}\left(\dfrac{W}{2}\right)+1. \end{cases} \tag{5}$$

Step 4: Traverse the pixel values of the image from the inner circle to the outer circle as shown in Fig. 6. The starting point and spiral direction of each circle are determined by chaotic random numbers generated from the chaotic sequence X_1. The left, top, right, and bottom directions of the circle are numbered sequentially as 0, 1, 2, and 3.

$$\begin{cases} X_1 = (S_1((\mathrm{end}-M+1:\mathrm{end})\times10^{16}) \bmod L)+1, \\ X_2 = (S_2((\mathrm{end}-M+1:\mathrm{end})\times10^{16}) \bmod L)+1, \end{cases} \tag{6}$$

$$\mathrm{direction} = \mathrm{mod}\left(\mathrm{floor}(X_1\times10^5),4\right). \tag{7}$$

Step 5: According to the chaotic sequence X_2, the binary bits 0 and 1 are obtained; therefore, whether the direction of the circle is clockwise or counterclockwise is chosen, with 0 being the clockwise direction and 1 being the counterclockwise direction.

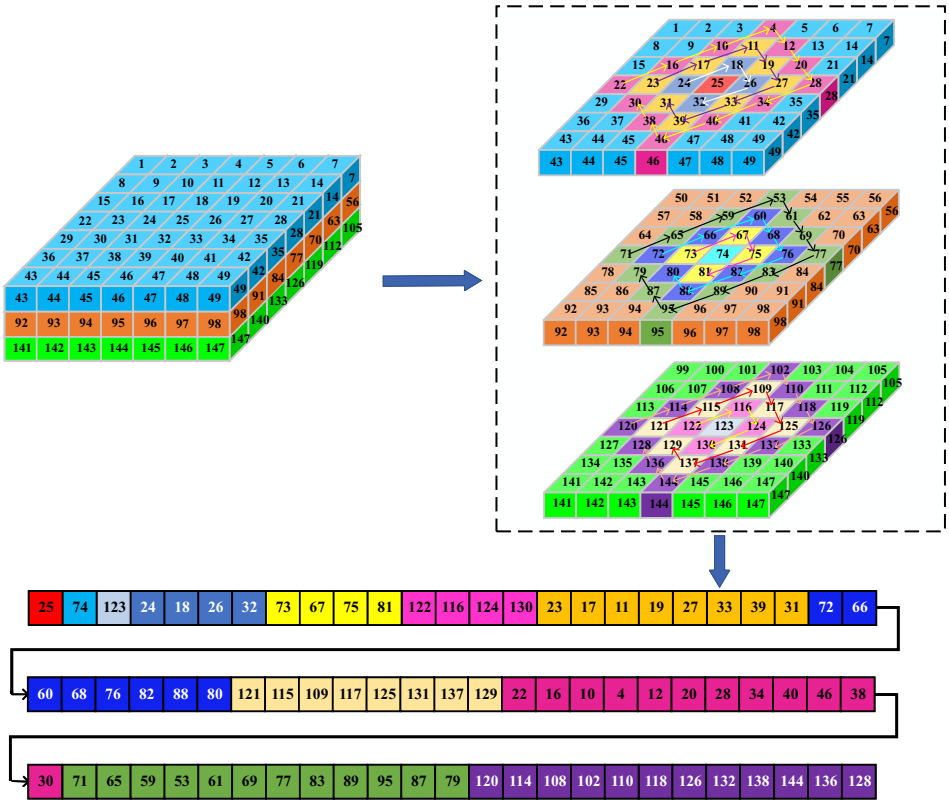


Fig. 7. The effect drawing of the first spiral transformation.

Step 6: It is worth noting that here all the pixel values of the inner first circle of each layer are to be traversed and placed in the empty matrix, followed by the inner second circle of each layer.

Step 7: After the first cycle, follow the translation operation of the two-dimensional spiral transformation, as shown in Fig. 8, and then perform the second spiral transformation with the same spiral steps as the first. The results are shown in Fig. 9.

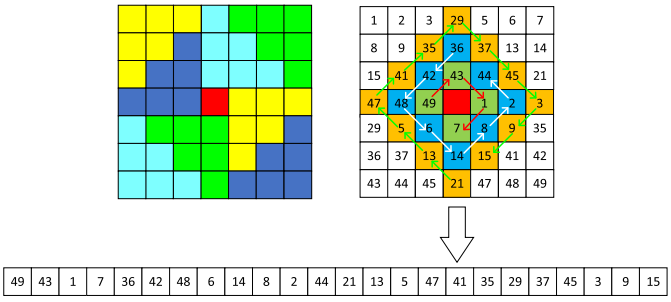


Fig. 8. Translation operation and the second round of spiral.

