

Hybrid medical image self-embedding watermarking encryption scheme based on strong S-box

Linian Wang(王励年), Xianying Xu(徐宪莹), Suo Gao(高锁), Jun Mou(牟俊)
Citation: Chin. Phys. B. 35, 090505 (2026). DOI: 10.1088/1674-1056/ae1c2e |
CSTR: 32038.14.CPB.ae1c2e
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

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), Jun Mou(牟俊)
Chin. Phys. B. 35, 080502 (2026). DOI: 10.1088/1674-1056/ae15f8 | CSTR: 32038.14.CPB.ae15f8

Hybrid computational analysis of fractional optical soliton structures in a dispersive Schrödinger model with applications in nonlinear optics

Mati ur Rahman, Sonia Akram, Laila A. AL-Essa
Chin. Phys. B. 35, 070503 (2026). DOI: 10.1088/1674-1056/ae5808 | CSTR: 32038.14.CPB.ae5808

Thermodynamic and real-time dynamic properties of complex Sachdev–Ye–Kitaev model

Sizheng Cao(曹思政), Xian-Hui Ge(葛先辉), Yi-Cheng Rui(芮易成)
Chin. Phys. B. 35, 060512 (2026). DOI: 10.1088/1674-1056/ae48c6 | CSTR: 32038.14.CPB.ae48c6

Color image encryption algorithm using a new four-dimensional hyperchaotic system

Bo Lin(林博), Min Liu(刘敏), Guodong Ye(叶国栋)
Chin. Phys. B. 35, 050502 (2026). DOI: 10.1088/1674-1056/ae0bff | CSTR: 32038.14.CPB.ae0bff

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, Yinghong Cao(曹颖鸿)
Chin. Phys. B. 33, 020503 (2024). DOI: 10.1088/1674-1056/ad0775

Hybrid medical image self-embedding watermarking encryption scheme based on strong S-box

Linian Wang(王励年), Xianying Xu(徐宪莹)†, Suo Gao(高锁), and Jun Mou(牟俊)

School of Information Science and Engineering, Dalian Polytechnic University, Dalian 116034, *China*

(Received 15 August 2025; revised manuscript received 31 October 2025; accepted manuscript online 6 November 2025)

As a newly emerging pillar industry in the medical field, telemedicine relies on the Internet and other transmission networks to complete the transmission of patient information and obtain the consultation results of telemedicine experts, which greatly improves the guarantee of patients' lives. At the same time, the secure transmission of medical data is also one of the important standards of telemedicine, because any attack or theft caused by the loss of small details, changes, or information leakage will affect the direction of treatment, resulting in serious consequences. Therefore, a new digital watermarking scheme for medical images is proposed in this paper, which combines image encryption and watermarking protection techniques. In the watermarking aspect, the Canny operator is used to obtain the self-embedding watermark image that is highly related to the plaintext, and the watermark embedding is realized by non-subsampled contourlet transform, discrete wavelet transform, Fourier transform, and other operations. An efficient S-box is constructed by using the generated chaotic sequence and the improved Z-transform, which fully disrupts the arrangement position of image pixels, and uses two-way diffusion to complete the distribution of plaintext information in ciphertext to realize image encryption. Simulation results and related tests show that the algorithm can successfully encrypt color and grayscale medical images and has good robustness and ability to resist various external attacks.

Keywords: medical image encryption, S-box, self-embedding watermark, canny operator, NSCT transform

PACS: 05.45.–a, 05.45.Gg

DOI: 10.1088/1674-1056/ae1c2e **CSTR:** 32038.14.CPB.ae1c2e

1. Introduction

The revolution and innovation in the field of communication have driven the rapid development of a large number of industries. Multimedia applications and digital image communication have been deeply cultivated in more fields, and services such as telemedicine, e-commerce, and e-banking have emerged one after another.[1] As an important reference material to assist doctors in the treatment of patients, medical images provide reference treatment direction by giving doctors feedback on the shape, size, location, and other information of various organs in the patient's body.[2–5] Around the world, there are many medical institutions that collect and record pathological information of different patients, and gradually improve treatment methods and plans by accumulating information.[6] For these medical images with important therapeutic applications, it is important to ensure that they are protected from various external attacks on the Internet or the hospital's internal network and achieve secure transmission.[7–11]

Cryptography,[12,13] information steganography,[14] watermarking,[15] and computer technology are some of the main forces to protect information and can provide good security for image information transmission. As a nonlinear system that meets the requirements of cryptography, chaos theory has a series of advantages, such as initial value sensitivity, unpredictability, randomness, etc.[16–19] Many image encryption schemes have been proposed based on its rich cryptographic characteristics.[20–24] For example, Xian *et al.* proposed a fractal sorting moment to complete image encryption by combining this matrix with a global diffusion method based on two chaotic sequences.[25] Lin *et al.* studied and proposed a brain-like initial enhancement coexisting hyperchaos based on coupled neural networks and an encryption scheme for biomedical images.[26] Zhang *et al.* proposed a scheme based on improved large-scale interval chaotic mapping and dynamic DNA coding, which is competitive in terms of security.[27]

As an important structural component of the AES cryptosystem, the S-box provides the source of the nonlinear part of the system, and people gradually realize the important role of the AES encryption algorithm.[28–32] At the same time, as a representative in the field of symmetric cryptographic keys, building an S-box with high encryption performance to protect image information is also a frontier research field. Academics have been working to come up with more efficient solutions.[33–36] For example, Khan proposed a multi-S-box algorithm based on chaos theory.[37] Zheng *et al.* used a dynamic S-box encryption algorithm dependent on double chaotic mapping.[38] Hussian *et al.* used a multi-S-box encryption algorithm dependent on Chebyshev mapping.[39] Finally, Liu *et al.* used three-dimensional chaotic mapping to

†Corresponding author. E-mail: xuxiany@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.

construct a dynamic S-box image encryption algorithm.[40]

For most application S-box schemes, building multi-S-box and dynamic S-box has always been the first choice of design schemes, which requires a lot of time and cost, and cannot give absolute assurance of security performance. Moreover, numerous continuous-time systems are referenced in the S-box design, which undoubtedly increases the time cost of the algorithm. Compared with a continuous system, a discrete chaotic system has faster iteration efficiency and complexity, and can provide better security support.[41] In addition, it is also considered that the single S-box structure has some shortcomings in image encryption. For example, image pixels cannot be correctly hidden for images with strong correlation and some binary images, and the histogram does not change significantly before and after encryption. To this end, the selected discrete chaotic system is used to construct the double S-box structure, and it is applied in the image encryption scheme.

As a general technology to solve copyright disputes and protect information security, digital watermarking can be classified into spatial watermarking[42,43] and frequency watermarking.[44] The former is easier to achieve, but it lacks robustness and resistance to attacks. As the first choice of watermarking technology, frequency domain watermarking mainly focuses on discrete cosine transform, discrete wavelet transform (DWT), singular value decomposition, and other operations, and realizes information protection by embedding a watermark on the decomposition coefficient of the carrier image.[45–47] In this paper, non-subsampled contourlet transform (NSCT), DWT, and Fourier transform are used to implement zero-watermark embedding in medical images. The algorithm's contributions are as follows:

1. An S-box with good performance is obtained by combining discrete chaotic sequences and an improved Z-transform design.

2. A self-embedding watermark related to the encrypted medical image through the Canny operator is obtained.

3. The scheme exhibits excellent reconstruction quality and low distortion in watermark restoration, and the PSNR test results are outstanding.

4. Simulation outcomes and performance evaluation indicate that the proposed algorithm can effectively complete image encryption and has good robustness and ability to resist various external attacks.

