Nonlinear Dyn (2024) 112:13571–13597
https://doi.org/10.1007/s11071-024-09732-3

ORIGINAL PAPER

Dynamic rotation medical image encryption scheme based on improved Lorenz chaos

Zhenlong Man · Chang Gao · Yu Dai · Xiangfu Meng

Received: 11 September 2023 / Accepted: 5 May 2024 / Published online: 4 June 2024

Abstract With the rapid development of AI technology and the continuous improvement of Internet technology, information technology and intelligent technology are gradually combined with medical treatment, which has given rise to the rapid rise of digital medical industry, and smart medical alliance has gradually become a hot topic in the medical field. The data and systems in medical institutions are frequently attacked by network due to their high value and vulnerability. A large number of network security attacks may damage medical services and affect patient safety. A dynamic rotation medical image encryption scheme based on improved Lorenz chaos is proposed for solving the security problems such as theft and tampering faced by digital medical images in Internet transmission. Firstly, in order to improve the key randomness and security of image encryption, we improved the classical Lorenz chaotic system. By adding new nonlinear adjustment terms and control parameters, the generated pseudo-random numbers are more unpredictable. From 0–1 test analysis, Lyapunov exponent and different analysis results, it can be seen that the improved Lorenz chaotic system has a wider range of chaotic parameters and better chaotic characteristics. We use the improved chaotic system as a key generator and apply it to the proposed image encryption scheme with dynamic rotation permutation and double diffusion. Under the premise of two kinds of scrambling modes within a block and between blocks, a pixel exchange threshold is innovatively designed to judge the feasibility and effectiveness of the exchange of pre-exchange pixels. The diffusion algorithm uses a relatively novel filter diffusion method to diffuse the scrambled image, and then uses a dynamic diffusion method to further improve the security of the ciphertext image. Through the analysis of the experimental results of a number of security tests, it can be seen that the proposed scheme is more effective in image encryption, and can effectively resist common attacks.

Keywords Block image encryption · Improved Lorenz chaotic system · Dynamic rotation scrambling · Filter diffusion

Z. Man (✉) · C. Gao · Y. Dai · X. Meng
School of Electronic and Information Engineering,
Liaoning Technical University, Liaoning 125105, China
e-mail: manzhenlong@lntu.edu.cn

Z. Man · X. Meng
Liaoning Key Laboratory of Radio Frequency and Big
Data for Intelligent Applications, Liaoning, China

1 Introduction

In modern hospitals, digital medical images play an increasingly important role in the diagnosis and treatment of diseases, so they have received more and more attention [1]. In general, these medical images may involve a lot of privacy of patients, and some are very confidential and sensitive. If these private images are stolen, viewed or used by unauthorized access, catastrophic accidents can occur [2]. For example, hackers or database administrators could use unauthorized images for their personal gain, medical marketing, and fraudulent insurance claims, which could lead to life-threatening risks. Medical data security is related to important and sensitive areas such as patient privacy and technology research and development. Once data leakage occurs, it will have a serious impact on patient groups, social stability and even national security. Therefore, the security protection and governance of medical data is very important [3]. This has also attracted widespread attention of researchers.

So far, scholars have proposed many effective methods for protecting medical images with high security levels. Among them, encryption technology is the most intuitive and effective method to convert images into unrecognizable images [4]. After the encrypted image, the original image can only be restored with the correct key. In 2018, Liu et al. [5] proposed a new simple chaotic system to encrypt images, using hyperbolic sine as its nonlinearity. Test results show that the encryption method can effectively encrypt images within a single round. In 2018, Jan Sher Khan et al. [6] proposed a DNA sequence-based medical image encryption scheme to protect medical image data from unauthorized access. First, for a given DNA sequence value, the hash value is calculated by SHA-512. The hash value is given as the secret key of the interleaved logical map. Through chaotic sequences, correlations between pixels are reduced using a shuffling process. The scrambled image is XOR with the diffuse chaotic random value. Compared with the traditional image encryption scheme, this scheme has more advantages. In 2019, Arunkumar et al. [7] proposed a robust image steganography method, which combines Redundant integer wavelet transform (RI-WT), discrete wavelet transform and Singular value decomposition (SVD) and Logistic chaotic mapping. In 2020, Zhou et al. [8] proposed a non-destructive medical image encryption scheme based on game theory Region of interest (ROI) parameter optimization and ROI position hiding. It realizes lossless encryption and decryption of images, and can flexibly and reliably protect medical images of different types and structures from various attacks. In 2020, Benssalah et al. [9] proposed a new medical image encryption scheme, The scheme combines Elliptic curve cryptography (ECC), Classical hill cipher, Arnold cat map (ACM) and Linear congruence generator (LCG). Introducing Confusion and Diffusion Properties on Encrypted Medical Images via Arnold Cat Mapping and LCG. The proposed encryption scheme is robust against various attacks and provides better security properties compared to state-of-the-art techniques. In 2020, Boussif et al. [10] proposed a novel encryption method. First divide the original image into blocks, then use the Virginia cipher algorithm to encrypt the image block by block, and then use the Arnold transformation to modify the key to protect the DICOM image. In 2021, Sondes Ajili et al. [11] used chaos-based AES algorithm to encrypt watermarked medical images, and experimental results demonstrated the robustness of the proposed scheme against various types of attacks. In 2021, Kamal et al. [12] proposed a new encryption algorithm for encrypting gray and color medical images. This algorithm introduces a new image segmentation technique based on image blocks. The image blocks are scrambled using a zigzag pattern, rotation, and random arrangement, and finally a Logistic chaotic map is used to generate a key to diffuse the scrambled image. In 2022, EI-Shafai et al. [13] proposed a method based on 3D chaos Mapped robust cryptosystem for secure Internet of medical things (IOMT) and medical image encryption in cloud services. Although various encryption schemes have been proposed for securing medical images, some of them still exist Defects in different aspects. With the improvement of computer computing power and the development of cryptanalysis theory, some developed encryption schemes have the risk of being cracked. Due to its unpredictable and ergodic nature, chaos theory is widely used to develop image encryption schemes to protect medical images.

The design of the encryption algorithm is important, but the key with high security and strong randomness plays a vital role. The keys used in the existing image encryption algorithms are all generated by chaotic systems. Chaotic system is a kind of nonlinear dynamical system, because its behavior exhibits extremely sensitive characteristics dependent on initial conditions, so it is very suitable as a key generator in image encryption algorithms. In recent years, many image encryption algorithms based on chaotic systems have been proposed: In 2021, Man et al. [14] proposed to use a five-dimensional conservative hyperchaotic system as the key generator to ensure the randomness of the key. This hyperchaotic system has a larger LE index value, which can guarantee ultra-high chaotic characteristics. In 2021, Sun et al. [15] studied a multi-image encryption scheme based on cascaded gyrator transform and high-dimensional chaos in order to increase the amount of encrypted data and improve transmission efficiency. The adoption of high-dimensional chaos and Kronecker product further ensures the security of the cryptosystem. In 2021, ul Haq et al. [16] constructed a 4D hybrid chaos map with hyperchaotic properties and high randomness behavior using 1D sinograms and 2D Thinker bell diagrams. Furthermore, a new image encryption scheme is introduced to explore the application of the proposed chaotic system. For images of size 256 × 256, the key size is increased by a factor of $(8!)^{65536}$, resulting in a strong cryptographic structure against well-known attacks. In 2023, A. Chamoli [17] proposed an optimal encryption method for color images based on 3D Chaotic Baker mapping diffusion model technology. The advantage is that it makes the model intrinsically sensitive to changing any pixel value or key. The efficiency of the algorithm depends on the experimental results. The newly proposed encryption model has built-in features of random binary sequences for the process of encrypting plaintext images into passwords. In 2023, Wang et al. [18] proposed a color image encryption algorithm, which uses double-layer Joseph scrambling, XOR diffusion, and is built on a laser chaotic system. The program first chooses the laser chaotic system because of its advantages of extended bandwidth and fast propagation speed. Simulation performance results show that the newly proposed method is practical.

But some chaos-based cryptosystems have been proven to have lower security levels due to the performance limitations of the chaotic systems used. Therefore, many scholars are committed to improving various chaotic systems: In 2020, Yin et al. [19] proposed a new algorithm for medical image encryption combining genetic simulated annealing particle swarm optimization and an improved quantum chaotic system for better security performance. First, a key stream is generated using a modified quantum chaotic system. Then the plaintext image is processed by the selection and crossover operations of the genetic algorithm. Then the simulated annealing algorithm, Particle swarm optimization (PSO) algorithm and optimized PSO algorithm are used. Through the above operations, the histogram of the scrambled image can be balanced to resist statistical attacks. Experimental results and performance analysis show that the encryption system proposed in this paper can resist many typical attacks, and has high security and encryption efficiency. In 2022, Lai et al. [20] constructed a new non-equilibrium chaotic system by introducing additional variables and constant terms into the three-dimensional chaotic system. Unlike previous nonequilibrium chaotic systems, the new system has period-doubling bifurcations and has the property of enforcing hidden chaotic attractors for large constant terms. Its security is analyzed from the aspects of computational complexity, statistical properties and the ability to resist several common attacks. Compared with several advanced algorithms, CMCT-IEA exhibits excellent security properties. In 2022, Hu et al. [21] proposed a crossed two-dimensional chaotic map that combines a sinusoidal chaotic system with a Logistic chaotic system. Compared with the traditional sinusoidal and Logistic chaotic systems, the new chaotic system has a hyperchaotic state. And the improved chaotic map is applied to the designed quantum image encryption algorithm, and the effectiveness of the improved chaotic system is proved through experimental simulation and security analysis.

Although improving the chaotic system can indeed improve the chaotic characteristics of the original chaotic system, most of the existing improvement methods are to improve the low-dimensional chaotic system or combine two or more low-dimensional chaotic systems. For the appeal problem, we will start with the high-dimensional chaotic system, and use the Lorenz chaotic system as the original chaotic system. By adding new nonlinear adjustment items and control parameters, the pseudo-random numbers generated by it will be more unpredictable. And through a series of chaotic analysis, it is proved that the sequence distribution generated by the improved Lorenz chaotic system is more uniform, and has a wider range of chaotic parameters and better chaotic characteristics. In order to further prove the effectiveness of the improved chaotic system, we use the improved chaotic system as the key generator of the image encryption algorithm. And a threshold scrambling method based on dynamic rotation is designed, a relatively novel filter diffusion method is introduced, and finally the statistical information of pixels is completely changed through dynamic diffusion. Experimental simulation and security analysis show that the algorithm has good security.

The main contributions of this paper are described as follows:

1. Improve the classic Lorenz chaotic system, and prove the effectiveness of the improved chaotic system through the bifurcation diagram, LE value and randomness analysis of the generated key.
2. A threshold scrambling method based on dynamic rotation is proposed, and it has a good scrambling effect.
3. Use the filter diffusion method to perform rapid global diffusion on the scrambled image to change the statistical relationship between pixels.
4. A dynamic diffusion method is designed and plaintext-related parameters are introduced to effectively resist chosen-plaintext attacks.

The rest of the paper is organized as follows: Sect. 2 describes the preparation of this paper. Section 3 introduces the encryption and decryption process in detail. Section 4 analyzes the security performance of the dynamic rotation image encryption scheme based on optimized Lorenz chaos mentioned in this paper. Section 5 concludes the full text.

2 Preparations

2.1 Lorenz chaotic System

The Lorenz system [22] is the first dissipative system found in numerical experiments to exhibit chaotic motion, and its state equation is described as follows:

$$\begin{cases} \frac{\mathrm{dx}}{dt} = a(y-x) \\ \frac{dy}{dt} = bx - y - xz \\ \frac{dz}{dt} = xy - cz \end{cases} \tag{1}$$

The three parameters are: a is the prandtl number, b is the rayleigh number, and c is the direction ratio. When a $= 10$ and $c = \frac{8}{3}$, if $b > 24.74$, the system will enter the chaotic state. When $b = 28$, the system enters the best chaotic state. Since the Lorenz chaotic system enters the optimal chaotic state only when the parameter is $b > 28$, this limits the range of chaotic parameters. In order to expand the range of chaotic parameters of the Lorenz system, new nonlinear adjustment items and control parameters are added to generate more unpredictable pseudo-random numbers and increase the key space.

Improved Lorenz system is described as follows:

$$\begin{cases} \frac{dx}{dt} = a(y-x) \times e^7 - ceil(a(y-x) \times e^7) \\ \frac{dy}{dt} = (bx - y - xz) \times e^7 - ceil((bx - y - xz) \times e^7) \\ \frac{dz}{dt} = (xy - cz) \times e^7 - ceil((xy - cz) \times e^7). \end{cases} \tag{2}$$

where a, b and c are system parameters. For specific analysis of chaotic characteristics, please refer to Sect. 2.2.

2.2 Performance analysis of Lorenz chaotic system

2.2.1 *Bifurcation diagram analysis*

We discuss the bifurcation diagrams of the classical Lorenz chaotic system and the improved Lorenz chaotic system respectively. When the control parameters are changed, in order to obtain better randomness, the output of the chaotic map should cover the whole area as much as possible and should be dispersed as much as possible instead of clustering to a specific part of the area. As shown in Fig. 1, the bifurcation diagram of the improved Lorenz chaotic system presents an approximately uniform pseudo-random distribution feature, indicating that the sequence distribution has good ergodicity. The uniformity of the distribution is significantly improved compared to the sequence distribution generated by the classical Lorenz chaotic system.

2.2.2 *Lyapunov index analysis*

The LE [23] quantitatively describes the speed at which adjacent phase space orbits diverge or converge exponentially. Whether the maximum LE value is

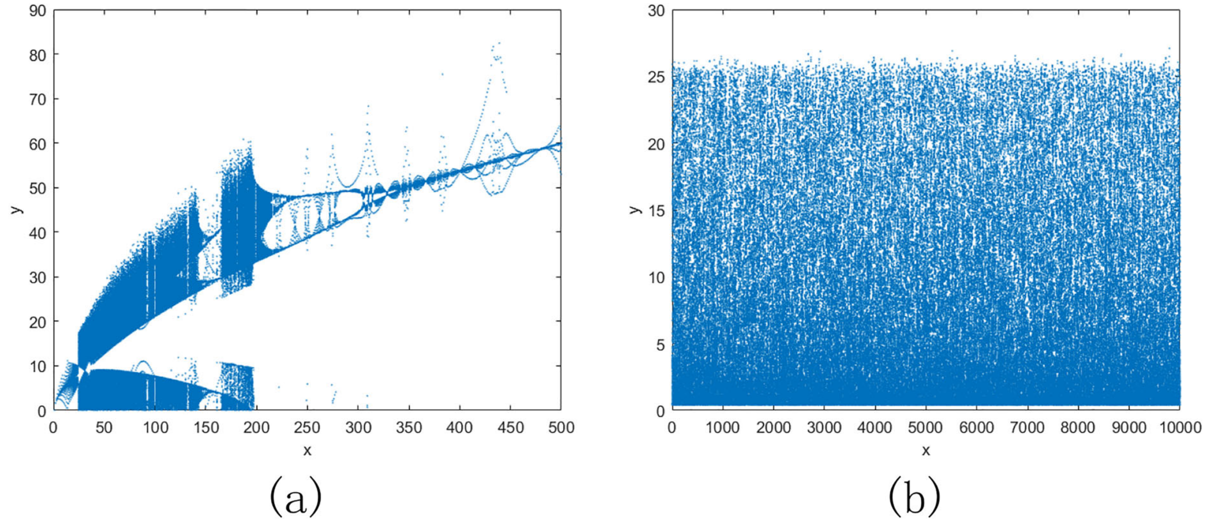


Fig. 1 Bifurcation diagram analysis: **a** bifurcation diagram of Lorenz chaotic system, **b** improve bifurcation diagram of Lorenz chaotic system

positive can very intuitively determine whether the system is in a chaotic state. The larger the positive value, the more obvious the chaotic characteristics and the higher the degree of chaos. The mathematical formula for calculating LE is defined as follows:

$$\lambda = \lim_{x\to\infty} \frac{1}{n} \sum\nolimits_{i=0}^{n-1} \ln|g'(x_i)| \tag{3}$$

where $g(x_i)$ is a time series of size n generated by the chaotic system. When $\lambda > 0$ indicates that the dynamic system is unstable, it indicates that the system is chaotic and unpredictable. On the contrary, when $\lambda < 0$, it indicates that the system is stable and non-chaotic.

