Advances in Differential Equations and Control Processes 2025, 32(4), 3511.
doi: https://doi.org/10.59400/adecp3511

Article

A ROI-based medical image encryption scheme using improved Lorenz chaotic system, hybrid pixel-bit permutation, and SHA-256 hashing

Huiqing Wu, Xiaohong Wang*

Shandong University of Engineering and Vocational Technology, Jinan 250200, China
*** Corresponding author:** Xiaohong Wang, sdgc_wxh@suet.edu.cn

CITATION

Wu H, Wang X. A ROI-based medical image encryption scheme using improved Lorenz chaotic system, hybrid pixel-bit permutation, and SHA-256 hashing. 2025; 32(4): 3511. https://doi.org/10.59400/adecp3511

ARTICLE INFO

Received: 8 July 2025
Revised: 5 August 2025
Accepted: 23 September 2025
Available online: 13 October 2025

Abstract: Medical images contain highly sensitive diagnostic and personal information that requires robust protection during storage and transmission. To address this, we propose a region-of-interest (ROI)-based hybrid encryption algorithm that combines pixel-level and bit-level permutation with bit-wise diffusion driven by an improved Lorenz chaotic system. The scheme first employs a robust ROI perception mechanism to accurately identify diagnostically important areas while avoiding unnecessary processing of non-critical regions, thereby enhancing computational efficiency and security. Image-dependent SHA-256 hashing is integrated to generate keystreams tightly bound to image content, improving key sensitivity and resisting plaintext attacks. Dual-layer chaotic scrambling ensures both global confusion and local diffusion, while a dedicated bit-wise diffusion stage further randomizes the ciphertext, strengthening resistance against differential, statistical, and noise-based attacks. Experimental evaluations demonstrate that the proposed method achieves high security and robustness: the average information entropy of encrypted images reaches 7.9992, and NPCR and UACI values are 99.63% and 33.47%, respectively. Compared with existing encryption techniques, the proposed algorithm exhibits higher randomness, stronger differential attack resistance, and better protection of sensitive medical data, without embedding ROI location metadata into non-interest regions. The results indicate that this approach provides an efficient and secure framework for safeguarding medical images in telemedicine, healthcare information systems, and other critical applications.

Keywords: medical image encryption; region of interest (ROI); improved Lorenz chaotic system; hybrid pixel-bit permutation; SHA-256 hashing; bit-wise diffusion; differential attack resistance

1. Introduction

In recent years, the intersection of chaotic dynamics and control theory has provided new paradigms for secure communications and information encryption. Chaotic systems, especially those modeled by nonlinear differential equations, exhibit sensitivity to initial conditions, ergodicity, and complex attractor behavior. These features are well-suited for designing robust encryption frameworks. Among them, the Lorenz system merged as a classical model widely used in dynamic key generation, owing to its simplicity and strong chaotic properties [1].

Classic studies such as Pecora and Carroll's work on chaos synchronization [2] and Chen's monograph on chaos control [3] laid the groundwork for linking chaos with secure system design. More recent developments have further extended this foundation

through adaptive control, sliding mode control, and observer-based synchronization approaches. These techniques have contributed to enhanced resilience in chaotic cryptosystems [4–6]. These studies reinforce the role of differential equation modeling in enabling control-oriented encryption strategies.

With the rapid development of the Internet, along with the widespread application of big data, 5G, and cloud computing have been deeply integrated into all aspects of society, profoundly transforming production methods and lifestyles. These computer-based information technologies have greatly advanced the intelligent development of modern systems and provided strong technical support for rapid societal progress [7–9]. As communication technologies continue to advance, multimedia content such as text, images, video, and audio has become a central medium for information exchange in daily life. In particular, in fields such as military defense, telemedicine, aviation communication, meteorological monitoring, commercial finance, and government administration, image data often contains highly sensitive information. Unauthorized disclosure may lead to severe security threats and significant harm to individual or organizational interests.

Cryptography is a core technology for ensuring information security. It protects data confidentiality, integrity, authenticity, and non-repudiation through techniques such as encryption, message authentication, identity verification, and digital signatures [10–13]. Historically, early cryptographic systems were based on limited keys and simple substitution due to technical constraints. With the development of computer and electronic communication technologies, modern cryptography has emerged, enabling the widespread use of advanced algorithms. Well-known standards such as DES [14], AES [15], and the asymmetric RSA algorithm [16] have achieved broad success in text encryption. However, unlike textual data, digital images typically contain a large amount of repetitive information and exhibit strong local dependency among neighboring pixels, which limits the effectiveness of conventional encryption algorithms in ensuring their security. To overcome these limitations, chaos-based encryption techniques have emerged as a widely explored solution [17–20]. One representative approach is the method introduced by Enayatifar et al. [21], which integrates DNA-based computation with cellular automata and utilizes a 2D Tinkerbell chaotic map to enhance encryption performance. Recent advances have explored hardware-friendly and high-complexity chaotic generators as well as content-aware and selective schemes for image and video encryption. For example, Gao et al. proposed a 3D memristive cubic map that integrates discrete memristors and demonstrates both strong chaotic dynamics and feasible hardware implementation for image encryption [22]. Parallel and neuron-inspired approaches have also been applied to improve throughput and robustness: a parallel color image encryption algorithm based on a 2D Logistic-Rulkov neuron map achieves channel-level parallelism and efficiency for color images [23].