The rest of this paper is structured as follows. Section 2 describes the theory related to the algorithm. Section 3 describes the construction process of the S-box and the process of digital watermark encryption. In Section 4, the simulation outcomes and performance evaluation of the algorithm are given. Section 5 is the conclusion of the paper.

2. Correlation theory

2.1. Discrete hyperchaotic mapping

Considering that discrete mapping can provide better time efficiency and complexity compared with continuous mapping, and the hyperchaotic system has better performance in randomness and complexity compared with the chaotic system, and can provide more secure and effective support for image encryption, this system is selected. The equation of state of the system is as follows, and the relevant dynamic characteristics are verified from the aspects of the phase diagram, LES index, bifurcation diagram, etc.[48]

$$\begin{cases} x_{n+1} = x_n + a\sin(y_n) - k\tanh({z_n}^2)x_n, \\ y_{n+1} = bx_n + c, \\ z_{n+1} = z_n + dx_n. \end{cases} \tag{1}$$

Parameters a and b in the equation are used to verify the characteristics of the system's dynamics. For parameter a, with $k = 1$, $b = 1.25$, $c = 1$, $d = 1$ and the initial conditions being $(x_0, y_0, z_0) = (1, 1, 1)$, the parameter range [1, 3.5] is selected. The bifurcation diagram of parameter a and the test results of LES are presented in Fig. 1. Moreover, from the obtained results, it can be observed that the transformation trends of the bifurcation diagram and LES within the interval are consistent, and as the value of a increases, period-doubling bifurcation and chaotic states successively appear. In a specific interval, the system achieves a super-chaotic state, and the attractor of the super-chaotic state is also presented in Fig. 1. For parameter b, given $a = 3$, $k = 0.7$, $c = 1$, $d = 1$, the initial values are $(x_0, y_0, z_0) = (1, 1, 1)$, and the value range is [1, 3]. The bifurcation diagram and LES of the parameters are shown in Fig. 2.

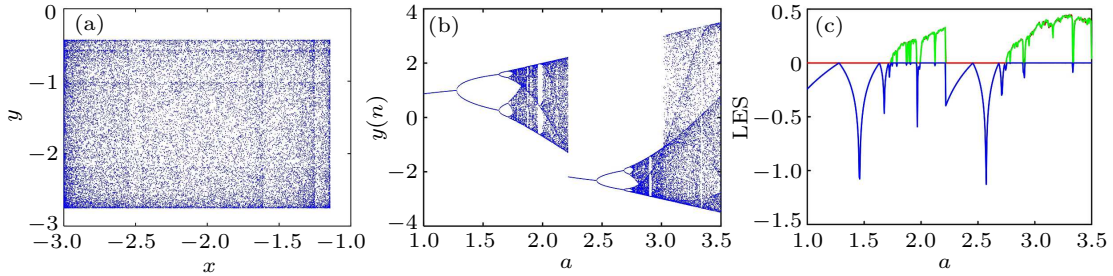


Fig. 1. Verification of dynamic characteristics of parameter a. (a) Phase diagram, (b) bifurcation diagram, (c) LES.

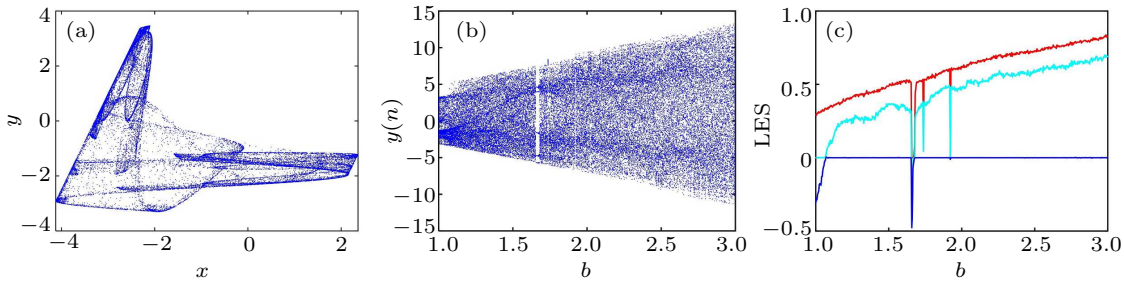


Fig. 2. Verification of dynamic characteristics of parameter b. (a) Phase diagram, (b) bifurcation diagram, (c) LES.

Through the systematic dynamic analysis of parameters a and b, it can be observed that the selected system exhibits rich dynamic characteristics and is suitable for the research of medical image encryption.

2.2. Image edge detection

Image edge detection, as an effective means to extract image feature information, can realize the feedback of the information to be transmitted with less data to a certain extent, and save the transmission time. In the medical field, doctors often scan human organs by laser and other means, and treat patients by obtaining contour, position, and other information, and there is a common relationship between the two. The Canny operator, as the best step edge detection operator, has some advantages, such as high recognition precision, accurate real location, and good anti-noise performance. Through edge detection and extraction of the encrypted medical image, the self-embedding watermark image highly related to the original image is obtained, which effectively enhances the robustness and saves the amount of transmitted data compared with embedding the patient's signature and personal textual information into the watermark. The results of a comparison of extraction with other operators are shown in Fig. 3.

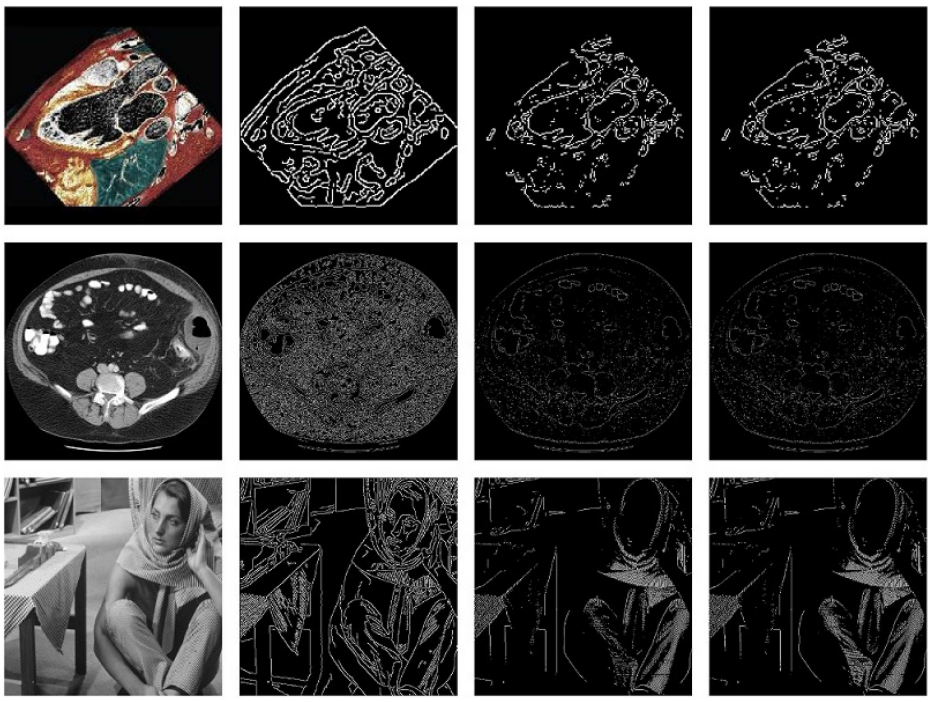


Fig. 3. Comparison of edge feature information extraction results of different operators. (a) Plaintext image, (b) Canny operator, (c) Prewitt operator, (d) Sobel operator.