Figure 2 shows the LE distribution of the Lorenz chaotic system before and after improvement. It can be clearly seen that only when the chaotic parameter before improvement is $b > 28$, it enters the optimal chaotic state, while the improved chaotic parameter $b > 0$ belongs to the optimal chaotic state. It should be noted that the LE value of the improved Lorenz chaotic system is relatively large, fluctuating around 14.3, which means that the improved Lorenz chaotic system has a wider range of control parameters and better chaotic characteristics.

2.2.3 The 0–1 test

The 0–1 test [24] is suitable for discrete sampled time series data and does not require phase space reconstruction. In this section, the 0–1 test of the chaotic system can achieve the effect of distinguishing periodic signals from chaotic signals. Observing the test results, if the signal is periodic, the value of K is close to 0. If the signal is chaotic, the value of K is close to 1.

We consider the chaotic sequence $\phi(j)$ of system (2) and then define the translation components p_c, q_c and mean square displacement $M_c(n)$ are defined as follows:

$$p_c(n) = \sum_{j=1}^{n} \phi(j)\cos(jc),\ q_c(n) = \sum_{j=1}^{n} \phi(j)\sin(jc) \tag{4}$$

$$M_c(n) = \lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{N} [p_c(j+n) - p_c(j)]^2 + [q_c(j+n) - q_c(j)]^2 \tag{5}$$

where $n = 1, ..., N$, $N = 5000$, c are arbitrary constants in the range of $(0, 2\pi)$.

From this, we can define the progressive growth rate K_c as defined as follows:

$$K_c = \lim_{n\to\infty} \frac{\log M_c(n)}{\log(n)} \tag{6}$$

Figure 3 shows the comparison dot plot of 0–1 test of Lorenz chaotic system before and after improvement. As can be seen from the figure, the improved

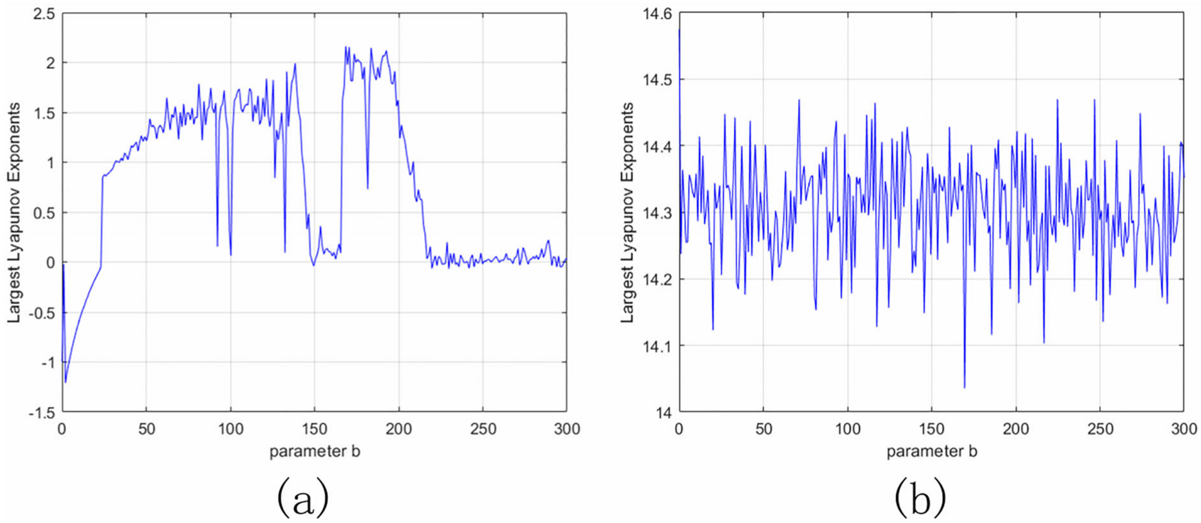


Fig. 2 Lyapunov index analysis: **a** LE graph for Lorenz chaotic system, **b** LE graph for improved Lorenz chaotic system

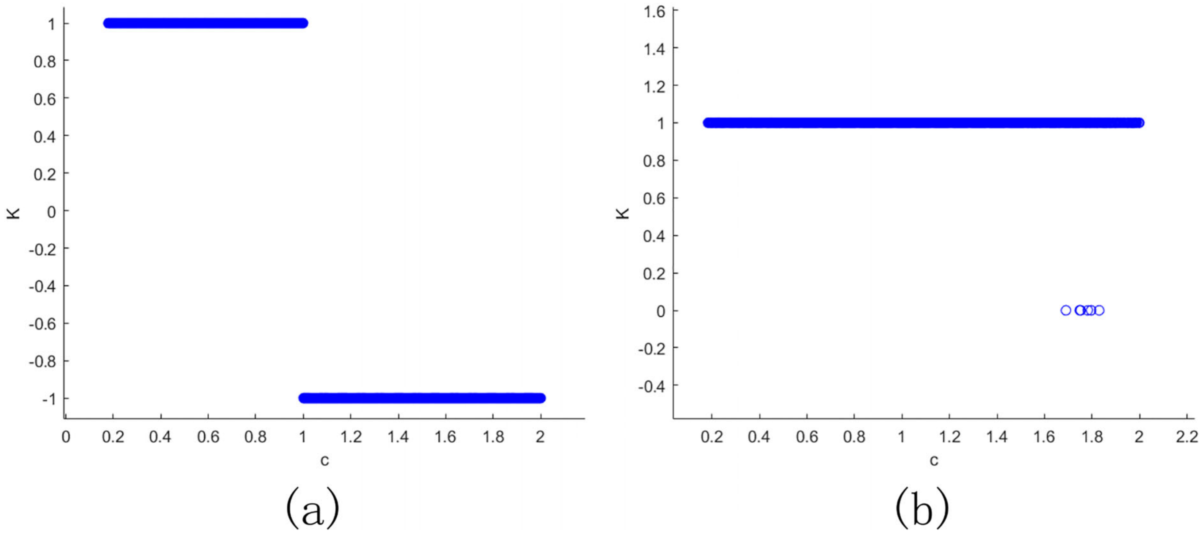


Fig. 3 The 0–1 text: **a** 0–1 test point diagram of Lorenz chaotic system, **b** 0–1 test point plot of improved Lorenz chaotic system

Lorenz system has a larger range of K value reaching 1, which proves that there are more chaotic signals in the improved chaotic system, which means that the improved chaotic system presents better chaos than the unimproved Lorenz system.

2.2.4 Permutation entropy analysis

Permutation Entropy (PE) [25] is defined by Bandt and Pompe. This paper presents an effective method for detecting the randomness of time series and the complexity of motion states of nonlinear systems. The larger the value of permutation entropy is, the better the chaotic degree of the sequence generated by the chaotic system is and the more complex the dynamic behavior is. In this subsection, we use the PE method to measure the permutation entropy of the Lorenz chaotic system before and after the improvement, and compare the two.

Figure 4 shows the permutation entropy values of the Lorenz chaotic system before and after the improvement. It can be seen from the figure that the permutation entropy value of the improved Lorenz chaotic system is larger than that of the system before

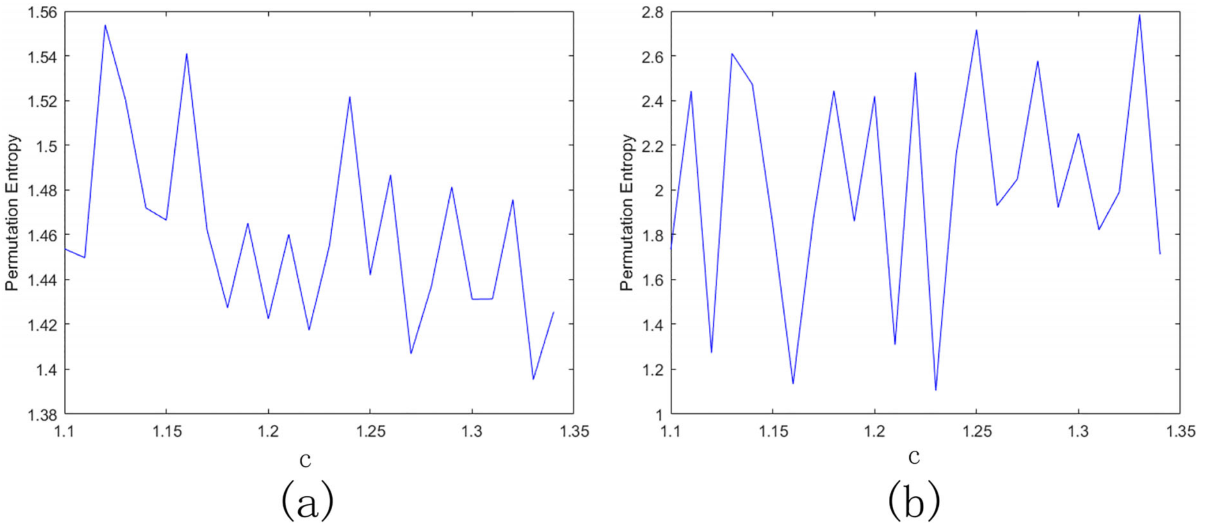


Fig. 4 Permutation entropy analysis: **a** Permutation entropy diagram of Lorenz chaotic system, **b** Permutation entropy diagram of improved Lorenz chaotic system

the improvement, and the chaotic effect is idealized, which proves that it has better nonlinear characteristics and more complex dynamic behavior.

2.2.5 *Sample entropy analysis*

Sample Entropy (SE) [26] is a new evaluation method of test time series complexity based on approximate entropy, which is used to describe the output similarity of dynamic systems. The larger the calculated SE value, the lower the regularity of the system and the more complex the chaotic behavior of the system. We define the m-dimensional time series $\{x_1, x_2, ..., x_N\}$ as follows:

$$SE(m, r, N) = -\log\frac{A}{B} \tag{7}$$

where $X_m(i) = \{x_i, x_{i+1}, ..., x_{i+m+1}\}$, m is the reconstruction dimension, r is the calculation threshold, we usually set $m = 2$, $r = 0.2 \times std$, (where std is the standard deviation of the measured time series). Where A, B denotes the number of vectors of $d[X_{m+1}(i), X_{m+1}(j)] < r$ and $d[X_m(i), X_m(j)] < r$, respectively. Where $d[X_m(i), X_m(j)] < r$, denotes the Chebyshev distance between $X_m(i)$ and $X_m(j)$.

Figure 5 shows the sample entropy values of the improved Lorenz chaotic system respectively, and it can be seen from the figure that the SE value of the classical Lorenz chaotic system shows a decreasing trend and has a small value, that is, the complexity is poor. The SE value of the improved Lorenz chaos shows an upward trend, and the value is larger than that of the chaotic SE value before the improvement, that is, the complexity is enhanced.

2.2.6 *NIST-800-22 test*

The National institute of standards and technology (NIST) [27] released a set of test sets for testing the quality of random number generators. The NIST test consists of 15 subtests for testing random (arbitrary length) binary sequences generated by a hardware-based or software-based encrypted random number or pseudorandom number generator. In the test experiments in this paper, we first run the modified Lorenz chaotic system using the MATLABR2022b software so that it produces chaotic test sequences. The floor() function is then used to perform a rounding operation on the chaotic test sequence to transform it into a sequence of decimal integers. And then the dec2bit() function is used to convert the sequence of decimal chaotic test integers to their binary representation. Finally the chaotic test sequence in binary form is saved in.mat format and NIST test is performed on it. When $p \geq 0.01$, the results of this subtest indicate that the test sequence is random and unpredictable. Conversely, if $p \leq 0.01$, the test sequence is not random. It can be seen from Table 1 that the improved chaotic

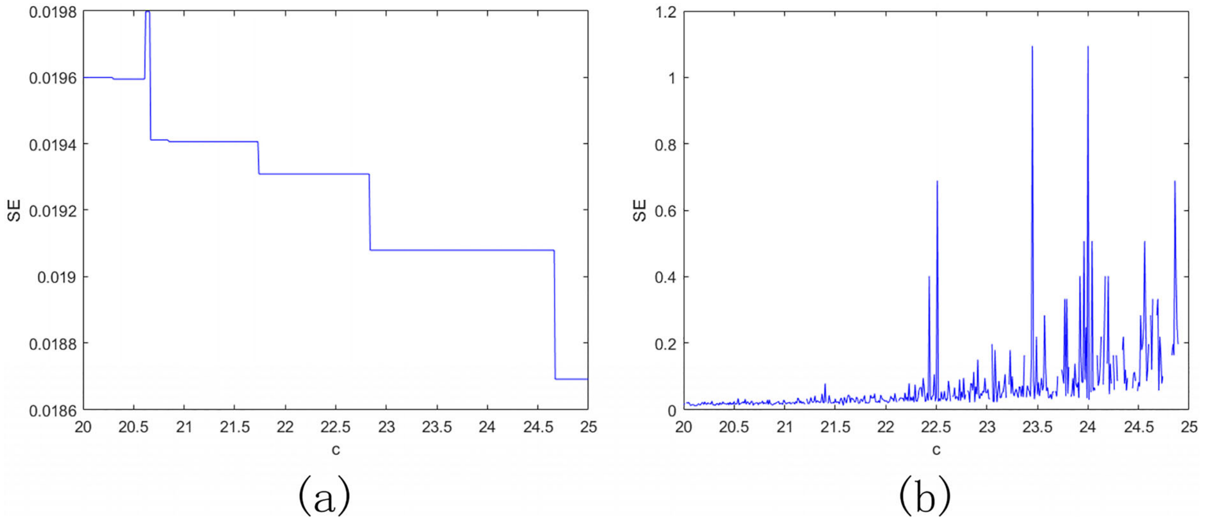


Fig. 5 Sample entropy analysis: **a** Sample entropy plot of Lorenz chaotic system, **b** Sample entropy plot of improved Lorenz chaotic system

system in this paper has high randomness and unpredictability.

2.3 Filter operation

Image filtering [28] is currently one of the most concerned and popular image processing techniques, such as image deblurring, image smoothing, and edge detection, etc. The commonly used definition of filtering in convolution operations is that a filter is a one-dimensional or two-dimensional matrix applied to each image pixel and its neighbors, where the central element of the filter is usually aligned with the current pixel and the other elements correspond to the neighbors. All multiplications between the filtered elements and the image pixels are then summed to obtain the filtered result. The filtering operation is shown in Fig. 6 Assuming that the size of the two-dimensional filtering mask is (2M+1) × (2M+1), the mathematical convolution operation of image filtering can be defined as:

Table 1 NIST test results for binary sequences produced by the modified Lorenz chaotic system

Test name	*P*-value	Result
Approximate entropy	0.205141	Success
Block-frequency	0.993280	Success
Cumulative sums (forward)	0.442430	Success
Cumulative sums (reverse)	0.552768	Success
FFT	0.422001	Success
Frequency test	0.309808	Success
Linear complexity	0.952669	Success
Long runs of ones	0.595242	Success
No overlapping templates	0.966313	Success
Overlapping templates	0.248340	Success
Rank	0.885022	Success
Runs	0.949741	Success
Serial	0.574546	Success
Universal	0.502335	Success
Random excursions	0.218533	Success

$$Out_{x,y} = \sum\nolimits_{i=-M}^{M} \sum\nolimits_{j=-M}^{M} W_{i+M+1,j+M+1} I_{x+1,y+1} \qquad (8)$$

where *W* is the filter mask, and *I* represents the original image.