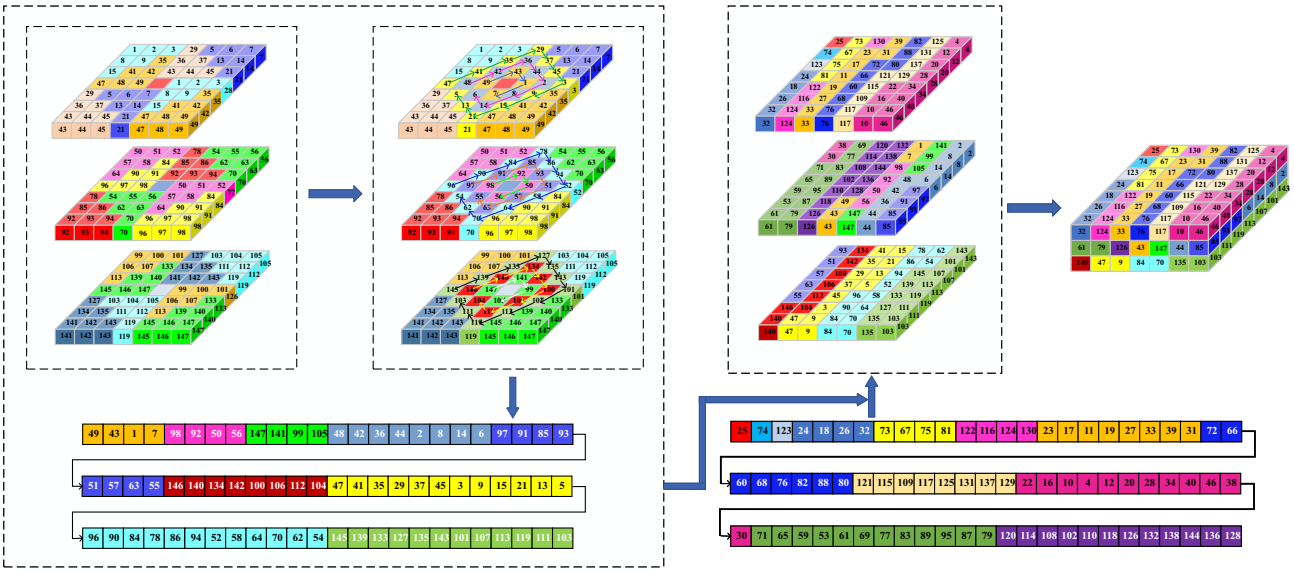


Fig. 9. Two spiral transformations and then reintegration into a cube.

3.3. Shift register and XOR combined diffusion

Step 1: The chaotic random number sequences r_1, r_2, r_3 generated using chaotic sequences S_1, and S_2 are again used in the diffusion algorithm, and the results are shown below:

$$\begin{cases} r_1 = \left(S_1((\text{end}-N+1:\text{end})\times 10^{16}\right) \bmod L+1), \\ r_2 = \left(S_2((\text{end}-N+1:\text{end})\times 10^{16}\right) \bmod (L-3)+1), \\ r_3 = \left(S_2((\text{end}-N+1:\text{end})\times 10^{16}\right) \bmod L+1). \end{cases} \quad (8)$$

Step 2: The image P_1 matrix is converted to an 8-bit binary matrix with a sequence of chaotic random numbers r_1, r_2 is used to control the selection of the bits of the P_1 matrix, followed by the XOR operation.

Step 3: The chaotic random number series r_3 is used to control the starting position of the cyclic shift of the binary matrix after the XOR operation, and the diffused cube is denoted as B. The following equation gives the result of the cyclic shift, where strcat$(\cdot)$ means to concatenate two strings:

$$P_1'(i,:) = \text{strcat}(P_1(i, r_3(i):\text{end}), P_1(i, 1:r_3(i)-1)). \quad (9)$$

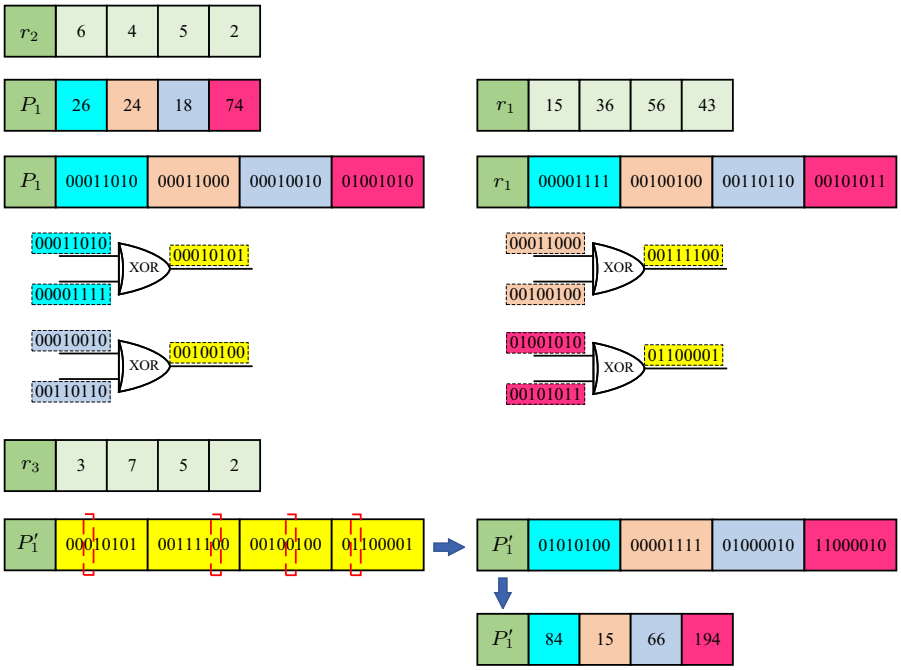


Fig. 10. String XOR and circular shift process.

4. Decryption scheme

The decryption process is the inverse of the encryption process. The detailed steps are as follows:

Step 1: Fuse multiple ciphertext images into a ciphertext image cube B' or decrypt the ciphertext cube B' directly.

Step 2: Use the same key as the encryption process to get the chaotic sequences S_1, S_2, and then use the chaotic sequences to get the chaotic random number sequences X_1, X_2, r_1, r_2, r_3.