2.3. NSCT transformation

NSCT transform is a kind of contour wave transform with superior performance, which consists of a nonsubsampled pyramid (NSP) filter and a nonsubsampled directional filter bank (NSDFB). Compared with wavelet transform and CT transform, it can capture the singular information in the image more effectively, and obtain abundant directional information images and multi-scale information images, with good translation invariance. The image is transformed by NSCT, and the low-pass sub-image and band-pass sub-image are decomposed by NSP at first. Further decomposition is implemented on the low-pass sub-image, while the high-frequency components in

different directions can be obtained by NSDFB decomposition of the band-pass sub-image, and more accurate direction information can be obtained. It is worth noting that considering the incompleteness of multi-scale decomposition, the background image obtained in the low-frequency part will contain some details of the original image, especially in the case of fewer decomposition layers. Therefore, when embedding the obtained watermark image, the plaintext is decomposed at three levels to reduce the display of more specific details. At the same time, DWT transform and Fourier transform are combined to achieve frequency domain watermark embedding. An example of the breakdown is shown in Fig. 4.

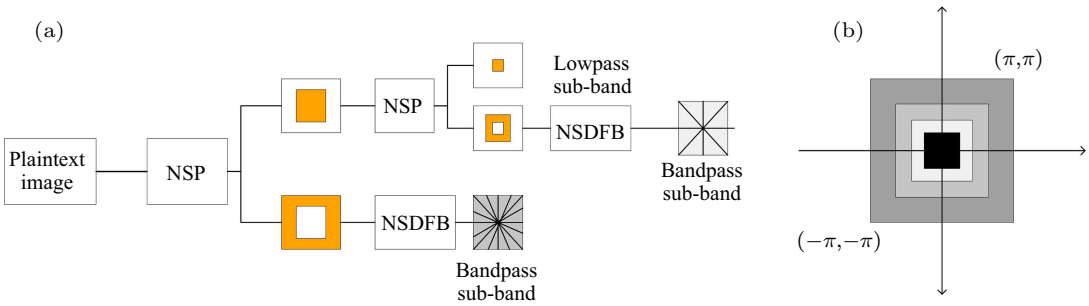


Fig. 4. (a) Decomposition structure diagram, (b) frequency domain decomposition structure diagram.

3. Encryption scheme

3.1. S-box building

This section gives the specific S-box generation process, combined with the generated random number sequence and Z-transformation to obtain the final required S-box. The S-box is applied to the proposed encryption algorithm, and the details of the generation are given. Relevant examples are given in Table 1.

Table 1. S-box generation example.

S-box	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	60	242	192	71	127	81	201	202	162	79	11	54	245	17	187	85
2	251	227	83	45	247	160	254	174	234	183	105	171	94	219	23	175
3	196	106	252	113	122	53	116	230	115	72	223	182	146	156	241	181
4	184	173	138	21	109	13	197	108	3	135	253	91	33	112	111	250
5	82	25	7	78	133	56	149	76	100	168	39	235	233	163	218	62
6	129	19	232	155	154	203	9	57	186	41	191	59	208	52	120	69
7	134	128	228	151	157	222	90	178	169	12	255	30	220	2	166	27
8	121	42	114	110	75	32	92	172	10	142	14	0	67	51	80	249
9	188	244	118	50	215	214	200	236	22	29	147	176	40	136	66	131
10	64	224	4	43	164	5	237	207	95	209	240	210	117	35	65	130
11	226	88	204	77	229	55	87	177	239	58	185	205	61	217	49	246
12	101	159	70	199	216	167	180	103	221	63	132	107	145	8	193	24
13	194	126	248	139	143	28	195	37	165	231	99	73	125	211	104	213
14	68	119	34	47	153	20	170	98	150	225	190	38	124	36	96	212
15	123	86	141	152	140	16	158	1	189	148	238	97	206	31	44	48
16	137	243	198	144	26	84	179	161	18	46	6	89	74	15	93	102

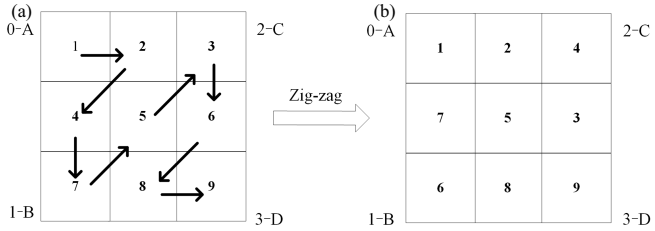


Fig. 5. Taking a 3×3 matrix as an example, the zig-zag transformation is completed. (a) Original matrix. (b) Transformed matrix.

Step 1: By entering the desired conditions of the system, three different chaotic sequences of X, Y, and Z are obtained.

Step 2: For the generated random numbers of the three sequences, keep four decimal places, multiply by 10^4 and perform modular operations on 256 to obtain the random number sequences X_1, Y_1, and Z_1 between [0,255].

Step 3: Select the subsequences of length 128 in the sequences X_1 and Y_1 to form matrix Q.

Step 4: Check whether the elements of the matrix are repeated, remove the repeated elements, and obtain the next digit in the corresponding sequence to ensure that the elements in the generated matrix Q appear only once.

Step 5: Record the four diagonal positions of matrix Q as A, B, C, and D. Averaging the random numbers in the se-

quence Z_1 and modulo 4, the result is the specific position where the Z transformation begins (0–A, 1–B, 2–C, 3–D).

Step 6: The matrix obtained through the operation of Step 5 is denoted as Q_1, which is the generated S-box.

3.2. S-box performance analysis

In order to better reflect the strong cryptography of the designed S-box, and prove that it can be applied in the field of image encryption, a comparison of the S-box's strong cryptographic features is indicated in Table 2. The nonlinear criterion, strict avalanche criterion (SAC), bit independence criterion (BIC), and differential approximate probability (DAP) are selected for evaluation. By comparative analysis, it seems that the designed S-box has good cryptographic characteristics and can be used in image encryption.

Table 2. A performance comparison of the designed S-box.

S-box	Nonlinearity Min Ave Max	BIC–SAC	BIC-nonlinearity	SAC Min Max	DAP
Proposed	105 107.1 110	0.503	103.4	0.4688 0.5941	12
Ref. [49]	100 105 108	0.5038	103.00	0.3906 0.6719	12
Ref. [50]	102 104.75 106	0.5017	103.00	0.3906 0.5938	12
Ref. [51]	102 104.25 108	0.5045	103.07	0.4219 0.6016	12
Ref. [52]	96 103.25 106	0.4864	103.07	0.3906 0.6719	44
Ref. [53]	104 106 108	0.4976	103.85	0.3906 0.5937	12
Ref. [54]	102 104 106	0.5019	103.5	0.4825 0.5175	10
Ref. [55]	84 100 106	0.4962	101.9	0.3712 0.6256	16

3.3. Digital watermarking encryption scheme

In order to ensure the safe transmission of medical images in modern communication networks such as the Internet, this paper proposes a new digital image watermarking encryption scheme for mixed encryption of color medical images and gray medical images. By embedding watermark information into carrier medical images, it can effectively avoid information copyright disputes, theft, and other problems. The S-box structure with strong cryptographic characteristics and two-way diffusion technology is used to encrypt and protect the transmitted medical images to the greatest extent to protect the safety of the patients. The specific operation details and solution flow chart follow.