Where $E_{2,2}$ is the filtered pixel of the corresponding pixel in the original image.

In 2017, Nianhua et al. [29] introduced Proposition 1 to prove that the filtering operation is reversible under certain conditions, so the filtering operation can be used to perform diffusion encryption on the image.

Proposition 1 For any given filter mask *W* of size (2M+1) × (2M+1), a plaintext image *p* of size $X \times Y$, and p' with gray level *F*, the specific operation is described as follows:

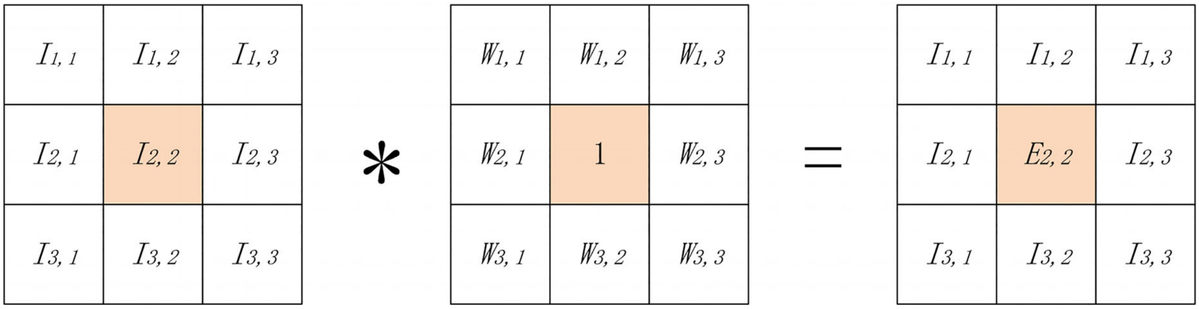

$I_{1,1}$ $I_{1,2}$ $I_{1,3}$
$I_{2,1}$ $I_{2,2}$ $I_{2,3}$
$I_{3,1}$ $I_{3,2}$ $I_{3,3}$
*
$W_{1,1}$ $W_{1,2}$ $W_{1,3}$
$W_{2,1}$ 1 $W_{2,3}$
$W_{3,1}$ $W_{3,2}$ $W_{3,3}$
=
$I_{1,1}$ $I_{1,2}$ $I_{1,3}$
$I_{2,1}$ $E_{2,2}$ $I_{2,3}$
$I_{3,1}$ $I_{3,2}$ $I_{3,3}$

Fig. 6 An example of an image filtering operation

$$I_{x,y} = \left(\sum\nolimits_{i=-M}^{M} \sum\nolimits_{j=-M}^{M} W_{i+M+1,j+M+1}P_{x+1,y+1}\right) \bmod F \tag{9}$$

The inverse operation is described as follows:

$$P_{x,y} = (I_{x,y} - \sum\nolimits_{i,j\in\{-M,\ldots,M\}\cap(i,j)\neq(0,0)} W_{i+M+1,j+M+1}P_{x+1,j+1}) mod\ F \tag{10}$$

If $P \in N,\ W \in N$, and $W_{M+1,M+1} = 1$.

Proof: Since $W_{M+1,M+1} = 1$, formula (5) can be rewritten as:

$$\begin{aligned} I_{x,y} &= \left(\left(\sum\nolimits_{i,j\in\{-M,\ldots,M\}\cap(i,j)\neq(0,0)} W_{i+M+1,j+M+1}P_{x+1,y+1}\right) + W_{M+1,M+1}P_{x,y}\right) \bmod F \\ &= \left(\left(\sum\nolimits_{i,j\in\{-M,\ldots,M\}\cap(i,j)\neq(0,0)} W_{i+M+1,j+M+1}P_{x+1,y+1}\right) + P_{x,y}\right) \bmod F \\ &= \left(\sum\nolimits_{i,j\in\{-M,\ldots,M\}\cap(i,j)\neq(0,0)} W_{i+M+1,j+M+1}P_{x+1,y+1}\right) + P_{x,y} - kF \end{aligned} \tag{11}$$

where k is an integer. Substitute into the above formula to get:

$$P_{x,y} \ = I_{x,y} + kF - \sum\nolimits_{i,j\in\{-M,\ldots,M\}\cap(i,j)\neq(0,0)} W_{i+M+1,j+M+1}P_{x+1,y+1} \tag{12}$$

Because $P \in N$, F is the gray level of P, $0 \leq P_{x,y} < F$, so formula (8) can be written as:

$$\begin{aligned} P_{x,y} &= \left(I_{x,y} + kF - \sum\nolimits_{i,j\in\{-M,\ldots,M\}\cap(i,j)\neq(0,0)} W_{i+M+1,j+M+1}P_{x+1,y+1}\right) \bmod F \\ &= \left(I_{x,y} - \sum\nolimits_{i,j\in\{-M,\ldots,M\}\cap(i,j)\neq(0,0)} W_{i+M+1,j+M+1}P_{x+1,y+1}\right) \bmod F \end{aligned} \tag{13}$$

Proposition 1 is proved.

3 Image encryption algorithm

A dynamic rotation image encryption algorithm based on optimized Lorenz chaos is proposed. The algorithm mainly includes improving chaotic system, dynamic round-robin scrambling, filter diffusion and dynamic diffusion. The encryption flow chart is shown in Fig. 7.

3.1 Encryption process

Step1 Take a plaintext image P of size $M \times N$ as the test image.

Step2 Divide the plaintext image up and down into two image blocks P_{img1} and P_{img2} of equal size.

$$\begin{cases} P_{img1} = P(1 : \dfrac{M}{2}, 1 : N) \\ P_{img2} = P(\dfrac{M}{2} + 1; M, 1 : N) \end{cases} \tag{14}$$

Step3 Take x_0, y_0, z_0 as initial values, iterate the chaotic system (2) t_0 times to generate the chaotic sequences X, Y, Z, delete the results of the first 200 iterations to avoid the avalanche effect, and obtain random keys $Lor_{key1}, Lor_{key2}, Lor_{key3}$ after transformation.

$$\begin{cases} Lor_{key1} = \bmod\left(floor\left(\left(X(200 : 200 + M \times N) \times 10^{15}\right), 256\right)\right) \\ Lor_{key2} = \bmod\left(floor\left(\left(Y(200 : 200 + M \times N) \times 10^{15}\right), 256\right)\right) \\ Lor_{key3} = \bmod\left(floor\left(\left(Z(200 : 200 + M \times N) \times 10^{15}\right), 256\right)\right) \end{cases} \tag{15}$$

Among them, the mod() function is the remainder, the *floor*() function is the rounding down, and t_0 is evaluated 7000 times.

Step4 Use keys Lor_{key2} and Lor_{key3} to construct chaos control table CCT.

$$CCT = reshape\left(\bmod\left(bitxor\left(Lor_{key2}, Lor_{key3}\right), \frac{M}{2}\right), M, N\right) \tag{16}$$

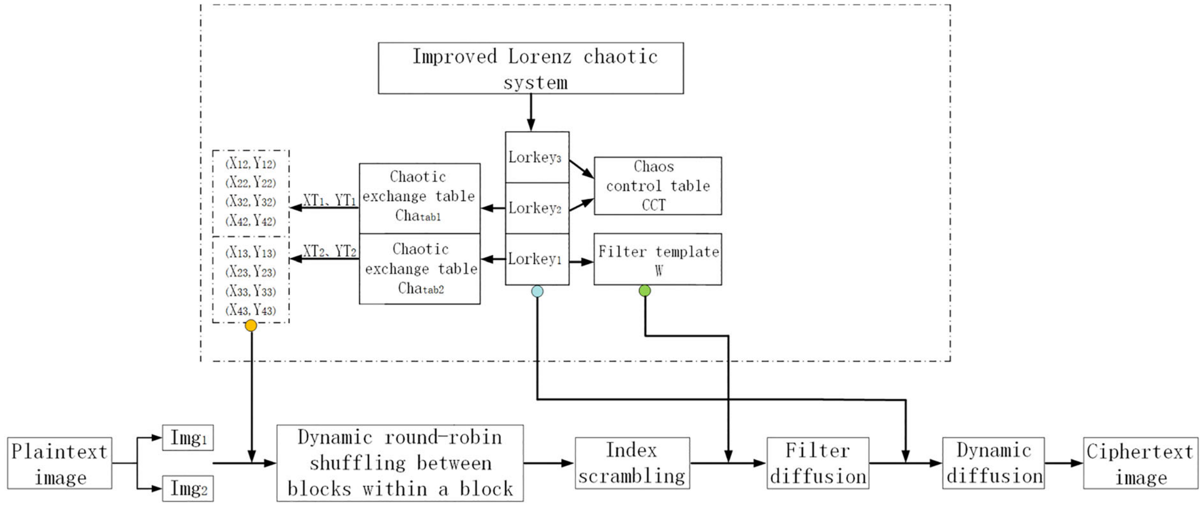


Fig. 7 Encryption flowchart

Step5 Use chaotic sequences X and Y to construct chaotic exchange tables Cha_{tab1}, Cha_{tab2} and Cha_{tab3}, Cha_{tab4}.

$$\begin{cases} Cha_{tab1} = floor\left(\bmod\left(X \times 10^{16}, \dfrac{M}{2}\right)\right) + 1 \\ Cha_{tab2} = floor\left(\bmod\left(X \times 10^{16}, M\right)\right) + 1 \end{cases} \tag{17}$$

$$\begin{cases} Cha_{tab3} = floor\left(\bmod\left(Y \times 10^{16}, \dfrac{M}{2}\right)\right) + 1 \\ Cha_{tab4} = floor\left(\bmod\left(Y \times 10^{16}, M\right)\right) + 1 \end{cases} \tag{18}$$

Step6-A Use the chaos exchange tables Cha_{tab1} and Cha_{tab2} obtained in Step5 to calculate and obtain x coordinate range XT_1 and y coordinate range YT_1 respectively. Using XT_1 and YT_1 to calculate 4 exchanged coordinate pairs $\left(C_{x12}, C_{y12}\right)$, $\left(\mathrm{C}_{x22}, \mathrm{C}_{y22}\right)$, $\left(\mathrm{C}_{x32}, \mathrm{C}_{y32}\right)$, $\left(\mathrm{C}_{x42}, \mathrm{C}_{y42}\right)$.

$$XT_1 = \begin{cases} \bmod\left(Cha_{tab1}(i,j) + \mu 1, \dfrac{M}{2}\right) + 1, if \;\; abs(Cha_{tab1}\;(i,j) - 2i) < \dfrac{M}{2} \\ Cha_{tab1}(i,j) \end{cases} \tag{19}$$

$$\begin{cases} \begin{cases} C_{x12} = unique\left(XT_1\left(1 : \dfrac{M \times N}{5}\right)\right) \\ C_{x12}(find(C_{x12} = 0) = []) \end{cases} \\ \begin{cases} C_{x22} = unique\left(XT_1\left(\dfrac{M \times N}{5} : \dfrac{M \times N}{4}\right)\right) \\ C_{x22}(find(C_{x22} = 0) = []) \end{cases} \\ \begin{cases} C_{x32} = unique\left(XT_1\left(\dfrac{M \times N}{4} : \dfrac{M \times N}{3}\right)\right) \\ C_{x32}(find(C_{x32} = 0) = []) \end{cases} \\ \begin{cases} C_{x42} = unique\left(XT_1\left(\dfrac{M \times N}{3} : \dfrac{M \times N}{2}\right)\right) \\ C_{x42}(find(C_{x42} = 0) = []) \end{cases} \end{cases} \tag{20}$$

$$YT_1 = \begin{cases} \bmod(Cha_{tab2}(i,j), N) + 1, if \;\; abs(Cha_{tab2}\;(i,j) - i) < \dfrac{N}{2} \\ Cha_{tab2}(i,j) \end{cases} \tag{21}$$

$$\begin{cases} \begin{cases} C_{y12} = unique\left(YT_1\left(1 : \dfrac{M \times N}{5}\right)\right) \\ C_{y12}\left(find\left(C_{y12} = 0\right) = []\right) \end{cases} \\ \begin{cases} C_{y22} = unique\left(YT_1\left(\dfrac{M \times N}{5} : \dfrac{M \times N}{4}\right)\right) \\ C_{y22}\left(find\left(C_{y22} = 0\right) = []\right) \end{cases} \\ \begin{cases} C_{y32} = unique\left(YT_1\left(\dfrac{M \times N}{4} : \dfrac{M \times N}{3}\right)\right) \\ C_{y32}\left(find\left(C_{y32} = 0\right) = []\right) \end{cases} \\ \begin{cases} C_{y42} = unique\left(YT_1\left(\dfrac{M \times N}{3} : \dfrac{M \times N}{2}\right)\right) \\ C_{y42}\left(find\left(C_{y42} = 0\right) = []\right) \end{cases} \end{cases} \tag{22}$$

Step6-B Use the chaos exchange tables Cha_{tab3} and Cha_{tab4} obtained in Step5 to calculate and obtain x coordinate range XT_2 and y coordinate range YT_2 respectively. Using XT_2 and YT_2 to calculate 4 exchanged coordinate pairs (C_{x13}, C_{y13}), (C_{x23}, C_{y23}), (C_{x33}, C_{y33}), (C_{x43}, C_{y43}).

$$XT_2 = \begin{cases} \bmod\left(Cha_{tab3}(i,j) + \mu 1, \dfrac{M}{2}\right) + 1, if \;\; abs(Cha_{tab3}\;(i,j) - 2i) < \dfrac{M}{2} \\ Cha_{tab3}\;(i,j) \end{cases} \tag{23}$$

$$\begin{cases} \begin{cases} C_{x13} = unique\left(XT_2\left(1 : \dfrac{M \times N}{5}\right)\right) \\ C_{x13}(find(C_{x13} = 0) = []) \end{cases} \\ \begin{cases} C_{x23} = unique\left(XT_2\left(\dfrac{M \times N}{5} : \dfrac{M \times N}{4}\right)\right) \\ C_{x23}(find(C_{x23} = 0) = []) \end{cases} \\ \begin{cases} C_{x33} = unique\left(XT_2\left(\dfrac{M \times N}{4} : \dfrac{M \times N}{3}\right)\right) \\ C_{x33}(find(C_{x33} = 0) = []) \end{cases} \\ \begin{cases} C_{x43} = unique\left(XT_2\left(\dfrac{M \times N}{3} : \dfrac{M \times N}{2}\right)\right) \\ C_{x43}(find(C_{x43} = 0) = []) \end{cases} \end{cases} \tag{24}$$

$$YT_2 = \begin{cases} \bmod(Cha_{tab4}(i,j), N) + 1, if \;\; abs(Cha_{tab4}(i,j) - i) < \dfrac{N}{2} \\ Cha_{tab4}(i,j) \end{cases} \tag{25}$$

$$\begin{cases} \begin{cases} C_{y13} = unique\left(YT_2\left(1 : \dfrac{M \times N}{5}\right)\right) \\ C_{y13}(find(C_{y13} = 0) = []) \end{cases} \\ \begin{cases} C_{y23} = unique\left(YT_2\left(\dfrac{M \times N}{5} : \dfrac{M \times N}{4}\right)\right) \\ C_{y23}(find(C_{y23} = 0) = []) \end{cases} \\ \begin{cases} C_{y33} = unique\left(YT_2\left(\dfrac{M \times N}{4} : \dfrac{M \times N}{3}\right)\right) \\ C_{y33}(find(C_{y33} = 0) = []) \end{cases} \\ \begin{cases} C_{y43} = unique\left(YT_2\left(\dfrac{M \times N}{3} : \dfrac{M \times N}{2}\right)\right) \\ C_{y43}(find(C_{y43} = 0) = []) \end{cases} \end{cases} \tag{26}$$

Among them, the $i = 1, 2, 3, \ldots, M, j = 1, 2, 3, \ldots, N_{\circ}$.*unique*() function is to remove the repeated numbers in the matrix, the *find*() function is to return the position of the non-zero element in the vector, and means to save the 0 element as empty.