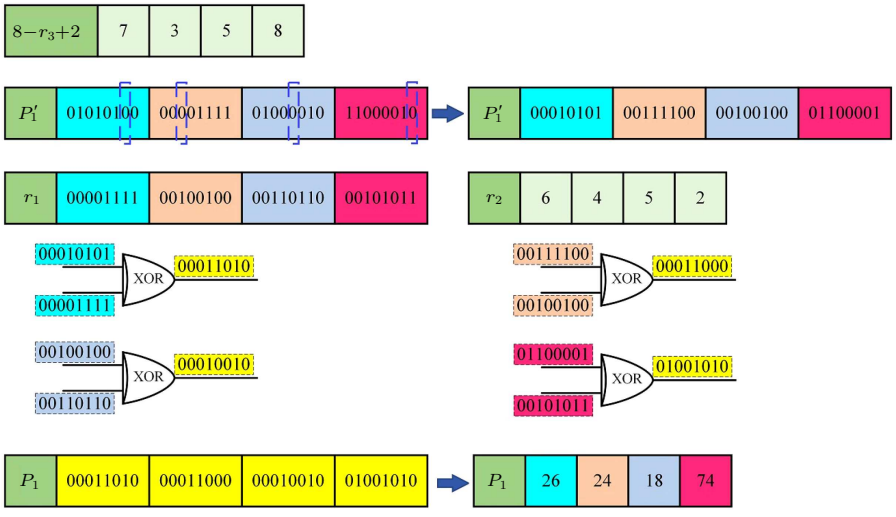


Fig. 11. String XOR and cyclic shift inverse procedure.

Step 3: Backpropagation is the process of reducing the expanded result to the desired result.

$$P_1(i,:) = \text{strcat}(P_1'(i, 8 - r_3(i) + 2 : \text{end}),$$
$$P_1'(i, 1 : 8 - r_3(i) + 1)). \tag{10}$$

Step 4: Figure 11 shows the detailed steps of the 8-bit binary string XOR and shift inverse process.

Step 5: The inverse disarray operation is performed on the result after inverse diffusion by first splitting the data of the two spiral transformations; the pixel value after the first spiral is noted as P_{21}, and the pixel value after the second spiral transformation is noted as P_{22}.

Step 6: For P_{22}, the translation is reversed according to the rules used in encryption, and then each pixel value is traversed in order from the outer circle to the inner circle. The direction of the spiral is determined by the chaotic sequence X_2, and the starting point is determined by X_1.

Step 7: The inverse helical transform operation is also performed in the same way for P_{21}, and the pixels at the center of each layer of the encryption process are sequentially extracted and put back to the center of the corresponding layer.

Step 8: Stack all the small $H \times W \times 1$ rectangles in their original order and restore them as $H \times W \times L$ sized cubes.

Step 9: The image is segmented into multiple watermarked images, for which NSCT decomposition, DCT transform, and SVD decomposition are performed, and then IDCT and INSCT are taken to obtain the embedded watermark as well as the decrypted plaintext image.

5. Simulation result

In order to see more clearly the practicality of the proposed algorithm in encrypting medical images and copyright protection, 13 medical images of different sizes are selected as plaintext images (dataset sources: https://github.com/linhandev/dataset) in this paper and tested using MATLAB 2019b simulation software. They are numbered in row-wise order (left to right, top to bottom) as 1.jpg through 13.jpg. Figure 12(a) gives the watermarked image after embedding the watermark in the plaintext image. It is split and re-fused into a watermarked image cube as shown in Fig. 12(b). The ciphertext image cube is obtained after disambiguation and diffusion operations as shown in Fig. 12(c). The ciphertext cube is segmented according to the size of the watermarked image, and the encryption effect of each image is shown in Fig. 13(a). The effect of decryption and segmentation of the ciphertext cube is shown in Fig. 13(b). After comparing Figs. 12(a) and 13(b), it can be seen that the decrypted image is visually identical to the image before encryption.

As Fig. 13(a) reveals, the encrypted image contains no discernible information about the original plaintext image, demonstrating that the proposed encryption scheme effectively safeguards patient privacy.

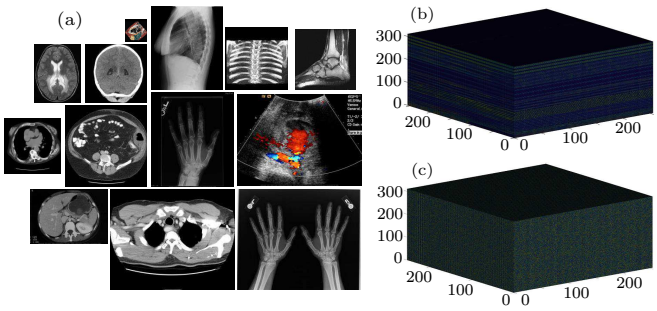


Fig. 12. Simulation results of the medical image encryption process. (a) Watermarked image. (b) Watermarked image cube. (c) Ciphertext image cube.

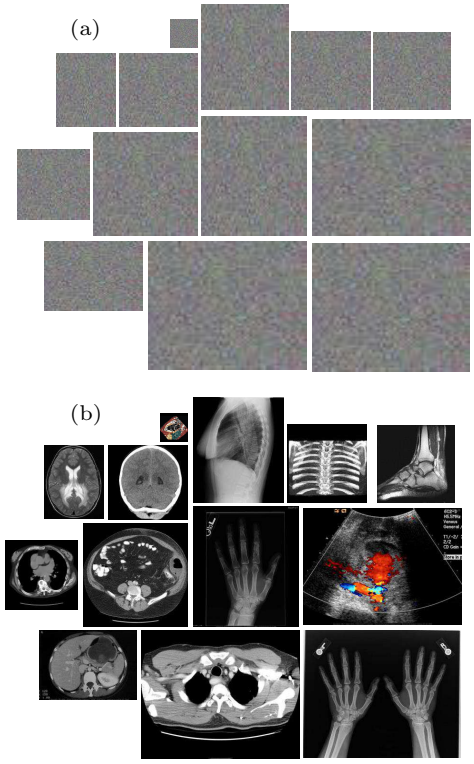
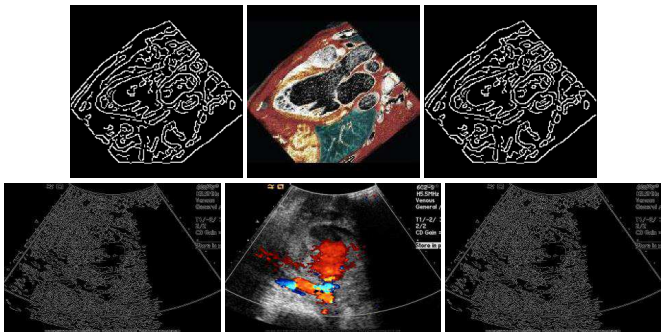


Fig. 13. Simulation results of the medical image decryption process. (a) Ciphertext image. (b) Decrypted image.