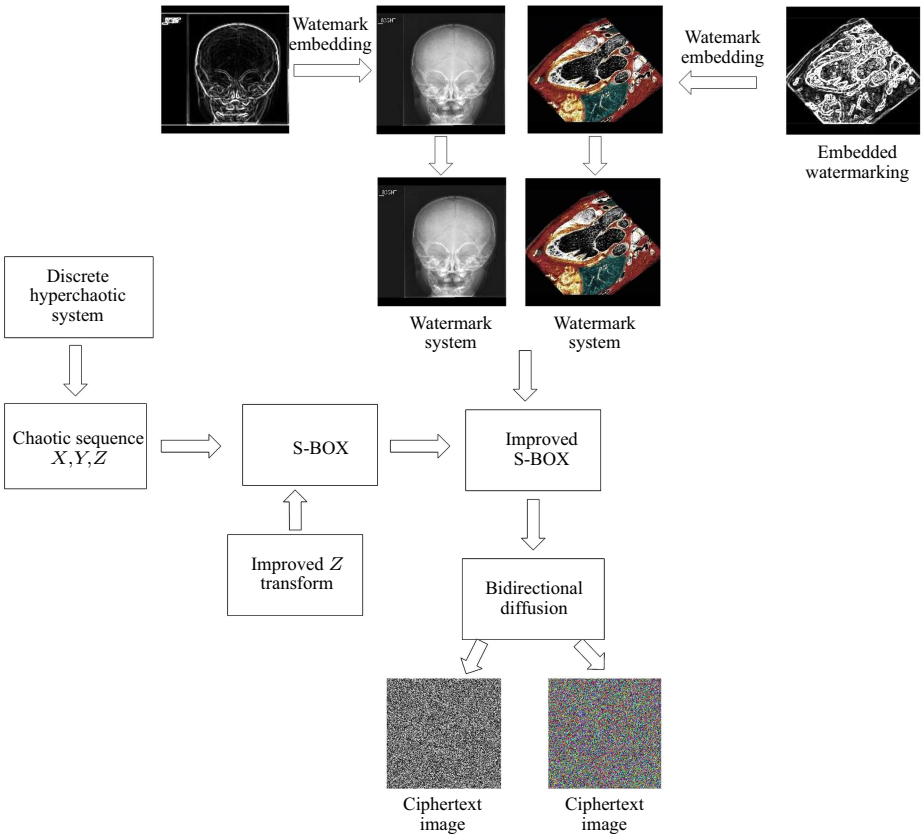


Fig. 6. Flowchart of the watermarking encryption scheme.

3.3.1. Digital watermark embedding

As a kind of watermarking with good robustness and anti-attack performance, frequency domain watermarking has been favored. In this paper, we first apply the image edge feature extraction method to obtain the self-embedding watermark. Combining NSCT, DWT, and Fourier transform, the watermark embedding in the frequency domain is realized. It is proven that a combination of the above methods can effectively ensure the invisibility and robustness of the watermark, and the effect is good. The specific implementation is as follows:

Step 1: Read the carrier medical image, denoted as P. P can be color or grayscale.

Step 2: The edge features of the carrier medical image P are extracted by the Canny operator, and the self-embedding watermark image highly related to P is obtained, denoted as W.

Step 3: The three-level NSCT transformation is carried out on image P, so that the obtained low-pass image component has fewer texture details, which is denoted as Q_3.

Step 4: The low-pass component Q_3 is transformed by DWT. The decomposed low-frequency component and the three high-frequency components are denoted as WW_1, WW_2, WW_3, and WW_4, respectively.

Step 5: The low-frequency component WW_1 is selected for Fourier decomposition transformation, and the obtained amplitude and phase are denoted as A and B, respectively.

Step 6: For the obtained self-embedding watermark image W, repeat the above operations, and the obtained amplitude and phase are denoted as A_1 and B_1.

Step 7: The phase B_1 of the watermark image multiplied by the embedding coefficient is added to the phase B of the original image. The construction of the embedding coefficient is realized by a random sequence generated by a chaotic sequence, which improves randomness.

Step 8: The new phase and the original amplitude are transformed by Fourier inversion to get the restored image. DWT inverse transformation and NSCT inverse transformation are continued to obtain the final watermark medical image, denoted as P_1.

3.3.2. S-box pixel scrambling

Using scrambling to change the position of pixels in medical images embedded with watermarks can not only hide the transmitted information but also improve the security level. The dual S-box structure is used to process the position of pixels, which effectively disrupts the distribution of original pixels. A detailed description of the implementation follows.

Step 1: Using the random number sequence X obtained by the iterative chaotic system, the index matrix is constructed, and the medical image with embedded watermark is scrambled for the first time, and the result P_2 is obtained.

Step 2: Convert the position coordinates of each pixel in P_2 to an 8-bit binary number and set (m, n).

Step 3: Set the first four digits of the 8-bit binary corresponding to m as m_1 and the last four digits as m_2, and set the first four digits of n as n_1 and the last four digits as n_2. Pixel x is searched in the first S-box according to the new coordinates (m_1, n_1). Pixel y is searched in the second S-box according to (m_2, n_2).

Step 4: Replace the positions of elements corresponding to (m,n) and (x,y) in P_2.

Step 5: Repeat the above calculation until all pixels in P_2 have been replaced and the scrambled result P_3 is obtained.

Taking a 4×4 size matrix as an example, an S-box is used to realize the change of pixel position. A 2-bit binary conversion is performed on the position coordinate (0, 0) of the first pixel value of 6 in the matrix, resulting in a new coordinate of (00, 00). Combine the first digit of x and y to get the coordinate (0, 0), in which case the corresponding position element 3 is obtained in S-box1. Combine the second digit of x and the second digit of y to get the coordinate (0, 0), and obtain the corresponding position element 2 in S-box2. By searching in the two S-boxes, the coordinate of the exchange pixel point is obtained as (3, 2), namely, pixel point 23. Repeat the above operations until all pixels have been processed.

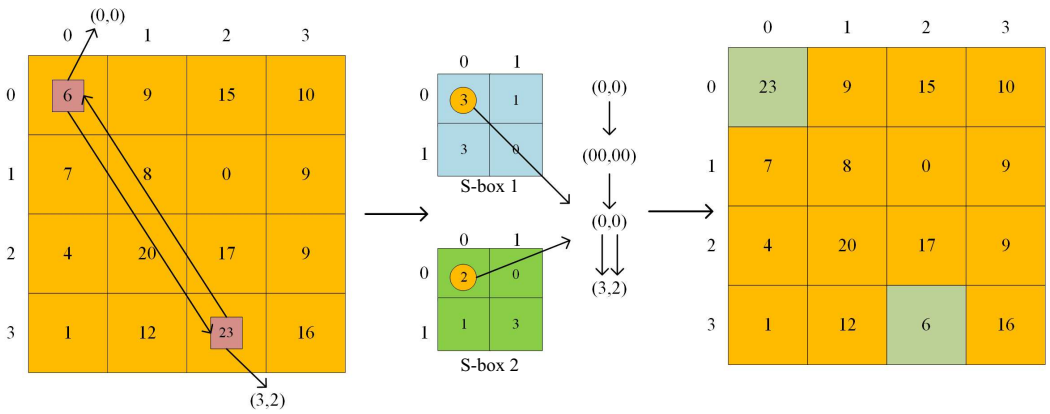


Fig. 7. Using the S-box structure to scramble image pixel positions.

3.3.3. Bilateral diffusion

Diffusion operation can hide the small changes of plaintext in the ciphertext image and can realize effective resistance to external attacks. The bidirectional diffusion method is used to further process the scrambled image. Compared with the unidirectional diffusion method, the connection between the front and back of adjacent pixels is enhanced, so that the changes caused by plaintext changes are more difficult to crack, and good performance test results are obtained. The implementation process is given, and the size of the image is denoted as $M \times N$.