Step7 Threshold rotation scrambling: perform intra-block scrambling and inter-block scrambling on the two image blocks P_{img1} and P_{img2}, in order to improve the efficiency and effect of image scrambling, thereby completely reducing the correlation of adjacent pixels of the image. Before selecting the two pixels to be randomly exchanged, add a judgment threshold of Cor_{thr}, only when the difference between the two pixels to be exchanged is greater than Cor_{thr}, the exchange is performed, otherwise the random coordinates need to be rotated and rejudged until the difference between two pixels is greater than the threshold Cor_{thr}, a schematic diagram of inter-block scrambling within a block is shown in Fig. 8, and a schematic diagram of round-robin scrambling based on an intra-block inter-block scrambling is shown in Fig. 9.

Step7-A If the chaos control table $CCT > \frac{M}{2}$, then carry out image block P_{img1} built-in chaos.

$$\begin{cases} P_{img1}(i,j) - P_{img1}(C_{x12}(i), C_{y12}(j)) > Cor_{thr} \\ \tau = P_{img1}(i,j) \\ P_{img1}(i,j) = P_{img1}(C_{x12}(i), C_{y12}(j)) \\ P_{img1}(C_{x12}(i), C_{y12}(j)) = \tau \end{cases} \tag{27}$$

$$\begin{cases} P_{img1}(i,j) - P_{img1}(C_{x22}(i), C_{y22}(j)) > Cor_{thr} \\ \tau = P_{img1}(i,j) \\ P_{img1}(i,j) = P_{img1}(C_{x22}(i), C_{y22}(j)) \\ P_{img1}(C_{x22}(i), C_{y22}(j)) = \tau \end{cases} \tag{28}$$

$$\begin{cases} \tau = P_{img1}(i,j) \\ P_{img1}(i,j) = P_{img1}(C_{x32}(i), C_{y32}(j)) \\ P_{img1}(C_{x32}(i), C_{y32}(j)) = \tau \end{cases} \tag{29}$$

If the chaos control table $CCT \leq \frac{M}{2}$, then carry out image block P_{img2} built-in chaos.

$$\begin{cases} P_{img2}(i,j) - P_{img2}(C_{x13}(i), C_{y13}(j)) > Cor_{thr} \\ \tau = P_{img2}(i,j) \\ P_{img2}(i,j) = P_{img2}(C_{x13}(i), C_{y13}(j)) \\ P_{img2}(C_{x13}(i), C_{y13}(j)) = \tau \end{cases} \tag{30}$$

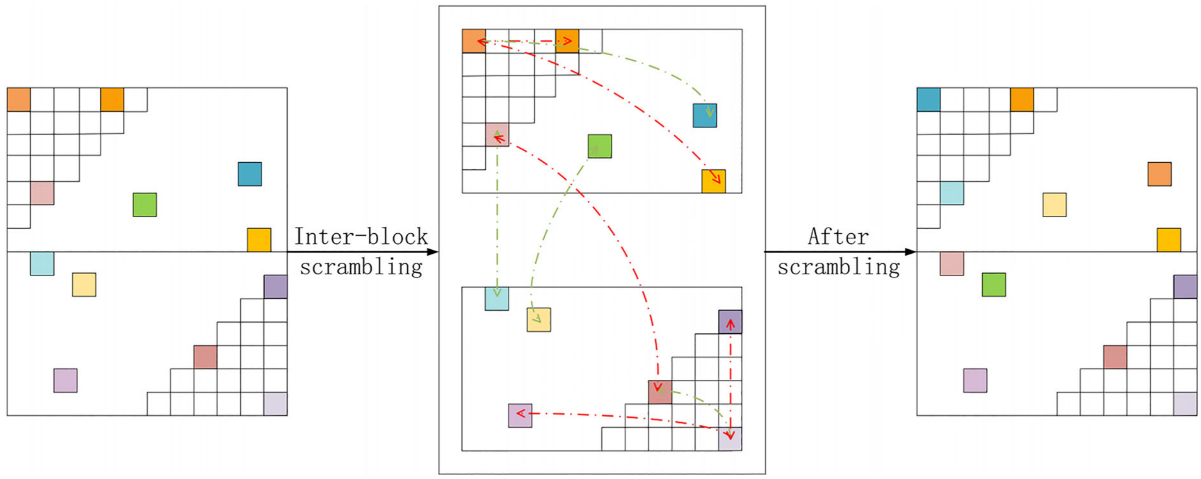


Fig. 8 Intra-block and inter-block scrambling

$$\begin{cases} P_{img2}(i,j) - P_{img2}\left(C_{x23}(i), C_{y23}(j)\right) > Cor_{thr} \\ \tau = P_{img2}(i,j) \\ P_{img2}(i,j) = P_{img2}\left(C_{x23}(i), C_{y23}(j)\right) \\ P_{img2}\left(C_{x23}(i), C_{y23}(j)\right) = \tau \end{cases} \tag{31}$$

$$\begin{cases} \tau = P_{img2}(i,j) \\ P_{img2}(i,j) = P_{img2}\left(C_{x33}(i), C_{y33}(j)\right) \\ P_{img2}\left(C_{x33}(i), C_{y33}(j)\right) = \tau \end{cases} \tag{32}$$

Step7-B If the chaos control table is $CCT > \frac{M}{2}$, perform inter-block scrambling according to the swap coordinate pairs obtained in Step6-A.

$$\begin{cases} P_{img1}(i,j) - P_{img2}\left(C_{x12}(i), C_{y12}(j)\right) > Cor_{thr} \\ \tau = P_{img1}(i,j) \\ P_{img1}(i,j) = P_{img2}\left(C_{x12}(i), C_{y12}(j)\right) \\ P_{img2}\left(C_{x12}(i), C_{y12}(j)\right) = \tau \end{cases} \tag{33}$$

$$\begin{cases} P_{img1}(i,j) - P_{img2}\left(C_{x22}(i), C_{y22}(j)\right) > Cor_{thr} \\ \tau = P_{img1}(i,j) \\ P_{img1}(i,j) = P_{img2}\left(C_{x22}(i), C_{y22}(j)\right) \\ P_{img2}\left(C_{x22}(i), C_{y22}(j)\right) = \tau \end{cases} \tag{34}$$

$$\begin{cases} \tau = P_{img1}(i,j) \\ P_{img1}(i,j) = P_{img2}\left(C_{x32}(i), C_{y32}(j)\right) \\ P_{img2}\left(C_{x32}(i), C_{y32}(j)\right) = \tau \end{cases} \tag{35}$$

If the chaos control table is $CCT \le \frac{M}{2}$, perform inter-block scrambling according to the swap coordinate pairs obtained in Step6-B.

$$\begin{cases} P_{img1}(i,j) - P_{img2}\left(C_{x13}(i), C_{y13}(j)\right) > Cor_{thr} \\ \tau = P_{img1}(i,j) \\ P_{img1}(i,j) = P_{img2}\left(C_{x13}(i), C_{y13}(j)\right) \\ P_{img2}\left(C_{x13}(i), C_{y13}(j)\right) = \tau \end{cases} \tag{36}$$

$$\begin{cases} P_{img1}(i,j) - P_{img2}\left(C_{x23}(i), C_{y23}(j)\right) > Cor_{thr} \\ \tau = P_{img1}(i,j) \\ P_{img1}(i,j) = P_{img2}\left(C_{x23}(i), C_{y23}(j)\right) \\ P_{img2}\left(C_{x23}(i), C_{y23}(j)\right) = \tau \end{cases} \tag{37}$$

$$\begin{cases} \tau = P_{img1}(i,j) \\ P_{img1}(i,j) = P_{img2}\left(C_{x33}(i), C_{y33}(j)\right) \\ P_{img2}\left(C_{x33}(i), C_{y33}(j)\right) = \tau \end{cases} \tag{38}$$

Step8 Concatenate the two image blocks P_{img1} and P_{img2}:

$$PZ = \left[P_{img1} : P_{img2}\right] \tag{39}$$

Step9 Further perform index scrambling on the integrated image PZ to completely reduce the correlation of adjacent pixels:

$$SCRP = PZ(index(X)) \tag{40}$$

Step10 Use the first group of masks W of size 3 × 3 generated by chaotic sequence X, and the masks can be used continuously.

$$\begin{cases} Key_W = \mathrm{mod}\left(floor\left(\left(X(200:200+M\times N\times 9)\times 10^{15}\right), 256\right)\right) \\ W = Key(0:9) \end{cases} \tag{41}$$

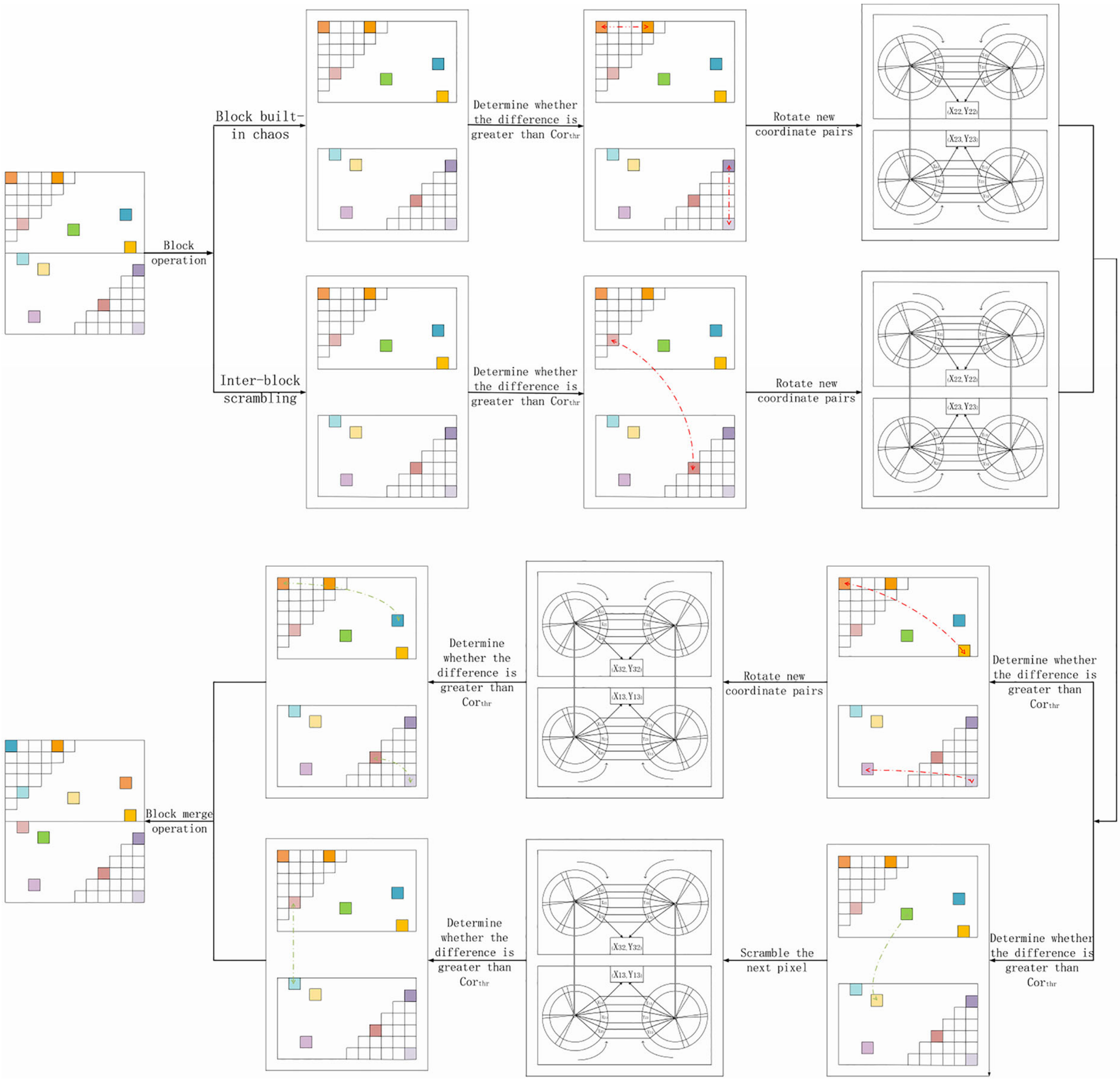


Fig. 9 Dynamic round-robin scrambling based on intra-block and inter-block thresholds

Step11 Combining the mask W given in Proposition 1 and Step10, we can design the image filtering operation for image encryption as:

$$EN_{x,y} = \left(\left(\sum_{i,j\in\{-2M,\dots,0\}\cap(i,j)\neq(0,0)} W_{i+2M+1,j+2M+1}EN_{x+1,y+1}\right) + SCRP_{x,y}\right) \bmod F \tag{42}$$

Step12 Further perform dynamic diffusion processing on $DE_{x,y}$ to obtain the final ciphertext image.

$$\begin{cases} \sigma = \mathrm{mod}\left(floor\left(Lor_{key2} \times 10^{16}\right), \theta\right) \\ DE(1) = \mathrm{mod}\left(bitxor\left(DE(1) + \sigma, Lor_{key1}(1)\right), 256\right) \\ DE(i+1, j+1) = bitxor\left(bitxor\left(DE(i,j), Lor_{key2}(i,j)\right), Lor_{key3}(i,j)\right) \end{cases} \tag{43}$$

where θ represents the user control parameter, $i = 1, 2, 3, \dots, M, j = 1, 2, 3, \dots, N$。

3.2 Decryption process

Since the proposed algorithm is a symmetric encryption algorithm, the decryption algorithm is the inverse

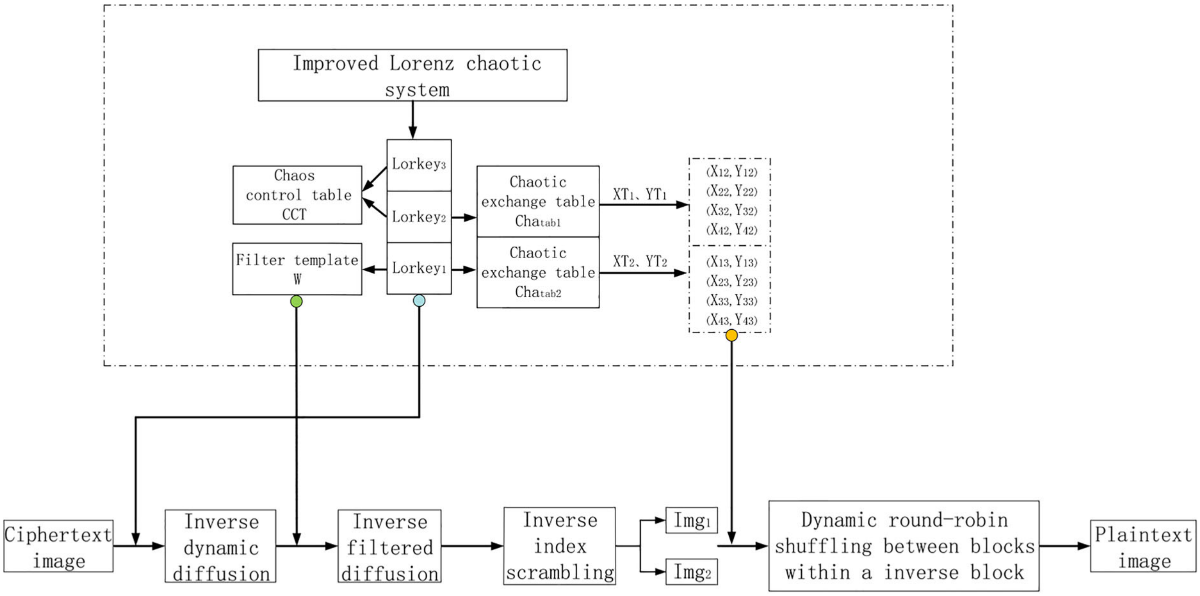


Fig. 10 Decryption flowchart

process of the encryption algorithm. The decryption steps are summarized as follows:

Step1 By using the generated control parameters σ and the key $Lor_{key1}, Lor_{key2}, Lor_{key3}$, the inverse dynamic diffusion operation is performed on the ciphertext image DE to obtain the image DE'.