Recently, the protection and secure transmission of medical images have become a growing research focus [24–28]. Unlike general-purpose images, medical images exhibit unique spatial and pixel distribution characteristics. Tissue or organ containing a lot of important information is usually distributed in the middle of the image, which

is the region of interest (ROI), which has higher requirements for confidentiality and security. In addition, it is a peripheral black background that almost contains no valid information, i.e., Region of Non-interest. When performing encryption on medical images, focusing selectively on the region of interest helps safeguard sensitive data and enhances overall security performance. Zhou et al. [29] divide the image into blocks, extract irregular ROI through the comparison result of block information entropy and threshold, and discuss the optimal value of block size and threshold by game theory, finally realize accurate encryption of ROI, protect the information of important regions, and do not deal with RONI. Similarly, Ping et al. [30] extracted ROI with accurate shape according to the block mean value of the image, and adopted the life cell-like automata with regular equilibrium to encrypt ROI and electronic medical record, and embedded the encrypted medical record information and ROI position information into RONI and ciphertext image respectively. Liu et al. [31] proposed two encryption modes: a full-encryption mode for all pixels and a semi-encryption mode where only the ROI is scrambled before global diffusion. In the video domain, selective encryption of critical regions using a 2D extended Schaffer function map combined with neural networks demonstrates the value of deep-learning-based ROI extraction and content-dependent key generation to resist chosen-plaintext attacks and to reduce computational load [32, 33].

Compared with these works, our scheme differs in three main aspects: we fuse a continuous-time chaotic generator with image-dependent SHA-256 hashing to produce keystreams tightly bound to image content; we combine pixel-level and bit-level permutation with a dedicated bit-wise diffusion stage to strengthen small-scale randomness; and we avoid explicit embedding of ROI-location metadata into RONI, thereby reducing leakage while still enabling deterministic ROI reconstruction. In summary, this work presents a medical image encryption scheme with three main contributions: (1) A novel medical image encryption scheme based on region-of-interest (ROI) perception is proposed, which fully leverages the structural characteristics of medical images to achieve targeted encryption of sensitive areas, improving both security and efficiency of the whole image. (2) A combination of pixel-level and bit-level permutation is designed using multiple keystreams generated from a Lorenz chaotic system and SHA-256, enhancing confusion and diffusion effects while preserving computational efficiency. (3) A bit-level diffusion mechanism driven by optimized chaotic sequences is introduced to further randomize the ciphertext, ensuring strong resistance to differential, statistical, and noise-based attacks.

The remaining of this paper is arranged as follows. Section 2 introduces the mathematical formulation and dynamic properties of the Lorenz chaotic system. Section 3 details the proposed method, including the extraction of ROI, keystream generation, and pixel- and bit-level scrambling and diffusion. Section 4 presents extensive simulation results and security analyses. Finally, Section 5 drives the conclusion.

2. Foundational knowledge

2.1. Lorenz system

The Lorenz system, originally derived from a simplified model of atmospheric convection, is a classic example of a continuous-time chaotic system governed by a set of coupled nonlinear ordinary differential equations. Mathematically, the Lorenz system is a nonlinear autonomous dynamical system described by the following set of first-order ordinary differential equations [34]:

$$\begin{cases} x = a(y - x) \\ y = x(c - z) - y \\ z = xy - bz \end{cases} \tag{1}$$

where a, b and c are positive constants that serve as system parameters. The system exhibits chaotic dynamics when these parameters are set to specific values, such as $a = 10$, $b = 8/3$ and $c = 28$. Due to its rich dynamic properties, the Lorenz system has been extensively used in control theory, cryptography, and secure communications as a prototype for studying chaos-based control and synchronization.

2.2. K-means clustering algorithm

Image segmentation is to divide an image into several non-overlapping areas so that the grayscale, color, texture and other features of the image are similar in the same area, and different areas show differences. Furthermore, areas with unique properties can be processed to extract targets of interest for different studies. Among various methods, the K-means algorithm offers a simple yet effective approach for clustering image pixels. As an unsupervised learning technique, it groups data based on similarity by minimizing intra-cluster variance. The algorithm begins by selecting k initial cluster centers at random. It then assigns each data point to the nearest center based on Euclidean distance, followed by iterative updates of the cluster centers until the grouping becomes stable or meets a convergence condition. Once all clusters have been assigned samples, new cluster centers are recalculated using methods such as the mean; if the cluster centers remain unchanged after several iterations of the above steps, the algorithm terminates, otherwise the process continues until convergence is achieved.