Step 1: Reading scrambled image P_3. At the same time, the obtained chaotic sequence is subjected to normalization processing, resulting in the values rand1, rand2, and rand3.

$$\begin{cases} \text{rand1} = X(2999:\text{end}), \\ \text{rand2} = Y(2999:\text{end}), \\ \text{rand3} = Z(2999:\text{end}), \end{cases} \tag{2}$$

$$\begin{cases} \text{rand1} = \text{round}((\text{rand1} - \min(\text{rand1}))/(\max(\text{rand1}) - \min(\text{rand1})) \times 255), \\ \text{rand2} = \text{round}((\text{rand2} - \min(\text{rand2}))/(\max(\text{rand2}) - \min(\text{rand2})) \times 255), \\ \text{rand3} = \text{round}((\text{rand3} - \min(\text{rand3}))/(\max(\text{rand3}) - \min(\text{rand3})) \times 255). \end{cases} \tag{3}$$

Step 2: A zero matrix E of the same size is constructed, and the pixel at position (1, 1) in P_3 is brought into the formula for calculation, and the new pixel value obtained is stored in the corresponding position of matrix E.

$$E(1,1) = \text{mod}((P(1,1) + (\text{rand3}(1) + \text{rand1}(1))), 256). \tag{4}$$

Step 3: The other elements of the first row except (1, 1) are substituted into formula (2) to obtain the new element values and place them in the corresponding positions of the matrix E.

$$\begin{aligned} E(i,1) = \text{mod}((&P(i-1,1) + E(i-1,1) + (\text{rand3}((i-1) \times N \\ &+ \text{rand1}((i-1) \times N))), 256). \end{aligned} \tag{5}$$

Step 4: The elements divided by (1,1) in the first column are brought into formula 3 for calculation, and the resulting new element value is placed in the corresponding position of the matrix E.

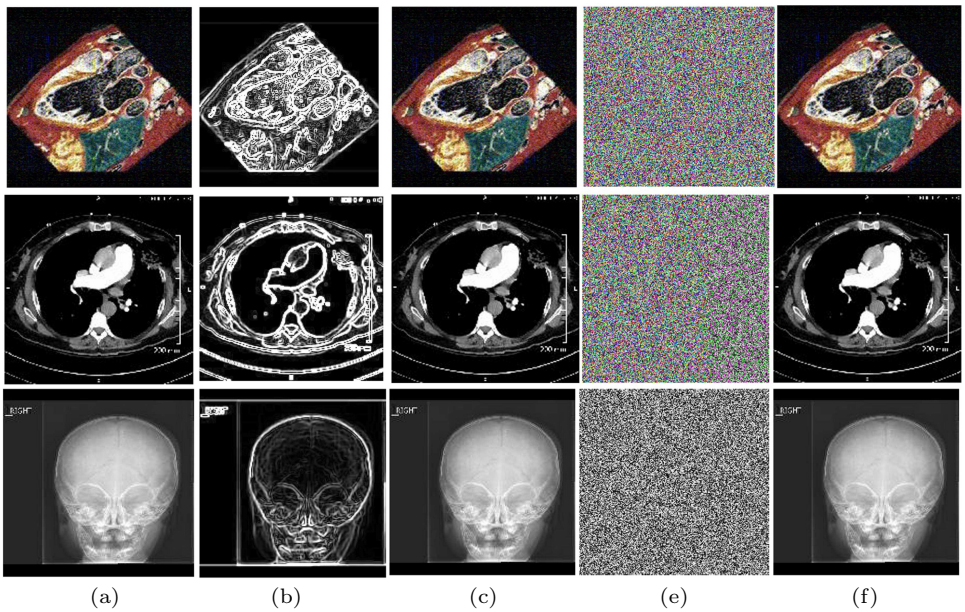
$$\begin{aligned} E(1,j) = \text{mod}((&P(1,j-1) + E(1,j-1) \\ &+ (\text{rand3}(j-1) + \text{rand1}(j-1))), 256). \end{aligned} \tag{6}$$

Step 5: The remaining pixels in the image are brought into formula 4, and the new pixels obtained are placed in the corresponding positions of matrix E. At this time, all pixels in P_3 have completed the diffusion operation.

$$\begin{aligned} E(i,j) = \text{mod}((&P(i-1,j-1) + E(i-1,j-1) \\ &+ (\text{rand3}((i-1) \times N + j - 1) \\ &+ \text{rand1}((i-1) \times N + j - 1))), 256). \end{aligned} \tag{7}$$

4. Simulation results and performance testing

To more intuitively reflect the practicability of the designed algorithm in medical image encryption and private information copyright protection, two kinds of color and gray medical images are watermarked and encrypted. The obtained



(a) (b) (c) (e) (f)

Fig. 8. Encryption results of color and grayscale medical images. (a) Carrier medical image, (b) self-embedding watermarking image, (c) watermarking image, (d) ciphertext image, (e) decryption image.

simulation results and related embedded watermarks are shown in the Fig. 8. It seems that the proposed algorithm can intuitively and effectively complete information encryption and copyright protection. Furthermore, in order to better demonstrate the generalizability of the algorithm design, the encryption and decryption effects are tested again for medical images of different sizes (i.e., 1018×1001, 180×180, and 583×1107). The results of the new test are shown in Fig. 9. It can be seen that for medical images of different sizes, the designed algorithm still has good encryption and decryption effects and the watermark is invisible.

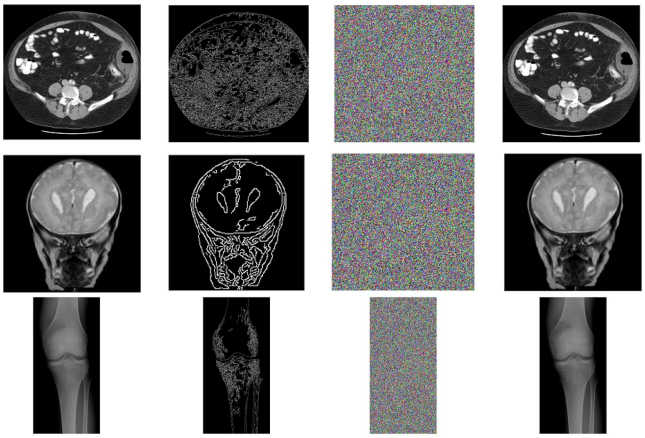


Fig. 9. Encryption and decryption results of medical images of different sizes.

4.1. Time efficiency

The encryption time represents the efficiency of the algorithm in practical application, and the faster the time, the higher the efficiency, and the greater the image value information transmitted. For medical images with practical therapeutic application value, the earlier the doctor obtains the relevant information about the patient, the more effectively the safety of the patient will be guaranteed. Further comparative analysis of time results is shown in Table 3. From the comparison results, it seems that the algorithm has high time efficiency and practical value in medical image transmission.

Table 3. Results of transmission time comparison.

Proposed	Ref. [56]	Ref. [57]	Ref. [58]	Ref. [59]
0.5241	3.3021	3.5781	0.823	1.256

4.2. Watermark extraction and reconstruction

Watermarking is the core method to maintain the copyright of information. The quality and distortion of the watermark extracted and reconstructed after a series of operations are important criteria to judge the quality of the embedded watermarking method. After the medical image is embedded and the encryption and decryption operations are completed, the embedded watermark is reconstructed and restored, and its specific PSNR value is calculated. Through visual observation and testing of the data support of PSNR value, the quality of the embedding method is proved. The obtained PSNR values are compared and shown in Table 4.