Step2 By utilizing mask W, image DE' is applied inverse dynamic diffusion operation to obtain image D.

The inverse filtering operation is formulated as follows:

$$D_{x,y} = \left(EN_{x,y} - \sum\nolimits_{i,j\in\{-2M,\ldots,0\}\cap(i,j)\neq(0,0)} W_{i+2M+1,j+2M+1} EN_{x+1,y+1}\right) \bmod F \tag{44}$$

Step3 By using chaotic sequence X, image D is scrambled by inverse index to obtain image PCA.

Step4 By using the exchange coordinate pairs generated by the chaotic exchange table Cha_{tab1}, Cha_{tab2}, Cha_{tab3} and Cha_{tab4}, under the control of the judgment threshold Cor_{thr}, the image PCA was rotated and scrambled by inverse threshold, and finally the plaintext image $srcImg$ was solved.

The decryption flow chart is shown in Fig. 10.

4 Experimental simulation and performance analysis

4.1 Key space analysis

With the development of supercomputers around the world (Such as Fugaku supercomputer in Japan, its peak performance has reached 537210.00 $TFlop/S$; Summit supercomputer in the United States, peak computing performance is 200794.90 $TFlop/S$; Sunway TaihuLight supercomputer in China, The peak computing performance is 125435.90 $TFlop/S$), which makes it possible to attack digitally encrypted images. Therefore, critical keyspace analysis becomes necessary. A keyspace is the set of all possible keys that can be used to generate a key, and its size depends on the length of the security key. It is one of the most important characteristics that determine the strength of a cryptosystem [30]. The size of the keyspace is determined by all the parameters used in the encryption process. When the keyspace is larger than 2^{100}, it is resistant to attacks such as brute force attacks. The main keys in the encryption algorithm proposed in this paper are all generated by the improved Lorenz chaotic system. The precision of the computer is 10^{-16}, and the key space for this scheme is $\left(10^{16}\right)^6 = 10^{96} > 2^{288} > 2^{100}$. Judging from the computing power of current computers, our scheme can effectively resist brute force attacks.

4.2 Key sensitivity analysis

Generally speaking, a good encryption algorithm requires that the encryption key be sensitive enough, which means that even a small change in the encryption key can cause a large change in the encrypted image. In this paper, by changing the initial parameter x of the chaotic system, the key sensitivity error value is calculated. The sensitivity error of the classical chaotic system to the initial parameter x is only 10^{-17}, while the sensitivity of the improved Lorenz chaotic system is enhanced. Its corresponding decrypted image result is shown in Fig. 11. When the key deviation is 10^{-19}, the image cannot be decrypted successfully. However, when the key deviation is 10^{-20}, the original image can be decrypted. It can be seen that the image is not allowed to be successfully decrypted when the key used for decryption purposes is slightly changed. It is proved that the key of the model proposed in this paper is extremely sensitive and can effectively resist brute force attack.

In order to observe the difference between the encrypted image and the incorrectly decrypted image more intuitively, this paper also uses the mean squared error (MSE) [31] standard for data analysis, and the data results are shown in Table 2.

$$MSE = \frac{1}{M \times N} \sum\nolimits_{i=1}^{M} \sum\nolimits_{j=1}^{N} (p(i,j) - d(i,j))^2 \quad (45)$$

Among them, M and N represent the size of the image, and (i,j) represents the coordinate points in the plaintext image p and the decrypted image d. The larger the MSE data measured experimentally in Table 2, the more secure the proposed encryption scheme.

4.3 Information entropy analysis

Entropy is an important measure of the amount of uncertainty in a system. It measures the uniform distribution of pixels in an image [32]. If the information entropy is equal to the bit length, the system is not vulnerable to statistical attacks. The mathematical equation for calculating entropy is described as follows:

$$H(m) = -\sum\nolimits_{i=0}^{2^N-1} p(m_i) \log_2 p(m_i) \quad (46)$$

where N represents the gray level of the image, and $\log_2 p(m_i)$ represents the probability that the gray level m_i appears in the image. For an ideal ciphertext image in the range of $[0, 255]$, the entropy value is 8. The test results of the method proposed in this paper are shown in Table 3. By comparing other literatures, it can be seen that the entropy value of the scheme proposed in this paper is closer to the theoretical value.

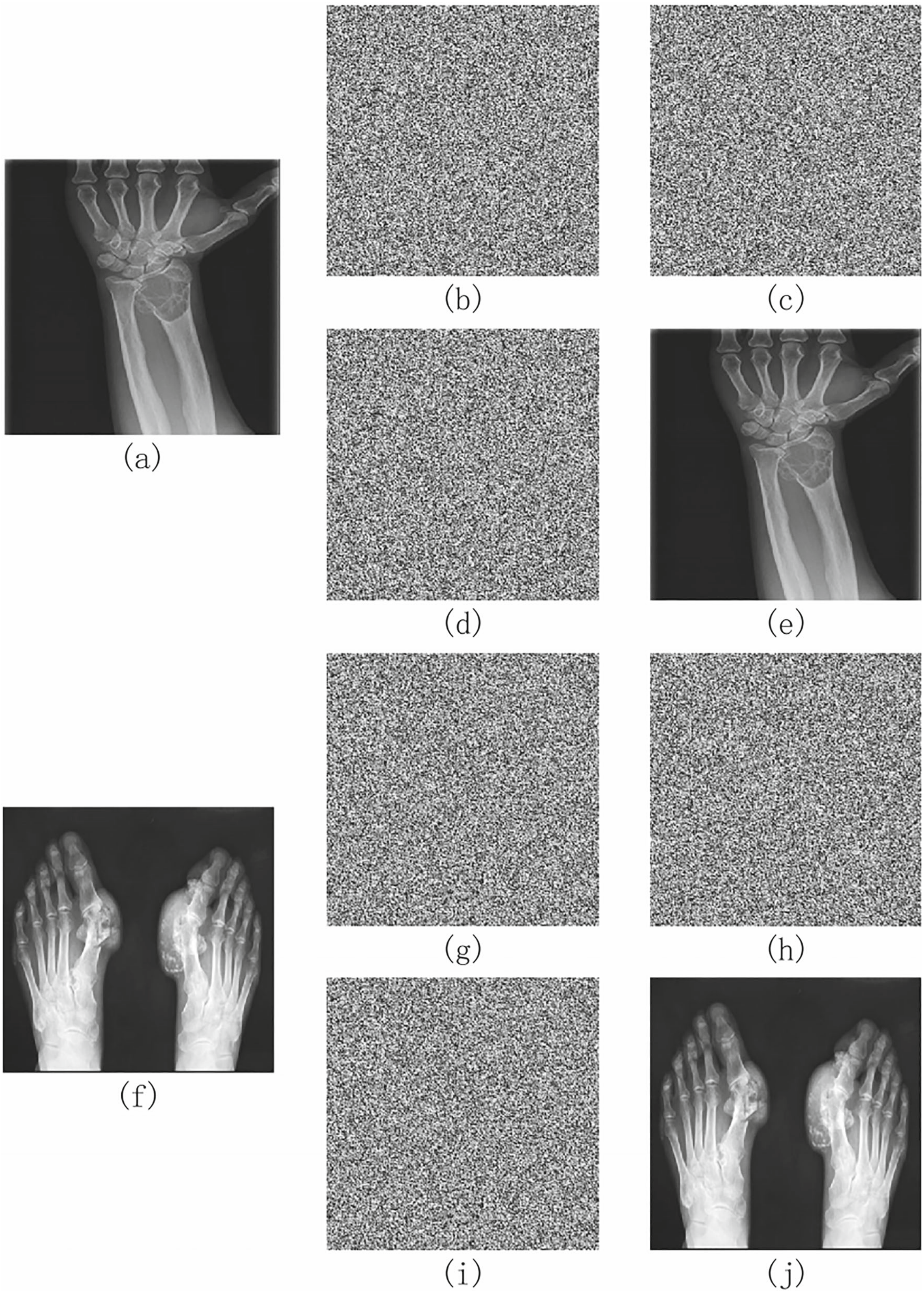
4.4 Histogram analysis

Histogram refers to the frequency statistics of each gray value in the image, reflecting the most basic statistical characteristics of the image [37]. If the encrypted image has a relatively average histogram, the ciphertext is considered to have high security. The encryption and decryption results of the proposed encryption algorithm are shown in Fig. 12, and the histogram analysis is shown in Fig. 13. As can be seen from the figure, the gray level distribution of plaintext image pixels is extremely uneven and fluctuates greatly, which means its pseudo-randomness and redundancy are low, and it is easy for attackers to obtain image-related information. Both fusion schemes show good consistency on the histogram of the ciphertext image, with high image redundancy and pseudo-randomness, effectively. It conceals the statistical probability distribution characteristics of the gray value of the pixel.

4.5 Correlation of two adjacent pixels

The correlation between adjacent pixels reflects the quality of the algorithm's scrambling effect [38]. The lower the correlation between adjacent pixels in a ciphertext image generated by a good encryption algorithm, the better the scrambling effect of the algorithm. We analyze the correlation between adjacent pixels in the horizontal, vertical and diagonal directions of the image. The correlation coefficient formula is described as follows:

$$C = \frac{\sum\nolimits_{i=1}^{N} \left(x_i - \frac{1}{N}\sum\nolimits_{i=1}^{N} x_i\right)\left(y_i - \frac{1}{N}\sum\nolimits_{i=1}^{N} y_i\right)}{\sqrt{\sum\nolimits_{i=1}^{N} \left(x_i - \frac{1}{N}\sum\nolimits_{i=1}^{N} x_i\right)^2 \times \sum\nolimits_{i=1}^{N} \left(y_i - \frac{1}{N}\sum\nolimits_{i=1}^{N} y_i\right)^2}} \quad (47)$$


(a)
(b)
(c)
(d)
(e)
(f)
(g)
(h)
(i)
(j)

◀**Fig. 11** Key sensitivity analysis: **a** The original picture of "wrist", **b** is the image encrypted using $x_1 + 10^{-19}$, **c** is the image of the failed decryption using $x_1\prime + 10^{-19}$, **d** is the image encrypted using $x_2 + 10^{-20}$, **e** is the image of the successfully decrypted using $x_2\prime + 10^{-20}$, **f** is the "foot" original image, **g** is the image encrypted using $x_3 + 10^{-19}$, **h** is the image of the failed decryption using $x_3\prime + 10^{-19}$, **i** is the image encrypted using $x_4 + 10^{-20}$, **j** is the image of the successfully decrypted using $x_4\prime + 10^{-20}$

Among them, x and y are the gray levels of two adjacent pixels in the image, and N represent the total number of pixels in the image. In this test, we randomly select 7500 pairs of adjacent pixels, and analyze the correlation between adjacent pixels in the plaintext grayscale image and the ciphertext image from three directions. Figures 14 and 15 show the correlation analysis of neighboring pixels of the proposed scheme. It can be seen that the pixel correlation distribution of the ciphertext image is relatively uniform. In terms of numerical analysis, the comparison results of the proposed scheme with other schemes are shown in Table 4. Observations show that the adjacent pixel correlation of the encryption algorithm in this paper is closer to 0, which is obviously better than the comparison algorithm. This shows that the proposed scheme effectively removes the correlation between adjacent pixels in the image and has better resistance to statistical attacks.

Table 3 Information entropy for the encryption

	Entropy
"Wrist"	**7.9979**
"Skull"	7.9978
"Thorax"	7.9978
"Foot"	7.9977
[33]	7.9976
[34]	7.9972
[35]	7.9577
[36]	7.4729

4.6 Peak signal-to-noise ratio analysis and ssim

Peak signal-to-noise ratio (PSNR) [41] is the most common and widely used image objective evaluation index. Multiple types of noise attacks will interfere with the pixel values of the original image. In order to measure the image quality after the noise attack, we usually refer to the PSNR value to judge whether the processing process can obtain good results. Its expression is described as follows:

$$PSNR = 10 \times \log_{10}\left(\frac{MAX_i^2}{MSE}\right) \tag{48}$$

In the formula, MAX_i represents the maximum value of the image color, and 8-bit sampling points represent 255. MSE is the mean square error between plaintext and ciphertext images.

Structure similarity index measure (SSIM) [42] means structural similarity, which is one of the indicators used to measure image quality and is also

Table 2 Mean square error analysis

Image	MSE
Original image of "wrist"-Key 1 Encryption graph	13773
Original image of "wrist"-Key 2 failed decryption diagram	13661
Key 1 Encryption graph-Key 2 failed decryption diagram	10908
Original picture of "foot"-Key 1 Encryption graph	13540
Original picture of "foot"-Key 2 failed decryption diagram	13463
Key 1 Encryption graph-Key 2 failed decryption diagram	10873
Original picture of "skull"-Key 1 Encryption graph	16487
Original picture of "skull"-Key 2 failed decryption diagram	16528
Key 1 Encryption graph-Key 2 failed decryption diagram	10910
Original picture of "thorax"-Key 1 Encryption graph	9072
Original picture of "thorax"-Key 2 failed decryption diagram	9060
Key 1 Encryption graph-Key 2 failed decryption diagram	10861

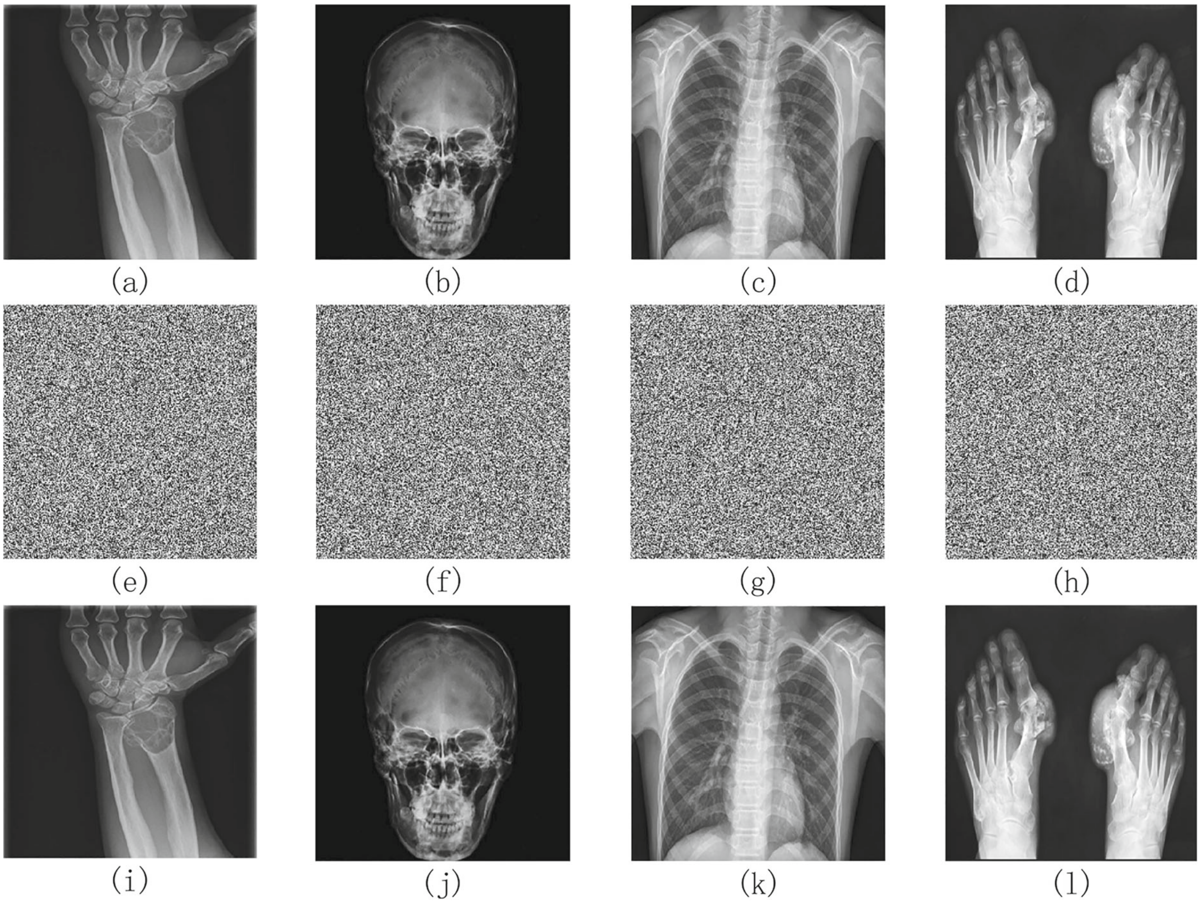


Fig. 12 Experimental results: **a** plain-image of "wrist", **b** plain-image of "skull", **c** plain-image of "thorax", **d** plain-image of "foot", **e** cipher-image of "wrist", **f** cipher-image of "skull", **g** cipher-image of "thorax", **h** cipher-image of "foot", **i** decryptionimage of "wrist", **j** decryption-image of "skull", **k** decryption-image of "thoraxand", **l** decryption-image of "foot"

a full-reference image quality evaluation indicator. It measures image similarity from three aspects of brightness, contrast and structure. Given two images x and y, their structural similarity can be defined as:

$$SSIM(x,y) = \frac{\left(2\mu_x\mu_y + C_1\right)\left(2\mu\sigma_x\sigma_y + C_2\right)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)} \tag{49}$$

The range of SSIM is $[0, 1]$, the larger the value, the better the image quality. When the two images are the same, $SSIM = 1$. Record the SSIM value between the plaintext image and the ciphertext image as $SSIM(a)$, and the SSIM value between the plaintext image and the decrypted image as $SSIM(b)$. The calculation results are shown in Table 5. It can be seen that the two fusion algorithms proposed in this paper are lossless decryption.