6. Performance test result

6.1. Watermark reconstruction

Embedding watermarks in images protects the copyright of information, but the recipient needs to perform watermark extraction and reconstruction operations on the decrypted medical images. The information quality and distortion degree after watermark reconstruction can be used to measure the quality of the proposed embedding algorithm. The quality of watermark reconstruction can be detected by observing or calculating the value of PSNR. Figure 14 shows the embedded watermark and the image after watermark extraction. Visually, there is no obvious difference. Table 1 compares the test results of PSNR with those of other literature.



(a) (b) (c)

Fig. 14. Watermark reconstruction. (a) Embedded watermark. (b) Watermarked image. (c) Watermark reconstruction image.

Table 1. The test and comparison results of PSNR.

Proposed	Ref. [37]	Ref. [38]	Ref. [39]	Ref. [40]
46.34	36.47	41.66	37.71	43.19

Step 1: The watermarked image undergoes NSCT decomposition to yield low-pass and band-pass sub-bands. The same sub-bands that were used during watermark embedding are then selected.

Step 2: Second, the selected sub-bands after NSCT decomposition are subjected to DCT decomposition, and the DCT coefficients can be obtained.

Step 3: Calculate the SVD value of the DCT coefficient and obtain the coefficient matrix $[S_e, \Sigma_e, V_e^T]$.

Step 4: Perform the watermark extraction operation according to the following formula. Among them, μ is the same gain factor as when embedded.

$$\Sigma_{w1} = \frac{\Sigma_e - \Sigma_p}{\mu}. \tag{11}$$

Step 5: Based on Σ_{w1}, a new SVD will be obtained, and then a new NSCT coefficient will be obtained.

Step 6: Next, inverse DCT and inverse NSCT operations are performed on the new NSCT coefficients, and finally the watermark image is obtained.

6.2. Key space and key sensitivity test

The key space is an important criterion used to reflect the algorithm's security. A robust encryption algorithm is resistant to both brute-force and exhaustive attacks. In chaotic image encryption algorithms, the key space is usually related to the initial conditions of the chaotic system. The key space in this paper is composed of the parameters a, b, c, and d of the discrete hyperchaotic mapping system and the initial values x_0, y_0, and z_0. During the encryption process, all parameters remain unchanged. During the decryption process, a slight perturbation is added to one of the parameters. Should decryption fail, the key space size for this parameter can then be computed. Through individual tests, it can be obtained that the total key space is 2^{363}, which is much larger than the standard value of 2^{100}. Therefore, it can be proven that this algorithm can effectively resist external brute force attacks and exhaustive attacks. Table 3 compares the key space sizes with those in other literature. Evidently, the key space of this algorithm is significantly larger than those of other comparative algorithms.

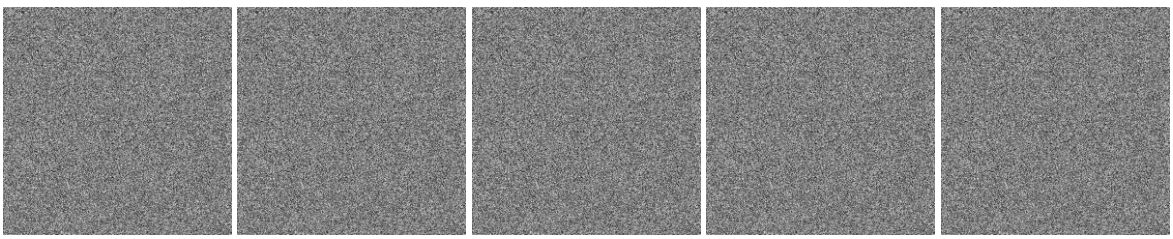
Table 2. Key space test results.

Keys	Space
b, c, d	10^{15}
a, x_0, y_0, z_0	10^{16}
Total	$10^{109} \approx 2^{363}$

Table 3. Key space of different algorithms.

Algorithms	Proposed	Ref. [41]	Ref. [42]	Ref. [43]	Ref. [44]
Key space	2^{363}	2^{266}	2^{210}	2^{154}	2^{197}

In chaotic image encryption, key sensitivity is divided into key sensitivity during encryption and decryption. The former is used to slightly disturb the key before encryption, which will result in entirely different encryption results, while the latter is used to slightly disrupt the key before decryption, which will result in decryption failure. The results of slight perturbations of different parameters are shown in Fig. 15. The results demonstrate that the image encryption algorithm is highly sensitive to the encryption key.



(a) Parameter a (b) Parameter b (c) Parameter c (d) Parameter d (e) Parameter x

Fig. 15. Key sensitivity test results.

6.3. Histogram analysis

The histogram is used to represent the frequency of occurrence of different levels of gray values in plaintext images and ciphertext images. The histogram of plaintext images has obvious peaks and troughs, making it easy for attackers to obtain relevant information about the images. The key to privacy protection lies in effectively hiding the important information in the

images. Ideally, the histogram of the ciphertext image should be evenly distributed, and the frequency of occurrence of the gray values should tend to be horizontal. Only in this way can the image information be effectively hidden. For the digital image watermarking encryption scheme proposed in this paper, three test results of the histograms of plaintext images and ciphertext images are randomly selected in Fig. 16. It can be found that the image information is effectively hidden.