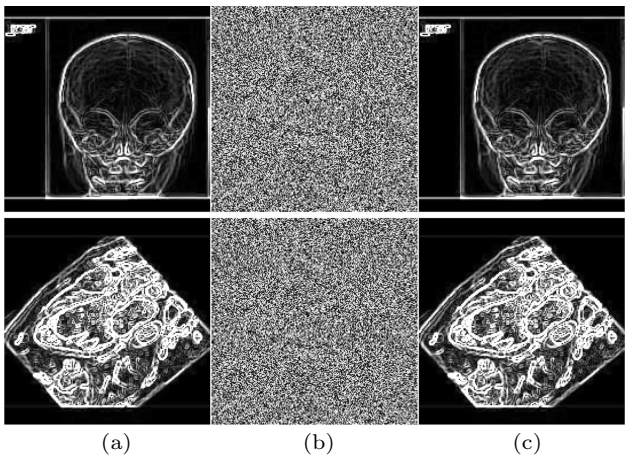


Fig. 10. (a) Embedding watermark, (b) watermark encryption, (c) watermark reconstruction.

Table 4. Testing the PSNR value.

Scheme	Proposed	Ref. [60]	Ref. [61]	Ref. [62]	Ref. [63]
PSNR(dB)	54.4	35.31	38.6088	49.0054	45.934

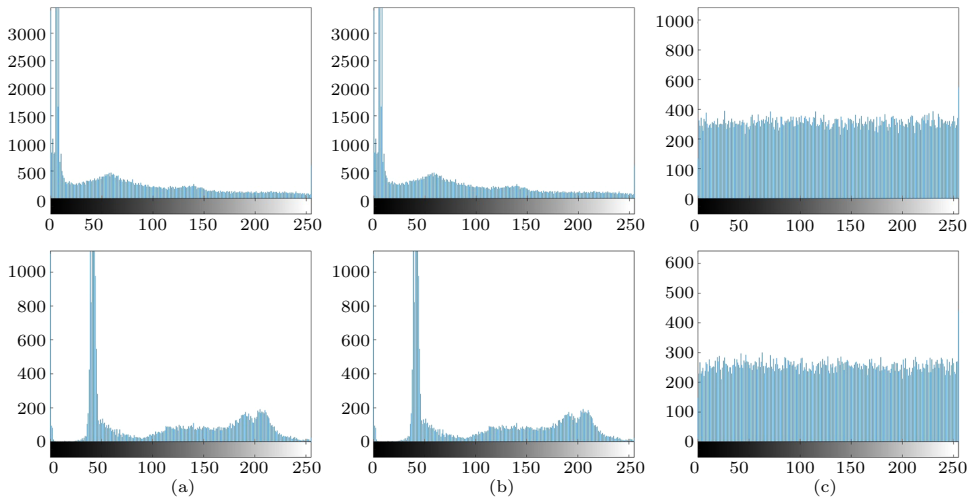


Fig. 11. Histogram test results obtained before and after encryption. (a) Plain image, (b) watermark image, (c) encrypted image.

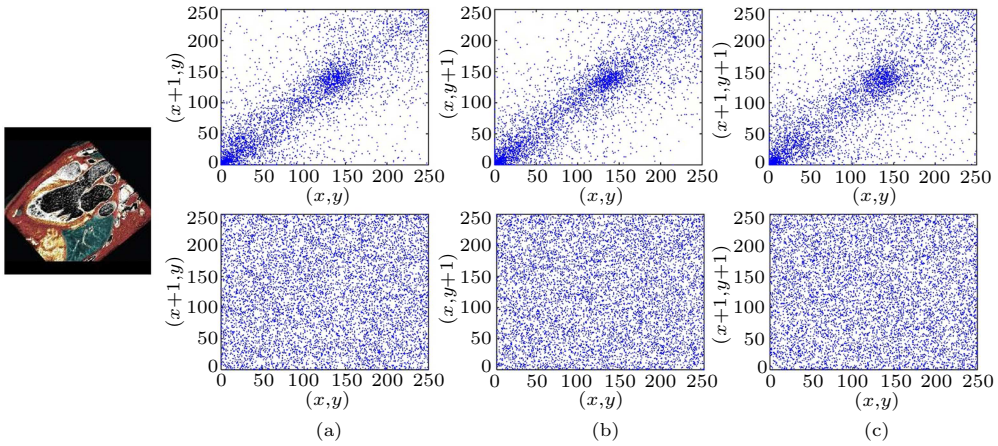


Fig. 12. Correlation comparison between adjacent pixels before and after encryption. (a) Horizontal direction, (b) vertical direction, (c) diagonal direction.

4.3. Histogram check

Histogram testing is one of the criteria to evaluate the resistance of algorithms to statistical attacks. By observing whether the distribution of each intensity pixel of plaintext before and after encryption is uniform, the performance of the algorithm is further reflected. The histograms obtained by effective encryption algorithms are highly smooth and consistent. The histogram results of the algorithm are shown in Fig. 11, which meet the relevant standards and can well resist statistical attacks.

4.4. Correlation text

Strong correlation is one of the characteristics of image information itself, and external attackers often use it as a starting point to crack the plaintext information. No matter what type of transmitted images, the harm caused by information disclosure is inestimable, especially for medical images. The loss and tampering of a patient's information will directly affect their treatment and recovery. Therefore, the proposed watermarking encryption algorithm should reduce the strong correlation between pixels to the greatest extent, so that the pixels are evenly distributed in the interval and cannot be destroyed by attackers. Color medical images are selected for verification, and the distribution of pixels before and after encryption is obtained, as shown in Fig. 12, which shows that the algorithm effectively realizes the low correlation between pixels.

4.5. Key space and key sensitivity testing

Exhaustive attack is a common method of password breaking: the password combination is cracked by conducting a lot of tests on the password. This means of attack has a great success rate for algorithms with small key space, so the proposed algorithm must have a large enough key space to avoid plaintext information breaking through exhaustive attacks. This paper selects a kind of three-dimensional discrete hyperchaos system as the carrier, with a, b, c, d, k and five parameters x_0, y_0, z_0 three initial values, respectively, to get their sensitivity to the test, the sensitivities of the 10^{-16}, 10^{-16}, 10^{-15}, 10^{-16}, 10^{-15}, 10^{-15}, 10^{-15}, 10^{-15}, the calculated total key space is about 2^{408}, which is much higher than the relevant standard requirements, so it can well resist brute force attacks such as exhaustive attacks. At the same time, after decrypting and restoring the disturbed ciphertext, the image obtained is still a noise-like image, indicating that the smallest disturbance cannot accurately decrypt the ciphertext image, showing the relevant excellent characteristics of the algorithm. Table 5 presents a comparison of relevant literature. Figure 13 presents the decryption results after perturbation of different parameters.

Table 5. Key space comparison with relevant references.

Scheme	Proposed	Ref. [64]	Ref. [65]	Ref. [66]
Total	2^{408}	2^{318}	2^{302}	2^{408}

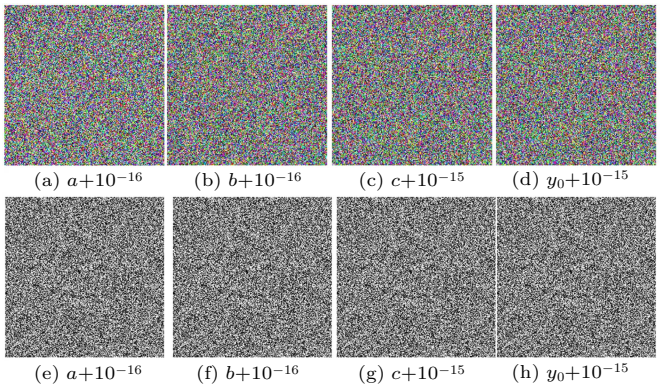


Fig. 13. Key sensitivity test for color medical images and grayscale medical images. The decryption results of the image under the perturbations of (a) $a+10^{-16}$, (b) $b+10^{-16}$, (c) $c+10^{-16}$, (d) y_0+10^{-15}.