4.7 Differential attack

Differential attack is a chosen plaintext attack, by finding plaintext pairs with specific and non-random properties, changing their pixel values, and comparing the differences according to the different encrypted images generated by the former, so as to obtain the most likely key. Differential cryptanalysis is the most basic method of cryptanalysis, and it is also one of the important indicators to measure the security of a block cipher. The differential attack is mainly evaluated by the value of the Number of pixels change rate (NPCR) [45] and the Unified average change intensity(UACI) [46]. The correlation coefficient formula is described as follows:

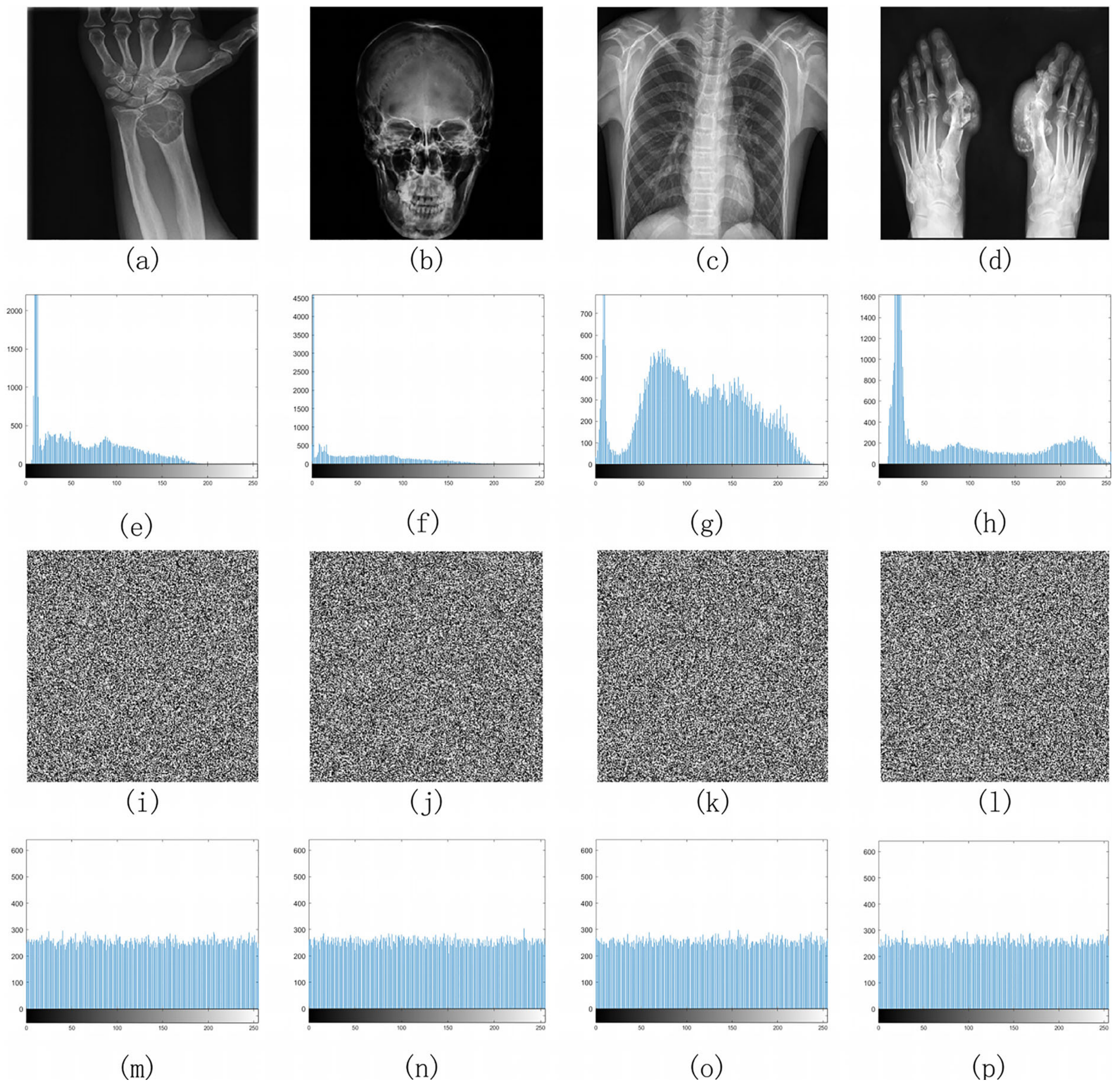


Fig. 13 Histogram analysis: **a–d** are plaintext images of "wrist", "skull", "thorax", and "foot", **e–h** are the plain-text histograms of "wrist", "skull", "thorax", and "foot", **i–1** are ciphertext images of "wrist", "skull", "thorax", and "foot", **m–p** are ciphertext histograms of "wrist", "skull", "thorax", and "foot"

$$NPCR = \frac{1}{M^2}\sum\nolimits_{i=1}^{M}\sum\nolimits_{j=1}^{M} D(i,j) \times 100\% \tag{50}$$

$$UACI = \frac{1}{M^2}\sum\nolimits_{i=1}^{M}\sum\nolimits_{j=1}^{M} \frac{|CI_1(i,j) - CI_2(i,j)|}{255} \times 100\% \tag{51}$$

where $CI_1(i,j)$ and $CI_2(i,j)$ denote two ciphertext images after changing pixel values in the same plaintext image. $D(i,j)$ is defined as follows:

$$D(i,j) = \begin{cases} 0 & if\ CI_1(i,j) = CI_2(i,j) \\ 1 & if\ CI_1(i,j) \neq CI_2(i,j) \end{cases} \tag{52}$$

For the password image mentioned in this paper, the NPCR and UACI values are calculated and shown in Table 6 (Theoretical values of NPCR and UACI are 99.6094% and 33.4635% respectively):

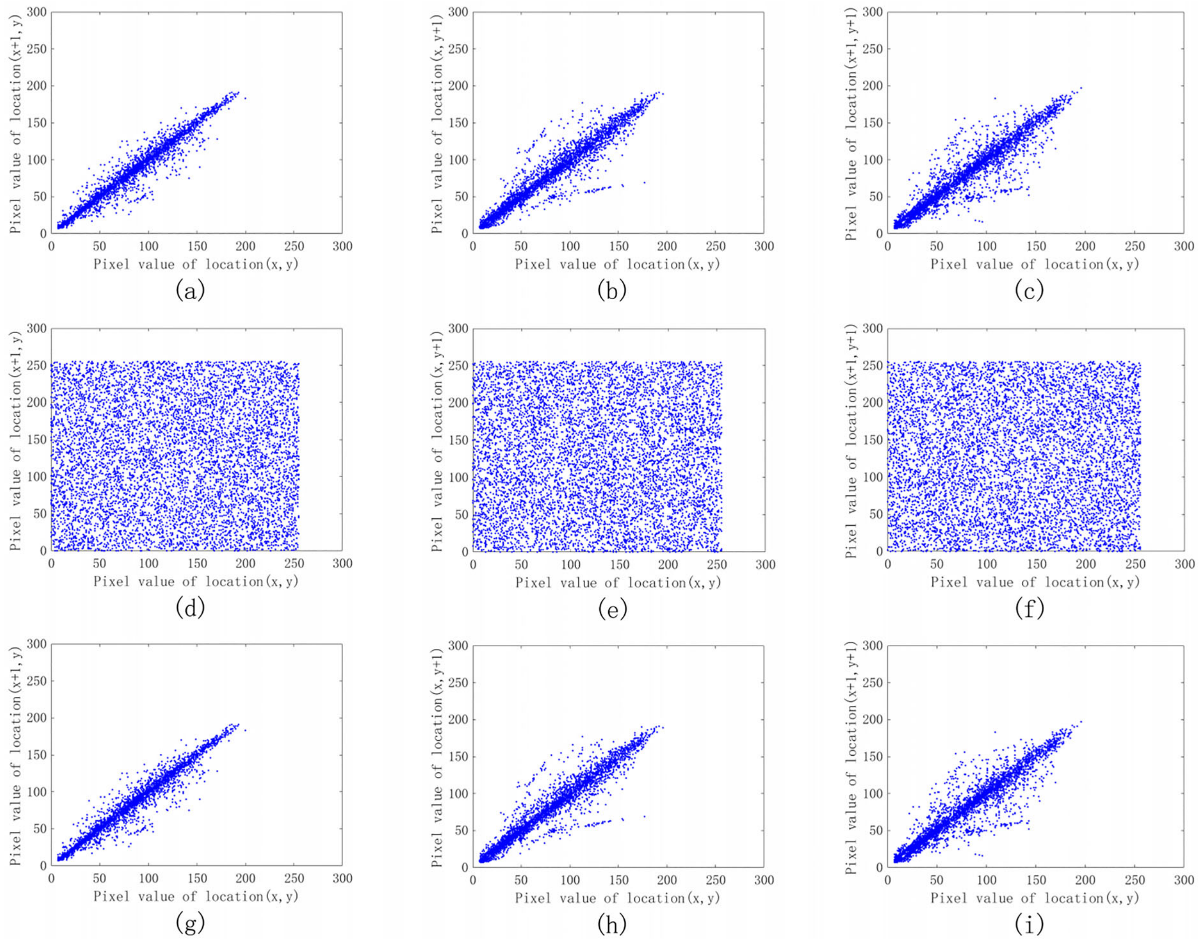


Fig. 14 The correlation plots of "wrist" image: **a** horizontal corre-lation of plain-image, **b** horizontal correlation of cipher-image, **c** horizontal correlation of decrypted image, **d** vertical correlation otplain-image, **e** vertical correlation of cipher-image, **f** vertical cor-relation of decrypted image, **g** diagonal correlation of plain-imagc, **h** diagonal correlation of cipher-image, **i** diagonal correlation ofdecrypted image

4.8 Four classic attack types

Cryptography is a security mechanism used to store and transmit sensitive data. It aims to study how to transmit information safely and confidentially, and can also effectively prevent potential attacks, and is not easy to be stolen, interpreted or tampered with by adversaries. Password attack is a method for attackers to brute force decryption of ciphertext, encryption key and other related encrypted content, aiming to grasp the defects in the encryption algorithm or encryption key, so as to crack the encrypted sensitive data and reduce the security of transportation. In cryptography, there are four classical types of attacks [50]:

1. known plaintext attack(KPA): The attacker knows the given plaintext and the corresponding ciphertext, which can be any non-empty subset (Known plaintext pairs), to derive the key and encryption algorithm.
2. Chosen plaintext attack(CPA): In addition to knowing the encryption algorithm, the attacker can also arbitrarily obtain the plaintext and the corresponding ciphertext that he thinks is beneficial to the attack, and the target is the pushout key.
3. Ciphtext only attack(COA): The attacker knows part of the ciphertext and the encryption algorithm, and uses all the keys to analyze these ciphertexts in turn. In general, the attacker uses brute-force to finally find out the plaintext or the key.

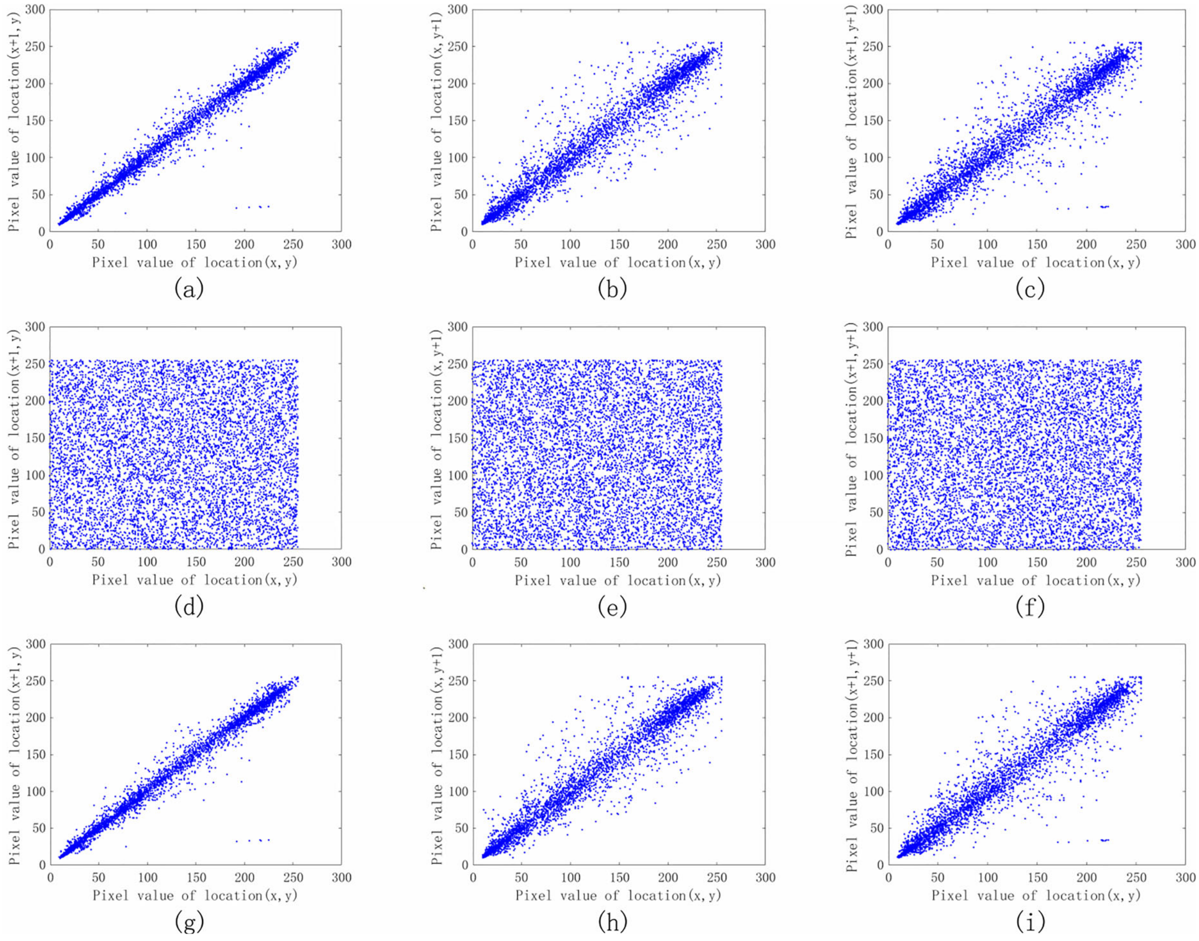


Fig. 15 The correlation plots of "foot" image: **a** horizontal correlation of plain-image, **d** horizontal correlation of cipher-image, **g** horizontal correlation of decrypted image, **b** vertical correlation olplain-image, **e** vertical correlation of cipher-image, **h** vertical correlation of decrypted image, **c** diagonal correlation of plain-image, **f** diagonal correlation of cipher-image, **i** diagonal correlation ofdecrypted image

Table 4 Correlation coefficients of the cipher-images

	Horizontal	Vertical	Diagonal
"Wrist"	− **0.0007**	0.0013	− 0.0085
"Skull"	− 0.0007	**0.0012**	**0.0004**
"Thorax"	− 0.0009	0.0028	− 0.0147
"Foot"	− 0.0008	0.0182	− 0.0021
[39]	0.0047	0.0031	0.0018
[40]	− 0.0455	0.0109	0.0228
[30]	0.0627	0.2557	0.0203

Table 5 PSNR and SSIM for the cipher-image

	PSNR	SSIM (a)	SSIM (b)
"Wrist"	6.7407	0.0055	1
"Skull"	**5.9595**	**0.0042**	1
"Thorax"	8.5534	0.0088	1
"Foot"	6.8148	0.0064	1
Average	7.0171	0.0062	1
[43]	7.5974	0.0064	–
[44]	8.6690	0.0102	–
[4]	8.5950	0.0124	–

4. Chosen ciphertext attack(CCA): Knowing the decryption algorithm, the attacker can choose any ciphertext and obtain the decrypted plaintext, and the target is the pushout key.