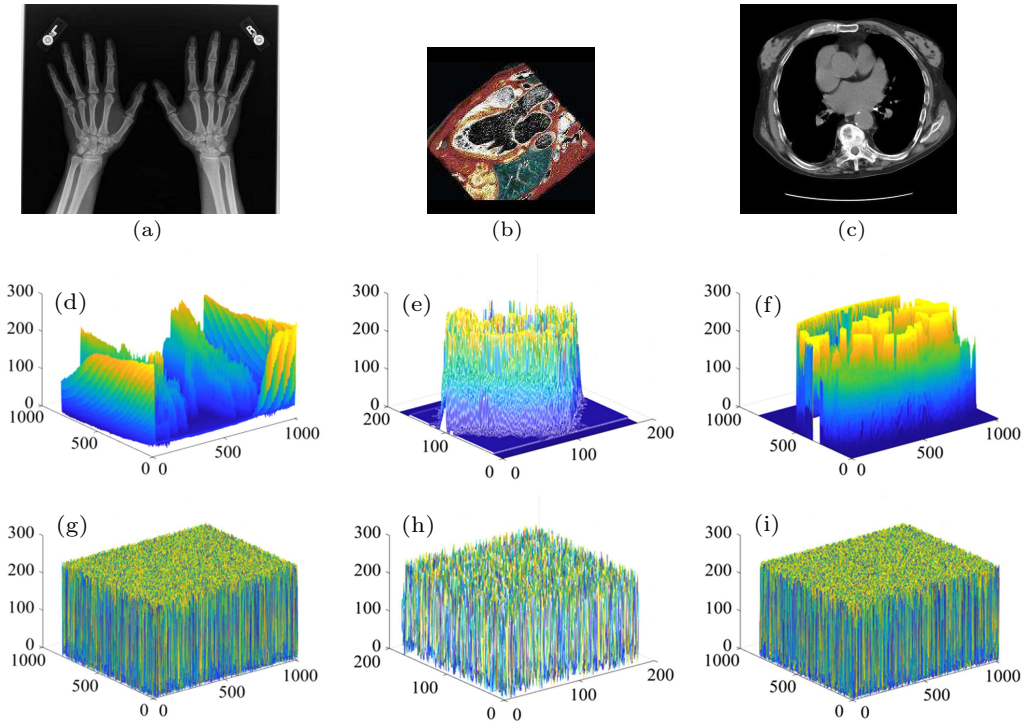


Fig. 16. Test results of plaintext and ciphertext image histograms. (a)–(c) Plaintext image. (d)–(f) Plaintext image histogram. (g)–(i) Ciphertext image histogram.

This paper selects the R channel of the plaintext image and ciphertext images for histogram testing and analysis.

6.4. Correlation test

The correlation test measures the strength of dependence between adjacent pixels in an image. In plaintext images, pixels exhibit strong correlations with their neighbors, which is essential for visual coherence. Table 4 presents the correlation coefficient test results for three medical images. It can be observed that the correlation coefficients of the encrypted images are close to 0, indicating that the proposed scheme achieves effective encryption.

As observed, the plaintext image exhibits strong pixel correlations, whereas the ciphertext image demonstrates uniform pixel distribution across the entire value range. This indicates the scheme's efficacy in effectively disrupting inter-pixel correlations.

Table 4. Different image correlation coefficient test results.

Images	Channel	Plaintext images			Ciphertext images		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
1.jpg	R	0.8902	0.9202	0.9525	0.0017	0.0012	–0.0012
	G	0.8764	0.9310	0.8874	0.0018	0.0017	0.0024
	B	0.8615	0.9322	0.8770	0.0014	–0.0033	0.0016
2.jpg	R	0.9404	0.8914	0.9295	–0.0019	0.0015	0.0005
	G	0.8541	0.8798	0.8895	0.0007	–0.0022	–0.0027
	B	0.9263	0.9374	0.8602	0.0011	0.0016	0.0025
3.jpg	R	0.9748	0.9710	0.9668	0.0022	–0.0037	0.0019
	G	0.8954	0.9621	0.8791	0.0006	0.0025	–0.0013
	B	0.9756	0.9514	0.8787	0.0052	–0.0019	0.0018

6.5. Information entropy test

Information entropy is used to reflect the degree of information contained in an image. Generally speaking, the larger the value of information entropy is, the richer the content of the image is, indicating that its randomness is stronger. For images with

gray values ranging from 0 to 255, the theoretical value of information entropy is 8, which is defined as $H = -\sum_{i=0}^{255} p(i)\log_2 p(i)$, where $p(i)$ represents the frequencies of the gray value of the i. During the process of image encryption, if the value of the information entropy of the encrypted image is closer to 8, it indicates that the pixel distribution of the image is uniform and has no obvious pattern. Attackers cannot obtain the relevant information of the plaintext image from it. Table 5 presents the information entropy of the plaintext image and ciphertext image of the above encryption scheme.

Table 5. Information entropy of different images.

Images	Image size	Plaintext images			Ciphertext images		
		R	G	B	R	G	B
1.jpg	$180\times180\times3$	3.8856	4.0248	4.7747	7.9989	7.9944	7.9993
2.jpg	$384\times475\times3$	5.5211	6.5862	5.2713	7.9908	7.9945	7.9961
3.jpg	$513\times478\times3$	6.2280	5.4514	6.4021	7.9914	7.9950	7.9969
4.jpg	$880\times1024\times3$	6.5585	4.3940	5.9396	7.9955	7.9968	7.9991
5.jpg	$512\times512\times3$	6.2214	5.2770	6.8027	7.9929	7.9930	7.9971
6.jpg	$500\times500\times3$	4.5343	4.4929	5.6601	7.9940	7.9980	7.9953

Table 6. Comparison of information entropy test results for ciphertext images with literatures.