4.6. NPCR and UACI analysis

A differential attack makes small changes to the plaintext and observes the change of ciphertext to break the cipher structure. Generally, the test results of NPCR and UACI are used to check the anti-differential attack capability of the algorithm. Both reflect the amount of pixel change and the average intensity of the overall image change, respectively. Table 6 presents

the test standards of both at the 0.05 confidence level and the test results obtained in this paper.

Table 6. NPCR and UACI test results.

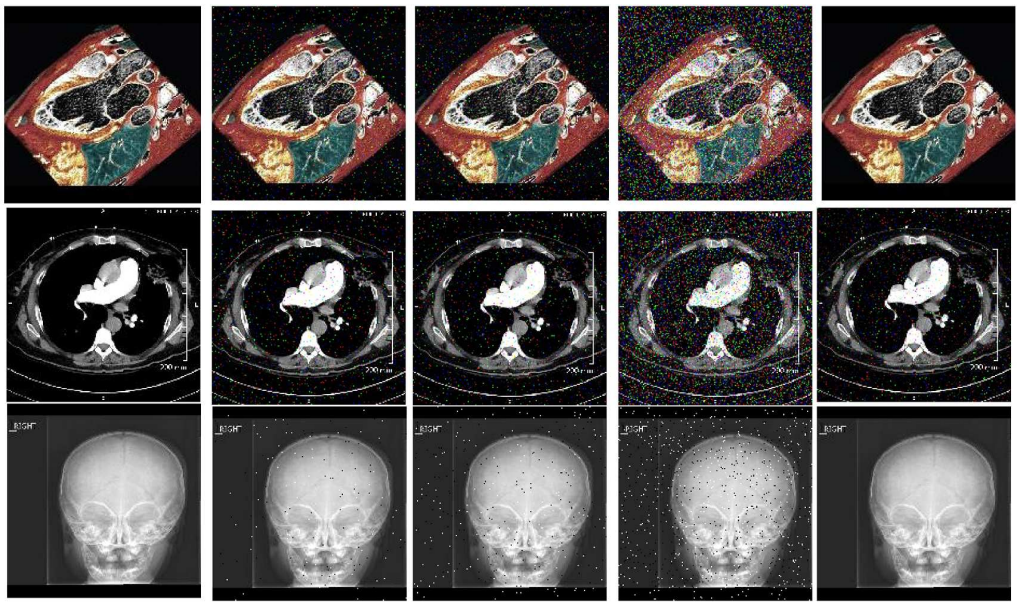
$NPCR_{0.05}$ (%)	$U_{0.05-}$,$U_{0.05+}$ (%)	NPCR (%)	UACI (%)
99.5893	(33.3730, 33.5541)	99.6014	33.4562

4.7. Information entropy

Information entropy provides a criterion for evaluating the uncertainty and invisibility of image information, which represents the expected probability of each pixel value in the image. Theoretically, the maximum value of information entropy is 8. The closer the result obtained after the algorithm test is to 8, the better the plaintext information can be hidden by the proposed algorithm. Table 7 compares the data with the literature. It can be seen that the algorithm test result is superior.

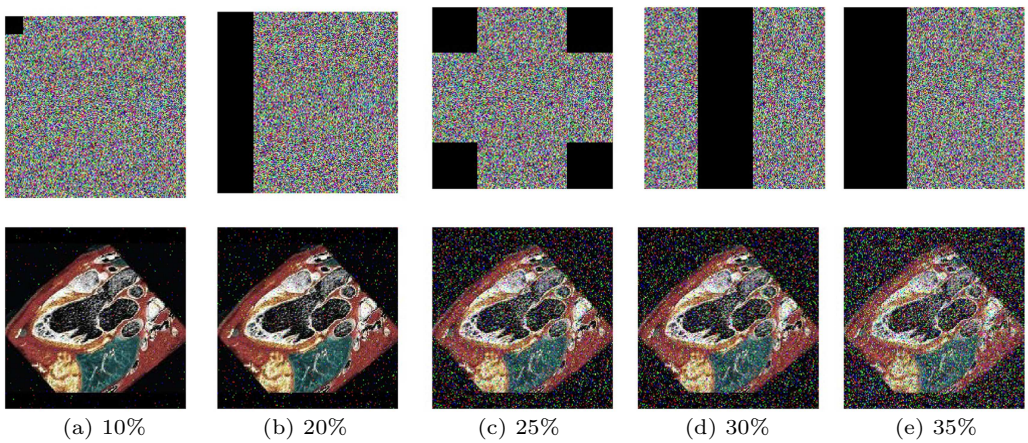
Table 7. Comparison of information entropy test results.

Proposed	Ref. [67]	Ref. [68]	Ref. [69]	Ref. [70]
7.9992	7.9979	7.9993	7.99740	7.909



(a) SPN, 0.008 (b) SPN, 0.03 (c) SPN, 0.06 (d) SPN, 0.08 (e) GN, 1×10^{-7}

Fig. 14. Different levels of salt-and-pepper noise and Gaussian noise attacks: (a) SPN: 0.008, (b) SPN: 0.03, (c) SPN: 0.06, (d) SPN: 0.08, (e) GN: 10^{-7}.



(a) 10% (b) 20% (c) 25% (d) 30% (e) 35%

Fig. 15. Resistance to reduction of shear attacks of different degrees: (a) 10%, (b) 20%, (c) 25%, (d) 30%, (e) 35%.

5. Conclusion

Medical images provide effective auxiliary materials for patient treatment, and cross-border medical treatment has become more sophisticated. As the importance of image information with special therapeutic significance has grown, it has become important to ensure its security in the transmission network. In this paper, a new self-embedding watermarking algorithm for color and grayscale medical images is proposed, which realizes the secure transmission of information by means of encryption and watermarking. In the aspect of watermarking, the self-embedding watermark, which is highly related to the encrypted medical image, is obtained by edge feature extraction. By combining NSCT transform, DWT decomposition, Fourier transform, and other technologies, wa-

termark embedding in the frequency domain is realized. In terms of encryption, the S-box structure with strong cryptographic characteristics is designed to realize the disturbance of pixel position, the plaintext information is further hidden by two-way diffusion technology to complete the diffusion operation, and the noise-like image after encryption is obtained. Simulation results show that the algorithm can achieve a good encryption effect for both color and gray medical images. The nonlinear criterion and strict avalanche criterion are tested to prove the strong cryptographic properties of the S-box. Large enough key space and high sensitivity to key changes prove that the algorithm has good resistance to external attacks, such as exhaustive attacks. The high efficiency of the transmission time ensures the reliability of the algorithm in real-time image transmission and reflects the high value of the algorithm in practical applications. The flat histogram, the low correlation of adjacent pixels, and the information entropy close to the theoretical value demonstrate the strong resistance of the algorithm to statistical attacks. The excellent results of NPCR and UACI demonstrate the superiority of the algorithm against differential attacks. In terms of robustness, the different degrees of resistance to shear and noise attacks, the extraction and reconstruction of the embedded watermark, and the PSNR test prove the feasibility of the embedded watermark method and the strong robustness of the algorithm. In summary, the proposed scheme has very high practical value and can provide theoretical support for research in related fields.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 62571079), the Basic Scientific Research Projects in the Department of Education of Liaoning Province (Grant No. LJ212410152011), the Doctoral Initiation Fund of Liaoning Province (Grant No. 2025-BS-0471), and the Research Startup Fund Project for Introducing Talents of Dalian Polytechnic University (Grant No. LJBKY2025070).