In 2012, Xingyuan Wang [51] put forward the conclusion: Obviously, chosen plaintext attack is the most powerful attack. If a cryptosystem can resist this attack, it canresist other types of attack. In the dynamic diffusion phase of the encryption algorithm proposed in this thesis, we use the plaintext information σ to generate the control parameters required to control the diffusion operation. This makes the diffusion operation associated with the plaintext image, which means that even if the plaintext image changes slightly, the diffusion process in the encryption algorithm will have different diffusion results, which is sufficient to resist the chosen plaintext attack. Therefore, the encryption algorithm proposed in this thesis has extremely high security and can effectively resist the above four attacks.

4.9 Anti-noise test analysis

In practical applications, digital images are usually affected by noise when they are broadcast on communication channels [52]. In order to test the noise resistance of the improved scheme in this paper, it is assumed that the encrypted image is affected by salt and pepper noise with densities of 0.05, 0.1, 0.15, and 0.2, and the corresponding decrypted image is shown in Fig. 16. It can be seen from the figure that the different decrypted images are noisy, but the important information of the original image can still be distinguished, so it can be concluded that the improved scheme can resist noise attacks.

4.10 Cropping attacks analysis

The image encrypted by chaotic system has good encryption effect, which makes the attacker unable to obtain effective information. Therefore, the attacker may break the integrity of the encrypted image [53], so that the receiver cannot decrypt the original image smoothly. Therefore, it is particularly important to know whether the encryption scheme has the ability to resist the shearing attack. In this thesis the encrypted image is cropped by the size of $1/4$ and $1/3$ of the original image, and the pixel value after cropping is set to zero, and the decryption results are shown in Figs. 17 and 18. By observing the quality of the decrypted image, it can be seen that the algorithm can effectively resist the cropping attack and recover the original image to a certain extent, so that the receiver can still identify the approximate content of the original image.

Table 6 UACI and NPCR performances

	NPCR	UACI
"Wrist"	**99.6094**	33.2683
"Skull"	99.6033	33.3160
"Thorax"	99.6582	**33.4364**
"Foot"	99.6017	33.3379
Average	99.6182	33.3397
[47]	99.5651	30.9132
[48]	99.6329	33.5899
[49]	99.6184	33.3974

4.11 Complexity analysis

The size of the plaintext image used in this paper is $M \times N$ and let n indicate the quantity of pixels inside the image. The complexity of the encryption algorithm proposed in this paper can be calculated by the operations discussed below. These operations include generating pairs of horizontal and vertical coordinates in a chaotic exchange table, dynamic rotation scrambling, index scrambling, filtered diffusion, and dynamic diffusion. The complexity of generating the horizontal and vertical coordinate pairs in the chaotic exchange table is $O(2n^2)$. Dynamic rotation scrambling consists of two parts: intra-block scrambling and inter-block scrambling, and its complexity is $O(4n^2)$. The complexity of indexed disruption, filtered diffusion and dynamic diffusion are $O(n)$, $O(n^2)$ and $O(3n)$ respectively. Therefore, the overall complexity of the image encryption scheme proposed in this paper is $O(4n + 7n^2)$, which is far less than the $O(78n^2)$ in the literature [54].

4.12 Time cost analysis

The time cost analysis [55] is usually the time required to test a real encryption/decryption run of an algorithm in a simulation platform. Because it can theoretically prove the feasibility of the proposed image encryption algorithm in efficiency, the analysis of the time cost of the encryption algorithm has become one of the important indicators to measure the performance of the encryption algorithm. A good encryption algorithm should take as little time as possible. Table 7

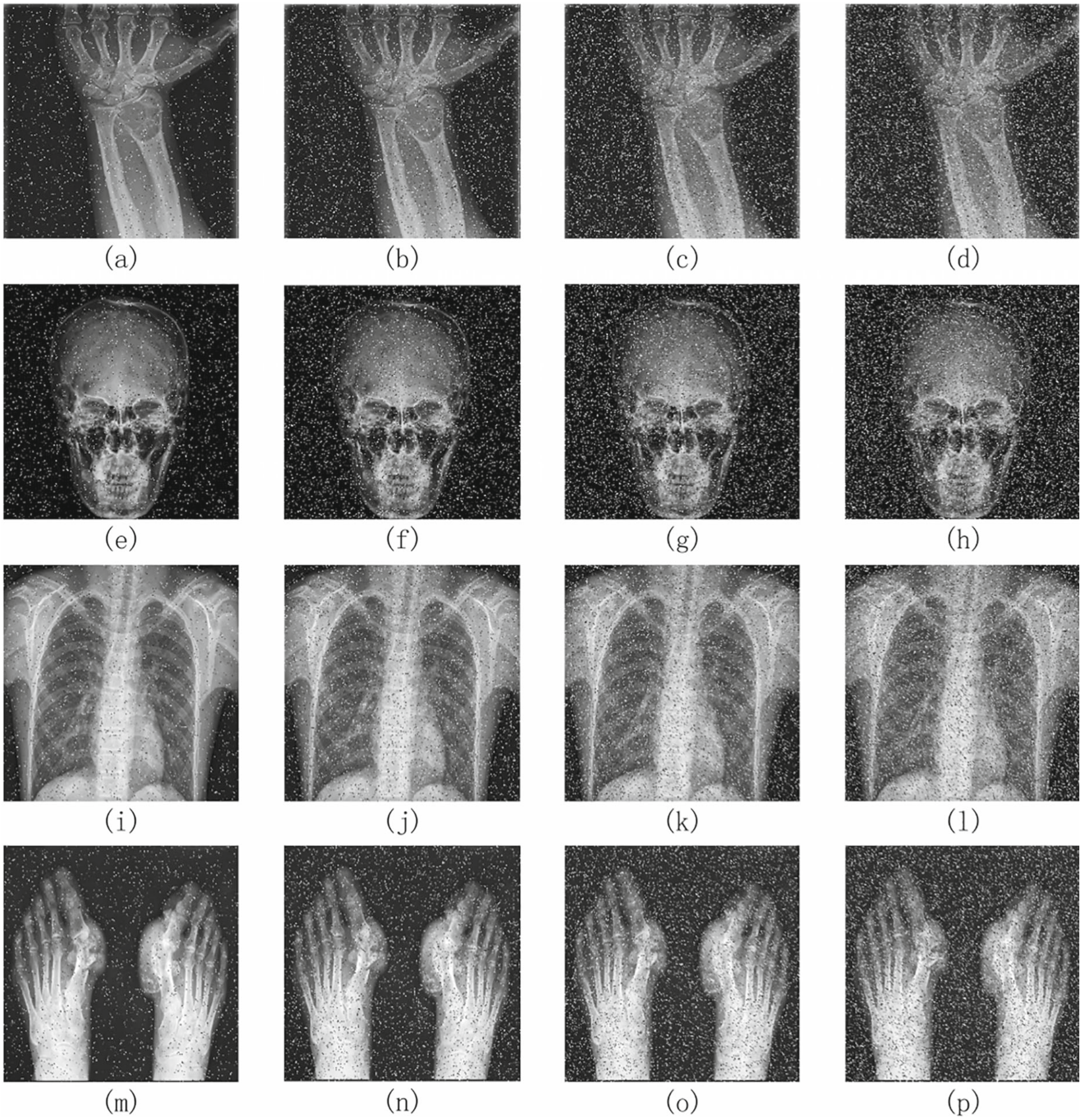


Fig. 16 Anti-noise test analysis: The first row are the “wrist” decryptimages with 0.05, 0.10, 0.15 and 0.20 salt and pepper noise respec-tively. The second row are the “skull” decrypt images with 0.05, 0.10.0.15 and 0.20 salt and pepper noise respectively. The third row arethe “thorax” decrypt images with 0.05, 0.10, 0.15 and 0.20 salt andpepper noise respectively. The forth row are the “foot” decrypt imageswith 0.05.0.10, 0.15 and 0.20 salt and pepper noise respectively

presents the comparison of the encryption time. Through the comparison, it can be concluded that the proposed encryption algorithm requires less time overhead.

5 Conclusion

This paper proposes a dynamic rotation medical image encryption scheme based on improved Lorenz chaos, the improved Lorenz chaotic system has a wider range of chaotic parameters and better chaotic

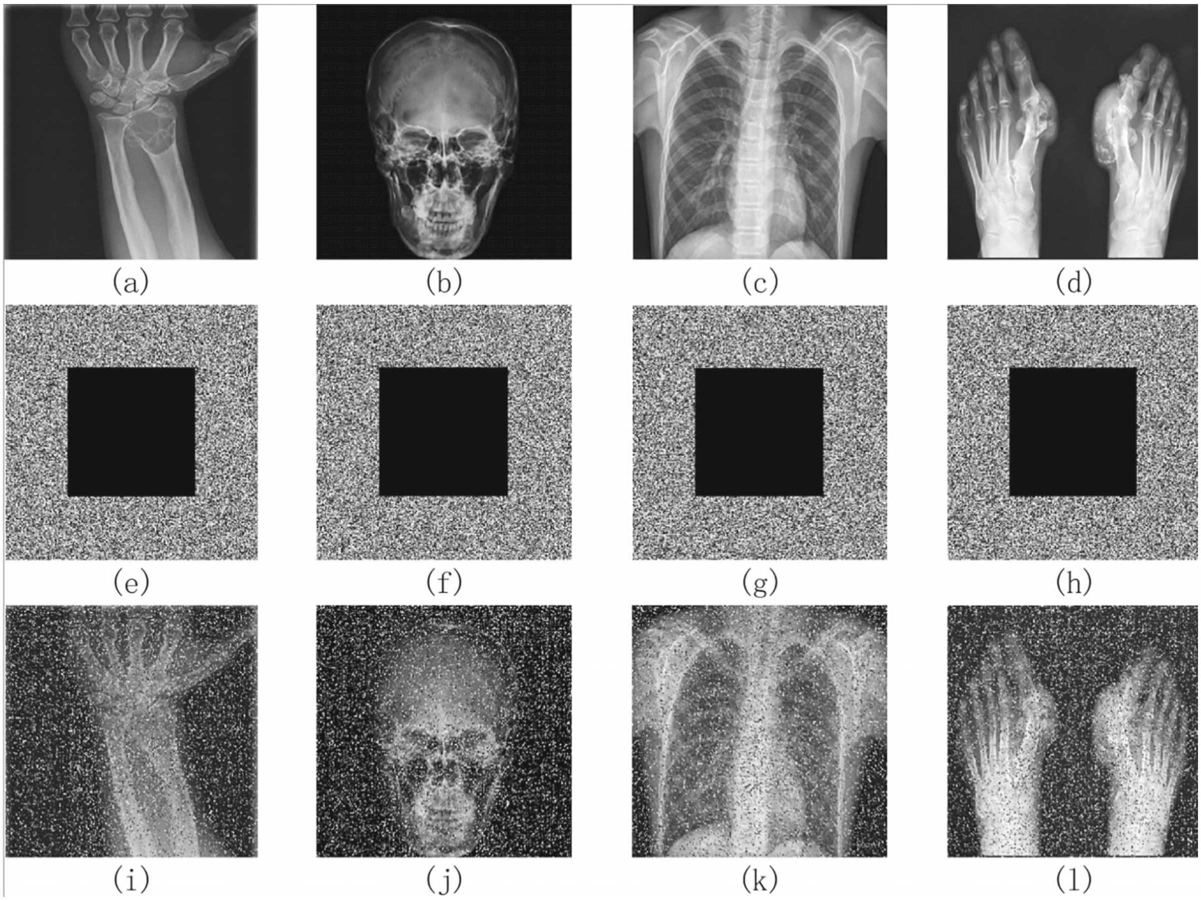


Fig. 17 Cropping attacks analysis: **a–d** as the “wrist”, “skull”, “chest”, “feet” plaintext image, **e–h** for cutting a quarter of the “wrist”, “skull”, “chest”, “feet” ciphertext image, **i–l** for cutting a quarter of the “wrist”, “skull” “chest” “feet” decrypted image

characteristics. It is further proved that the improved chaotic system can be used as an encryption key generator by proposing a dynamic round-robin scrambling and double-diffusion algorithm. In the proposed dynamic rotation scrambling algorithm, the pixel exchange threshold is added, which can effectively improve the scrambling effect. The combination of filter diffusion and dynamic diffusion ensures the security of medical image encryption algorithm. Experimental simulation and performance analysis show the effectiveness of the proposed encryption scheme. The shortcoming of this paper is that the test results of UACI are not close enough to the ideal value. The future work includes three aspects: First, on the premise of ensuring the parameter range of the improved Lorenz chaotic system, different from other improved chaotic algorithms, a new hyperchaotic Lorenz chaotic system will be proposed. Second, the existing dynamic round-robin scrambling algorithm is simplified to improve the scrambling efficiency. Third, an efficient diffusion algorithm will be proposed and combined with the chaotic system, so as to effectively reconcile the difference between two ciphertext images encrypted from the same plaintext image. So as to improve the NPCR, UACI and other performance analysis test results, so that the test results are closer to the ideal value.

Funding The research work of this article is partiallyfunded by the National Natural Science Foundation of China project (61772249). Basic Research Project of Liaoning Provincial Department of Education (JYTQN2023208). Soft Science Research Program of Huludao Science and Technology Bureau (2023JH (1)4/03*b*).

Data availability The data that support the findings of thisstudy are available from the corresponding author uponreasonable request.