Schemes	Correlation coefficient		
	R	G	B
Proposed	7.9989	7.9944	7.9993
Ref. [45]	7.9987	7.9985	7.9951
Ref. [46]	7.9966	7.9975	7.9976
Ref. [47]	7.9972	7.9965	7.9962
Ref. [48]	7.9965	7.9963	7.9967

The results demonstrate that the ciphertext's information entropy nears the ideal value of 8. This indicates that this scheme can not only achieve the purpose of protecting patients' privacy visually but also hide medical image information in data.

6.6. Differential attack test

Differential attack testing is performed by simultaneously encrypting the plaintext image twice. Before the second encryption, minor changes must be made to the plaintext image. The differences between the ciphertext images obtained after the two encryptions are compared through NPCR and UACI. C_1 and C_2 represent ciphertext images, and the normalized pixel change rate (NPCR) is calculated using Eq. (12). If the NPCR value exceeds the theoretical threshold of 99.6094%, or if the UACI value approaches the standard benchmark of 33.4635%, it can indicate that the algorithm has a good anti-differential ability. Table 7 compares this scheme with other literature.

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M\times N}\times 100\%, \tag{12}$$

where $D(i,j)$ is a bipolar array of the same size as C_1 and C_2, given by

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j), \\ 1, & C_1(i,j) \neq C_2(i,j), \end{cases} \tag{13}$$

where $C(i,j)$ is the pixel value at position (i,j) in the ciphertext image, the unified average changing intensity (UACI) can be calculated using

$$\mathrm{UACI} = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255\times M\times N}\times 100\%. \tag{14}$$

Table 7. Comparing the ability of different algorithms to resist differential attacks.

Schemes	$\mathrm{NPCR}_{\mathrm{aver}}$ (%)	$\mathrm{UACI}_{\mathrm{aver}}$ (%)
Proposed	99.6158	33.4654
Ref. [49]	99.6133	33.4434
Ref. [50]	99.6241	33.4741
Ref. [51]	99.6031	33.4122
Ref. [52]	99.5972	33.4357

6.7. Robustness test

In chaotic image encryption, robustness is mainly used to evaluate the noise attacks and malicious shearing attacks by attackers during the image transmission. Whether the recipient can successfully decrypt the original image is closely related to the proposed algorithm. Common noises are divided into salt-and-pepper noise and Gaussian noise. The following test of noise attack involves applying different degrees of noise to the ciphertext cube. The quality of the algorithm is evaluated by the value of image restoration quality (PSNR), as shown in Fig. 17. Generally speaking, if the PSNR value is between 30 dB and 40 dB, the distortion degree of the image is considered acceptable. If the value is greater than 40 dB, it indicates that the algorithm has a strong anti-noise ability. If it is lower than 30 dB, it can be considered that the quality is poor. Figure 18 shows the restoration of the image after adding salt-and-pepper noise with an intensity of 0.03 to the ciphertext cube. Figures 17 and 18 demonstrate that the encryption scheme maintains decryption capability even when the ciphertext image is subjected to noise attacks.

During the image transmission process, malicious cutting may occur. A good encryption and decryption scheme is to ensure that the original image information can still be decrypted after the image is cut. The PSNR test results of 12.5%, 20% and 30% shear rates are shown in Fig. 19. It can be seen that

the value of PSNR decreases with the increase of the shear rate. Figure 20 shows the restoration effect of medical images with a shear rate of 20%. It can be seen that the decrypted image can still be observed.

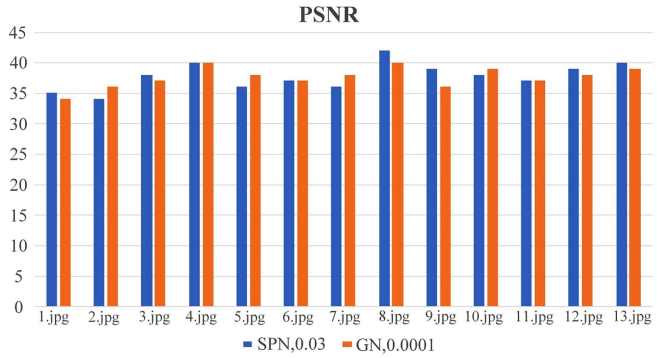


Fig. 17. Statistical graph of noise attack test results.

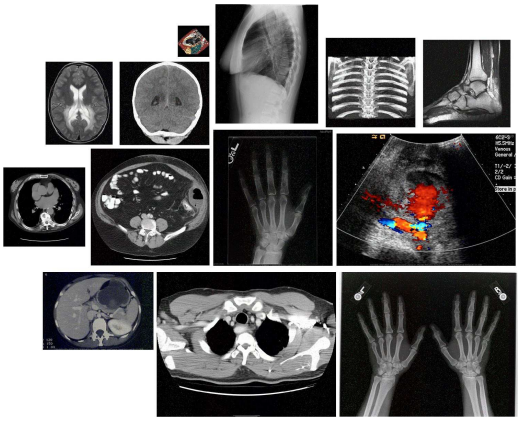


Fig. 18. Visual effects with noise attack test, SPN, 0.03.

It can be seen from this that the proposed encryption and decryption scheme has better robustness and can better protect the private information of patients during the image transmission process.