References

[1] Li C, Li Y and Yu W 2025 *Nonlinear Dyn.* **113** 3857
[2] Liu X, Song L, Liu S and Zhang Y 2021 *Sustainability* **13** 1224
[3] Fei Y, Hui S, Qiulin Y, Xinxin K, Pradip K S and Shuo C 2023 *IEEE Transactions on Network Science and Engineering* **10** 845
[4] Li B, Peng H, Luo X, Wang J, Song X, Pérez-Jiménez M J and Riscos-Núez A 2021 *International Journal of Neural Systems* **31** 2050050
[5] Hermessi H, Mourali O and Zagrouba E 2021 *Signal Processing* **183** 108036
[6] Yu F, He S and Yao W 2025 *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*
[7] Lin H, Wang C, Cui L, Sun Y, Zhang X and Yao W 2022 *Nonlinear Dyn.* **110** 841
[8] Yu F, Su D and He S 2025 *Chin. Phys. B* **34** 050502
[9] Yu F, Tan B, He T, He S, Huang Y and Cai S 2025 *Mathematics* **13** 726
[10] Li C, Zhang Y, Li H and Zhou Y 2024 *The Visual Computer* **40** 731
[11] Yu F, Musoya G Y and Rongyao G 2025 *Axioms* **14** 638
[12] Lai Q, Wan Z, Zhang H and Chen G 2022 *IEEE Transactions on Neural Networks and Learning Systems* **34** 7824
[13] Gao S, Wu R, Iu H H C, Erkan U, Cao Y and Li Q 2025 *Computer Science Review* **58** 100816
[14] Bala K R, Rajesh K N, Raajan N R, Manikandan G, Srinivasan A and Narasimhan D 2022 *Wireless Personal Communications* **127** 979
[15] Attaullah, Shah T and Jamal S S 2020 *Wireless Personal Communications* **110** 1429
[16] Gao X, Sun B and Cao Y 2023 *Chin. Phys. B* **172** 030501
[17] Hu L L, Chen M X, Wang M M and Zhou N R 2025 *Knowledge-Based Systems* 113804
[18] Cao Y, Liu Y, Wang K and Xu X 2024 *IEEE Access*
[19] Su J, Fang S and Hong Y 2024 *Chin. Phys. B* **33** 070502
[20] Wang L, Banerjee S and Cao Y 2024 *Nonlinear Dyn.* **112** 8637
[21] Gao S, Ding S, Iu H C, Erkan U, Toktas and Mou J 2025 *Chaos* **35**
[22] Cao P and Teng L 2024 *Nonlinear Dyn.* **112** 13539
[23] Han Z, Cao Y and Banerjee S 2025 *Chin. Phys. B* **34** 030503
[24] Gao S, Iu, H. H. C, Erkan, U, Simsek, C, Toktas, A and Cao Y 2025 *IEEE Transactions on Circuits and Systems for Video Technology*
[25] Xian Y and Wang X 2021 *Information Sciences* **547** 1154
[26] Lin H, Wang C, Cui L, Sun Y, Xu C and Yu F 2022 *IEEE Transactions on Industrial Informatics* **18** 8839
[27] Zhang S and Liu L 2021 *Mathematics and Computers in Simulation* **190** 723
[28] Hafsa A, Sghaier A, Malek J and Machhout M 2021 *Multimedia Tools and Applications* **80** 19769
[29] Alawida M 2024 *IEEE Transactions on Industrial Informatics* **20** 10530
[30] Gupta M and Sinha A 2021 *International Journal of Information Technology* **13** 933
[31] Parah S A, Sheikh J A, Ahad F, Loan N A and Bhat G M 2017 *Multimed Tools Applications* **76** 10599
[32] Hadj B A, Ali Pacha A and Hadj Said N 2023 *Journal of Optics* **53** 1170
[33] Zhu S, Deng X and Zhang W 2023 *Mathematics and Computers in Simulation* **207** 322
[34] Khompysh A, Kapalova N and Algazy K 2022 *Cogent Engineering* **9** 2080623
[35] Liu H, Liu J and Ma C 2023 *Multimedia Tools and Applications* **82** 23899
[36] Jun W J and Fun T S 2021 *IEEE Access* **9** 120596
[37] Khan M 2015 *Nonlinear Dyn.* **82** 527
[38] Zheng J and Zeng Q 2022 *Applied Intelligence* **52** 15703
[39] Hussain I, Anees A, Alkhaldi A H, Aslam M, Siddiqui N and Ahmed R 2019 *Optica Applicata* **49** 317
[40] Liu H, Liu J and Ma C 2023 *Multimedia Tools and Applications* **82** 23899
[41] Tong X, Liu X and Zhang M 2024 *Nonlinear Dyn.* **112** 20437
[42] Kumar S and Singh B K 2021 *Multimedia Tools and Applications* **80** 9315
[43] Cao H, Hu F and Sun Y 2020 *Optiks* **262** 169319
[44] Liu D, Su Q, Yuan Z and Zhang X 2021 *The Visual Computer* **37** 2355
[45] Li Z, Zhang H, Liu X, Wang C and Wang X 2021 *Digital Signal Processing* **115** 103062
[46] Mohammed A O, Hussein H I, Mstafa R J and Abdulazeez A M 2023 *Multimedia Tools and Applications* **82** 32855
[47] Ernawan F, Ariatmanto D and Firdaus A 2021 *IEEE Access* **9** 45474
[48] Ren L, Mou J and Banerjee S 2023 *Chaos, Solitons & Fractals* **167** 113024
[49] Liu H, Kadir A and Xu C 2020 *Applied Mathematics and Computation* **376** 125153
[50] Naseer A and Siddiqui N 2020 *International Journal of Computer Science and Information Security* **18**
[51] Liu L and Lei Z 2019 *J. Phys.: Conf. Ser.* **1303** 012090
[52] Khan M and Asghar Z 2018 *Neural computing and applications* **29** 993
[53] Cavu, Ka S, Pehlivan I and Zengin A 2017 *Chaos, Solitons Fractals* **95** 92
[54] Liu H, Kadir A and Niu Y 2014 *AEU-international Journal of Electronics and Communications* **68** 676
[55] Khan M, Shah T and Batool S I 2016 *Neural Computing and Applications* **27** 677
[56] Shaffque A, Ahmed J and Rehman M U 2021 *IEEE Access* **9** 59108

[57] Hussain I, Anees A, Aslam M, Ahmed R and Siddiqui N 2018 *Euro. Phys. J. Plus* **133** 167
[58] Zahid A H and Arshad M J 2019 *Symmetry* **11** 437
[59] Balajee M K and Gnanasekar J M 2016 *TEM Journal* **5** 67
[60] Priya S and Santhi B 2021 *Mobile Networks And Applications* **26** 2501
[61] Thakur S, Singh A K and Ghrera S P 2020 *Multimedia Tools and Applications* **79** 4263
[62] Balasamy K and Ramakrishnan S 2019 *Cluster Computing* **22** 4431
[63] Soualmi A, Alti A and Laouamer L 2018 *Arabian Journal for Science and Engineering* **43** 7893
[64] Zhang Z, Mou J and Banerjee S 2024 *Chin. Phys. B* **33** 020503
[65] Cui M, Zhang C, Chen Y, Zhang Z, Wu T and Wen H 2021 *IEEE Access* **9** 18052
[66] Ma J Z,Yang Y G and Jiang D H 2024 *Physica Scripta* **99** 125263
[67] Liu H, Zhao B and Huang L 2019 *Entropy* **21** 343
[68] Liu J, Tang S, Lian J, Ma Y and Zhang X 2019 *Multidimensional Systems And Signal Processing* **30** 1637
[69] Kumar S, Panna B and Jha R K 2019 *Medical Biological Engineering Computing* **57** 2517
[70] Chai X, Gan Z, Yuan K, Chen Y and Liu X 2019 *Neural Computing and Applications* **31** 219