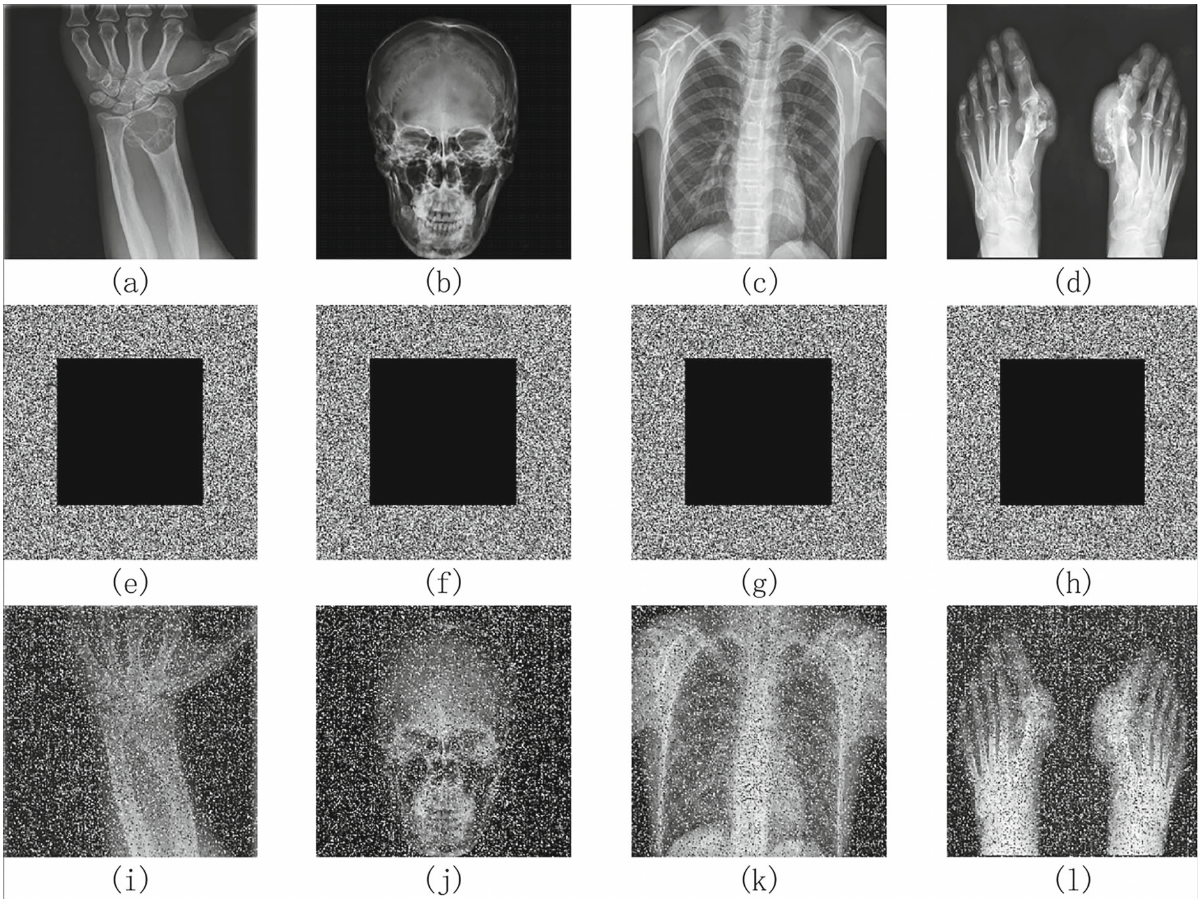


Fig. 18 Cropping attacks analysis: **a–d** as the "wrist", "skull", "chest", "feet" plaintext image, **e–h** for cutting a third of the "wrist", "skull", "chest", "feet" ciphertext image, **i–l** for cutting a third of the "wrist", "skull" "chest" "feet" decrypted image

Table 7 Time cost analysis

	Encryption time (s)	Decryption time (s)
"Wrist"	**0.274965**	**0.083769**
"Skull"	0.276108	0.084757
"Thorax"	0.296967	0.086027
"Foot"	0.276366	0.085994
Average	0.281102	0.085137
[55]	20.432300	–
[56]	17.627770	–

Declarations

Conflict of interest The authors declare that they haveno conflict of interest.

References

1. Man, Z., Li, J., Di, X.: Medical image encryption scheme based on self-verification matrix. IET Image Proc. **15**(12), 2787–2798 (2021)
2. Rajagopalan, S., Janakiraman, S., Rengarajan, A.: Medical data security for bioengineers. In: Butta Singh, Barjinder Singh Saini (eds) Medical image encryption: microcontroller and FPGA perspective, pp. 278–304. IGI Global, Pennsylvania (2019)
3. Wu, Y., Zhang, L., Berretti, S., Wan, S.: Medical image encryption by content-aware dna computing for secure healthcare. IEEE Trans. Industr. Inf. **19**(2), 2089–2098 (2022)
4. Wang, T., Ge, B., Xia, C., Dai, G.: Multi-image encryption algorithm based on cascaded modulation chaotic system and block-scrambling-diffusion. Entropy **24**(8), 1053–1076 (2022)
5. Liu, J., Ma, Y., Li, S., Lian, J., Zhang, X.: A new simple chaotic system and its application in medical image encryption. Multimed Tools Appl. **77**, 22787–22808 (2018)

6. Khan, J. S., Ahmad, J., Abbasi, S. F., Kayhan, S. K. et al: DNA sequence based medical image encryption scheme, In: 2018 10th computer science and electronic engineering (CEEC). IEEE, pp. 24–29. (2018)
7. Arunkumar, S., Subramaniyaswamy, V., Vijayakumar, V., Chilamkurti, N., Logesh, R.: Svd-based robust image steganographic scheme using riwt and dct for secure transmission of medical images. Measurement **139**, 426–437 (2019)
8. Zhou, J., Li, J., Di, X.: A novel lossless medical image encryption scheme based on game theory with optimized roi parameters and hidden roi position. IEEE Access **8**, 122210–122228 (2020)
9. Benssalah, M., Rhaskali, Y.: A secure dicom image encryption scheme based on ecc, linear cryptography and chaos, In: 2020 1st international conference on communications, control systems and signal processing (CCSSP). IEEE, pp. 131–136, (2020)
10. Boussif, M., Aloui, N., Cherif, A.: Securing dicom images by a new encryption algorithm using arnold transform and vigenère cipher. IET Image Proc. **14**(6), 1209–1216 (2020)
11. Ajili, S., Hajjaji, M.A., Mtibaa, A.: Cryptowatermarking algorithm using weber's law and aes: a view to transfer safe medical image. Sci. Program. **2021**, 1–22 (2021)
12. Kamal, S.T., Hosny, K.M., Elgindy, T.M., Darwish, M.M., Fouda, M.M.: A new image encryption algorithm for grey and color medical images. IEEE Access **9**, 37855–37865 (2021)
13. El-Shafai, W., Khallaf, F., El-Rabaie, E.-S.M., El-Samie, F.E.A.: Proposed 3d chaos-based medical image cryptosystem for secure cloud-iomt ehealth communication services. J. Ambient. Intell. Humaniz. Comput. **15**(9), 1–28 (2022)
14. Man, Z., Li, J., Di, X., Sheng, Y., Liu, Z.: Double image encryption algorithm based on neural network and chaos. Chaos Solitons Fractals **152**, 111318–111334 (2021)
15. Sun, X., Shao, Z., Shang, Y., Liang, M., Yang, F.: Multiple-image encryption based on cascaded gyrator transforms and high-dimensional chaotic system. Multimed Tools Appl. **80**, 15825–15848 (2021)
16. ul Haq, T., Shah, T.: 4d mixed chaotic system and its application to rgb image encryption using substitution diffusion. J. Inf. Secur. Appl. **61**, 102931–102943 (2021)
17. Chamoli, A., Ahmed, J., Alam, M.A., Alankar, B.: A diffusion model based on the features of the 3d chaotic baker map for image encryption. Int. J. Intell. Syst. Appl. Eng. **11**(5s), 173–180 (2023)
18. Wang, L., Cao, Y., Jahanshahi, H., Wang, Z., Mou, J.: Color image encryption algorithm based on double layer josephus scramble and laser chaotic system. Optik **275**, 170590–170603 (2023)
19. Yin, S., Li, H.: Gsapso-mqc: medical image encryption based on genetic simulated annealing particle swarm optimization and modified quantum chaos system. Evol. Intel. **14**, 1817–1829 (2021)
20. Lai, Q., Zhang, H., Kuate, P.D.K., Xu, G., Zhao, X.-W.: Analysis and implementation of no-equilibrium chaotic system with application in image encryption. Appl. Intell. **52**(10), 11448–11471 (2022)
21. Hu, M., Li, J., Di, X.: Quantum image encryption scheme based on 2d s ine 2-l ogistic chaotic map. Nonlinear Dyn. **111**(3), 2815–2839 (2023)
22. Singh, K.N., Singh, O., Singh, A.K., Agrawal, A.K.: Eimol: a secure medical image encryption algorithm based on optimization and the lorenz system. ACM Trans. Multimed. Comput. Commun. Appl. **19**(2s), 1–19 (2023)
23. Trujillo-Toledo, D., López-Bonilla, O., García-Guerrero, E., Esqueda-Elizondo, J., Cárdenas-Valdez, J., Tamayo-Pérez, U., Aguirre-Castro, O., Inzunza-González, E.: Real-time medical image encryption for h-iot applications using improved sequences from chaotic maps. Integration **90**, 131–145 (2023)
24. de Pedro-Carracedo, J., Ugena, A.M., GonzalezMarcos, A.P.: Dynamical analysis of biological signals with the 0–1 test: a case study of the photoplethysmographic (ppg) signal. Appl. Sci. **11**(14), 6508–6527 (2021)
25. Hou, W., Li, S., He, J., Ma, Y.: A noval image-encryption scheme based on a non-linear cross-coupled hyperchaotic system with the dynamic correlation of plaintext pixels. Entropy **22**(7), 779–800 (2020)
26. Zhao, X., Liu, J., Liu, H., Zhang, F.: Dynamic analysis of a one-parameter chaotic system in complex field. IEEE Access **8**, 28774–28781 (2020)
27. Gao, S., Wu, R., Wang, X., Wang, J., Li, Q., Wang, C., Tang, X.: A 3d model encryption scheme based on a cascaded chaotic system. Signal Process. **202**, 108745–108758 (2023)
28. Yu, F., Gong, X., Li, H., Wang, S.: Differential cryptanalysis of image cipher using block-based scrambling and image filtering. Inf. Sci. **554**, 145–156 (2021)
29. Hua, Z., Zhou, Y.: Design of image cipher using block-based scrambling and image filtering. Inf. Sci. **396**, 97–113 (2017)
30. Lin, H., Wang, C., Cui, L., Sun, Y., Xu, C., Yu, F.: Brain-like initial-boosted hyperchaos and application in biomedical image encryption. IEEE Trans. Industr. Inf. **18**(12), 8839–8850 (2022)
31. Hu, X., Wei, L., Chen, W., Chen, Q., Guo, Y.: Color image encryption algorithm based on dynamic chaos and matrix convolution. IEEE access **8**, 12452–12466 (2020)
32. Lin, H., Wang, C., Cui, L., Sun, Y., Zhang, X., Yao, W.: Hyperchaotic memristive ring neural network and application in medical image encryption. Nonlinear Dyn. **110**(1), 841–855 (2022)
33. Deepika, J., Rajan, C., Senthil, T.: Security and priacy of cloud-and iot-based medical image diagnosis using fuzzy convolutional neural network. Comput. Intell. Neurosci. **2021**, 1–17 (2021)
34. Akkasaligar, P.T., Biradar, S.: Selective medical image encryption using dna cryptography. Inf. Secur. J. Glob. Perspect. **29**(2), 91–101 (2020)
35. Shafique, A., Ahmed, J., Rehman, M.U., Hazzazi, M.M.: Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain. IEEE Access **9**, 59108–59130 (2021)
36. Heidari, S., Naseri, M., Nagata, K.: Quantum selective encryption for medical images. Int. J. Theor. Phys. **58**, 3908–3926 (2019)
37. Ding, Y., Tan, F., Qin, Z., et al.: Deepkeygen: a deep learning-based stream cipher generator for medical image

encryption and decryption. IEEE Trans. Neural Netw Learn. Syst. **33**(9), 4915–4929 (2021)

38. Gafsi, M., Abbassi, N., Hajjaji, M.A., Malek, J., Mtibaa, A.: Improved chaos-based cryptosystem for medical image encryption and decryption. Sci. Program. **2020**, 1–22 (2020)
39. Abdelfatah, R.I., Saqr, H.M., Nasr, M.E.: An effficient medical image encryption scheme for (wban) based on adaptive dna and modern multi chaotic map. Multimed. Tools Appl. **82**(14), 22213–22227 (2023)
40. Chen, Y., Tang, C., Ye, R.: Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process. **167**, 107286–107298 (2020)
41. Chen, X., Hu, C.J.: Adaptive medical image encryption algorithm based on multiple chaotic mapping. Saudi J. Biol. Sci. **24**(8), 1821–1827 (2017)
42. Panwar, K., Singh, A., Kukreja, S., Singh, K.K., Shakhovska, N., Boichuk, A.: Encipher gan: an end-to-end color image encryption system using a deep generative model. Systems **11**(1), 36–51 (2023)
43. Rajagopalan, S., Poori, S., Narasimhan, M., Rethinam, S., Vallipalayam Kuppusamy, C., Balasubramanian, R., V. Moorthi Paramasivam Annamalai, A. Rengarajan,: Chua's diode and strange attractor: a three-layer hardware–software co-design for medical image confidentiality. IET Image Process. **14**(7), 1354–1365 (2020)
44. Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M., Qin, Z.: DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. IEEE Internet Things J. **8**(3), 1504–1518 (2020)
45. Wu, Y., Noonan, J.P., Agaian, S., et al.: NPCR and UACI randomness tests for image encryption. Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun **1**(2), 31–38 (2011)
46. Srinivasu, P.N., Norwawi, N., Amiripalli, S.S., Deepalakshmi, P.: Secured compression for 2d medical images through the manifold and fuzzy trapezoidal correlation function. Gazi Univ. J. Sci. **35**(4), 1372–1391 (2021)
47. Abdelfattah, R. I., Mohamed, H., Nasr. M. E.: Secure image encryption scheme based on dna and new multi chaotic map, In: Journal of physics: conference series, IOP Publishing, vol. 1447, no. 1, pp. 012053–012065. (2020)
48. John, S., Kumar, S.: 2d lorentz chaotic model coupled with logistic chaotic model for medical image encryption: towards ensuring security for teleradiology. Proced. Comput. Sci. **218**, 918–926 (2023)
49. Abd-Elhafiez, W.M., Heshmat, M.: Medical image encryption via lifting method. J. Intell. Fuzzy Syst. **38**(3), 2823–2832 (2020)
50. Benssalah, M., Rhaskali, Y., Drouiche, K.: An effficient image encryption scheme for tmis based on elliptic curve integrated encryption and linear cryptography. Multimed. Tools Appl **80**(2), 2081–2107 (2021)
51. Wang, X., Teng, L., Qin, X.: A novel colour image encryption algorithm based on chaos. Signal Process. **92**(4), 1101–1108 (2012)
52. Wang, X., Yin, S., Shafiq, M., Laghari, A.A., Karim, S., Cheikhrouhou, O., Alhakami, W., Hamam, H.: A new v-net convolutional neural network based on four dimensional hyperchaotic system for medical image encryption. Secur. Commun. Netw. **2022**, 1–14 (2022)
53. Rani, N., Mishra, V., Sharma, S.R.: Image encryption model based on novel magic square with differential encoding and chaotic map. Nonlinear Dyn. **111**(3), 2869–2893 (2023)
54. ElKamchouchi, D.H., Mohamed, H.G., Moussa, K.H.: A bijective image encryption system based on hybrid chaotic map diffusion and dna confusion. Entropy **22**(2), 180–198 (2020)
55. Yousif, N.A., Mahdi, G.S., Hashim, A.T.: Medical image encryption based on frequency domain and chaotic map. Int. J. Saf. Secur. Eng. **12**(4), 467–473 (2022)
56. Zhu, H., Dai, L., Liu, Y., et al.: A three-dimensional bit-level image encryption algorithm with Rubik's cube method. Math. Comput. Simul **185**, 754–770 (2021)

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