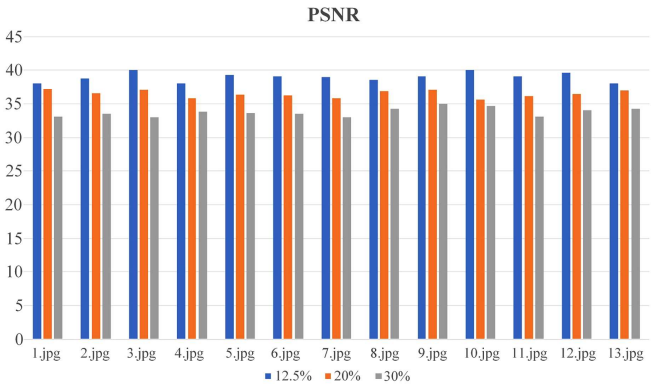


Fig. 19. Statistical graph of shearing attack test results.

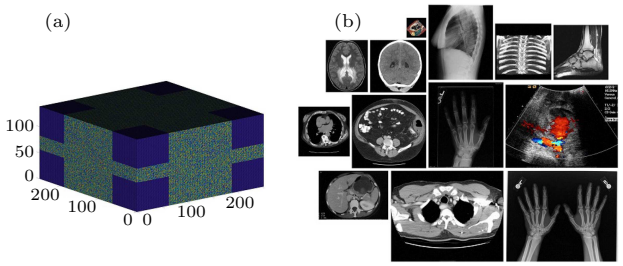


Fig. 20. Decrypted images with 20% shearing rate.

6.8. Analysis of encryption speed

In the privacy-preserving encryption of medical images, encryption speed is a very critical performance indicator, which usually refers to the time required for the encryption process. The faster the encryption speed and the shorter the time taken, the more efficient it is, while transmitting the same information to ensure security. The encryption and decryption times and speeds for images are given in Table 8. A comparison of the encryption speed of the proposed encryption scheme with other schemes is shown in Table 9, which shows the advantages of the scheme.

Table 8. Medical image encryption and decryption time and speed.

Encryption	Time (s)	Speed (MB/s)	Decryption	Time (s)	Speed (MB/s)
Scrambling	1.54	11.37	Inver-scrambling	1.35	12.97
Diffusion	9.31	1.88	Inver-diffusion	0.21	83.39
Total	10.85	1.61	Total	1.56	11.22

Table 9. Comparison of encryption speed with different algorithms.

Schemes	Proposed	Ref. [53]	Ref. [54]	Ref. [55]	Ref. [56]	Ref. [57]	Ref. [58]
Speed of encryption	1.61	5.02	3.96	4.22	2.99	5.14	1.65

Comparative analysis shows that the proposed encryption algorithm is superior to other algorithms in several aspects, including encryption speed and high security.

7. Conclusion

Aiming at the transmission security problems and copyright disputes arising from information interaction in the medical field, this paper proposes a new watermark encryption scheme for medical image cubes. The construction of the scheme includes two parts: watermark embedding and encryption realization. The image edge information obtained by the Canny operator is used as the embedded watermark, and the high similarity between the watermarked image and the plaintext image greatly improves the guarantee of embedding

without visualization, while the frequency domain embedding achieved by the combination technique realizes more effective resistance to external attacks. For encryption, the two-dimensional image is converted into a three-dimensional cube, and the dynamic spiral operation is used to realize the disruption of pixel points in the cube hierarchy. In terms of diffusion, the shift register principle is used to conceal the pixel information effectively by applying the XOR operation between the pixel value and the chaotic sequence. Simulation tests involving 13 medical images of varying sizes demonstrate the scheme's successful encryption and decryption performance across diverse image quantities and dimensions. The successful passing of a series of tests on the scheme verifies that it can effectively resist external sophisticated attacks. Finally, the embedded watermark is extracted and reconstructed, and given a comparison test to verify the ability to handle copyright disputes.

References

[1] El-Shafai W, Khallaf F, El-Rabaie E S M and El-Samie F E A 2021 *Journal of Ambient Intelligence and Humanized Computing* **12** 9007
[2] Pankaj S and Dua M 2024 *Information Security Journal: A Global Perspective* **33** 332
[3] Jain K, Aji A and Krishnan P 2021 *Pattern Recognition Letters* **152** 356
[4] Man Z, Gao C, Dai Y and Meng X 2024 *Nonlinear Dyn.* **112** 13571
[5] Ke G, Wang H, Zhou S and Zhang H 2019 *Measurement* **135** 385
[6] Lai Q and Hua H 2025 *Expert Systems with Applications* **264** 125854
[7] Gao S, Iu H H C, Erkan U, Simsek C, Toktas A, Cao Y, Wu R, Mou J, Li Q and Wang C 2025 *IEEE Transactions on Circuits and Systems for Video Technology* **35** 7706
[8] Huang Q X, Yap W L, Chiu M Y and Sun H M 2022 *IEEE Access* **10** 66345
[9] Jamal S S, Hazzazi M M, Khan M F, Bassfar Z, Aljaedi A and ul Islam Z 2024 *Expert Systems with Applications* **238** 122030
[10] Gao S, Ding S, Iu H H C, Erkan U, Toktas A, Simsek C, Wu R, Xu X, Cao Y and Mou J 2025 *Chaos: An Interdisciplinary Journal of Nonlinear Science* **35** 073105
[11] Dong Y, Yan R and Yin C 2024 *Scientific Reports* **14** 24735
[12] Singh D, Kaur S, Kaur M, Singh S, Kaur M and Lee H N 2024 *Computer Science Review* **54** 100659
[13] Chai X, Tang Z, Gan Z, Lu Y, Wang B and Zhang Y 2024 *Biomedical Signal Processing and Control* **90** 105877
[14] Ayubi P, Jafari Barani M, Yousefi Valandar M, Yosefnezhad Irani B and Sedagheh Maskan Sadigh R 2021 *Artificial Intelligence Review* **54** 1237
[15] Jackson J and Perumal R 2025 *Nonlinear Dyn.* **113** 7277
[16] Deng Q, Wang C, Sun Y and Yang G 2025 *IEEE Transactions on Cybernetics* **55** 3926
[17] Gao S, Zhang Z, Li Q, Ding S, Iu H H C, Cao Y, Xu X, Wang C and Mou J 2025 *IEEE Transactions on Dependable and Secure Computing* **22** 8011
[18] Wang X, Chen S and Zhang Y 2021 *Optics & Laser Technology* **139** 106837
[19] Zhang Y 2020 *Information Sciences* **520** 177
[20] Yu Z, Zhu K, Wang Y and Yang F 2025 *Chaos, Solitons & Fractals* **194** 116233
[21] Gao S, Wu R, Iu H H C, Erkan U, Cao Y, Li Q, Toktas A and Mou J 2025 *Computer Science Review* **58** 100816
[22] Yang F, Song X and Yu Z 2025 *Nonlinear Dyn.* **113** 7213
[23] Ma T, Mou J, Al-Barakati A A, Jahanshahi H and Miao M 2023 *Physica Scripta* **98** 105202
[24] Deng Q, Wang C, Sun Y, Deng Z and Yang G 2024 *IEEE Transactions on Circuits and Systems I: Regular Papers* **72** 300
[25] Tan S, Sun J, Tang Y, Sun Y and Wang C 2024 *Nonlinear Dyn.* **112** 5749
[26] Lai Q, Lai C, Zhang H and Li C 2022 *Chaos, Solitons & Fractals* **158** 112017
[27] Li Y, Li C, Li Y, Moroz I and Yang Y 2024 *Chaos, Solitons & Fractals* **182** 114800
[28] Zhang H, Kone M M K, Ma X Q and Zhou N R 2025 *Journal of the Franklin Institute* **362** 107511
[29] Hu L L, Chen M X, Wang M M and Zhou N R 2025 *Knowledge-Based Systems* **324** 113804
[30] Qiu H, Xu X, Jiang Z, Sun K and Xiao C 2022 *Nonlinear Dyn.* **110** 2869
[31] Wang L, Zhou N, Sun B, Cao Y and Mou J 2024 *Chin. Phys. B* **33** 050501
[32] Alexan W, Hosny K and Gabr M 2025 *Cluster Computing* **28** 1
[33] Gao X, Mou J, Banerjee S, Cao Y, Xiong L and Chen X 2022 *Journal of King Saud University-Computer and Information Sciences* **34** 1535
[34] Ma J Z, Yang Y G, Jiang D H and Liao X 2024 *Physica Scripta* **99** 125263
[35] Hosny K M, Elnabawy Y M, Salama R A and Elshewey A M 2024 *Scientific Reports* **14** 30597
[36] Cui J, Cao Y, Jahanshahi H, Mou J and Sun B 2024 *Multimedia Tools and Applications* **84** 15099
[37] Gao S, Zhang Z, Iu H H C, Ding S, Mou J, Erkan U, Toktas A, Li Q, Wang C and Cao Y 2025 *IEEE Internet of Things Journal* **12** 18115
[38] Wang L, Banerjee S, Cao Y, Mou J and Sun B 2024 *Nonlinear Dyn.* **112** 8637
[39] Wang X, Dai X, Wang Y and Wang E 2025 *Nonlinear Dynamics* **113** 7315
[40] Fan D, Zhang X, Kang W, Zhao H and Lv Y 2022 *Sensors* **22** 4752
[41] Dong Y, Yan R and Yin C 2024 *Scientific Reports* **14** 24735
[42] Chen H, Liu Z, Tanougast C, Liu F and Blondel W 2021 *Optics and Lasers in Engineering* **137** 106375
[43] Xian Y, Wang X, Yan X, Li Q and Wang X 2020 *Optics and Lasers in Engineering* **134** 106202
[44] Alkhonaini M A, Gemeay E, Zeki Mahmood F M, Ayari M, Alenizi F A and Lee S 2024 *Scientific reports* **14** 16701
[45] Cai C, Cao Y, Jahanshahi H, Mou J and Sun B 2024 *Journal of the Franklin Institute* **361** 106874
[46] Thakor V A, Razzaque M A and Khandaker M R 2021 *IEEE access* **9** 28177
[47] Wei D, Jiang M and Deng Y 2023 *Expert Systems with Applications* **213** 119074
[48] Wang X and Liu H 2022 *Chaos, Solitons & Fractals* **164** 112586
[49] Liang Q and Zhu C 2023 *Optics & Laser Technology* **160** 109033
[50] Lai Q and Zhang H 2023 *Optics & Laser Technology* **166** 109626
[51] Melendez-Melendez G and Cumplido R 2022 *Engineering Science and Technology, an International Journal* **34** 101080
[52] Qu G, Meng X, Yang X, Wu H, Wang P, He W and Chen H 2021 *Optics and Lasers in Engineering* **137** 106376
[53] Yuan Y, Liu Y, Guo J, Han Y and Wang X 2023 *Optik* **295** 171509
[54] Singh D, Udmale S S and Singh S K 2023 *Journal of Ambient Intelligence and Humanized Computing* **14** 4841
[55] Liu Y, Jiang Z, Xu X, Zhang F and Xu J 2020 *Optics & Laser Technology* **127** 106171
[56] Wang X and Liu H 2022 *Chaos, Solitons & Fractals* **164** 112586
[57] Cai C, Wang Y, Cao Y, Sun B and Mou J 2024 *Applied Intelligence* **54** 5944
[58] Gao X, Mou J, Banerjee S, Cao Y, Xiong L and Chen X 2022 *Journal of King Saud University-Computer and Information Sciences* **34** 1535