Applying the K-means algorithm to image segmentation essentially involves clustering pixels, ultimately resulting in k compact and distinct clusters. For medical images, setting the number of clusters to three can effectively separate the ROI from the background.

3. The proposed image encryption algorithm

The proposed encryption framework is fundamentally driven by a nonlinear chaotic dynamical system, namely the Lorenz system, which functions as a sensitive controller and keystream generator. Its evolving state trajectory is shaped by the system's initial values and control parameters, and further influenced by the image hash value generated through SHA-256. This interaction forms a dynamic control

mechanism that governs the scrambling and diffusion processes throughout the encryption pipeline.

This dynamical approach ensures that each encryption operation is uniquely determined by both the image content and the secret key. As a result, the scheme achieves high complexity, strong unpredictability, and robust resistance to known-plaintext and differential attacks. The adoption of a well-established chaotic system with intrinsic properties such as ergodicity, topological mixing, and sensitivity to initial conditions enables the encryption process to follow a controlled and secure evolution within the state space. These operations effectively disrupt pixel positions and values, producing a visually unintelligible encrypted image, as illustrated in **Figure 1**.

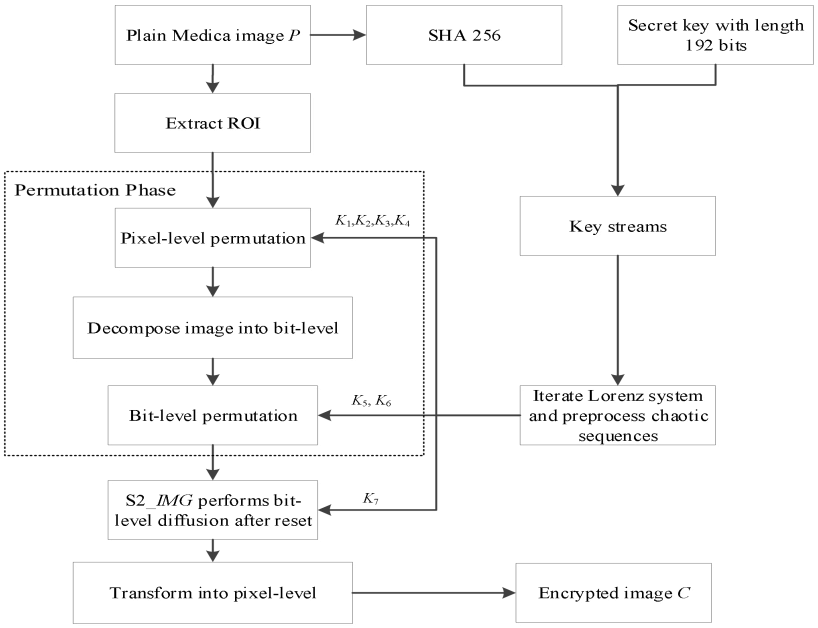


Figure 1. The flowchart of image encryption algorithm.

3.1. Extract ROI and get coordinate information

Input: Plain medical image P,

Output: ROI coordinates $Pos(a, b, c, d)$

Process:

Let $P \in \mathbb{R}^{M\times N}$ denote the input grayscale medical image, and let I_b be the background intensity threshold (typically $I_b = 0$). The ROI region is defined as the minimal rectangular area covering all pixels whose intensity exceeds the threshold:

$$\mathcal{R}_{ROI} = \{(i, j) \mid P(i, j) > I_b\} \tag{2}$$

Then, the bounding box of ROI is defined by the coordinate tuple Pos(a, b, c, d), where

$$a = \min_{(i,j)\in\mathcal{R}_{BOI}} j, b = \min_{(i,j)\in\mathcal{R}_{BOI}} i \tag{3}$$

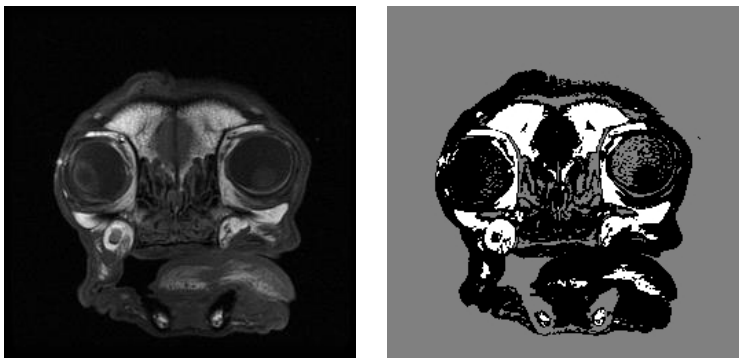
$$c = \max_{(i,j)\in\mathcal{R}_{GOI}} j - a + 1, d = \max_{(i,j)\in\mathcal{R}_{GOI}} i - b + 1 \tag{4}$$

This formalization describes an intensity-based control mechanism for automatically selecting the ROI region. It ensures that all foreground information is

enclosed, while background regions are excluded to enhance encryption efficiency.

To compute these parameters in practice, the image is traversed row-wise and column-wise: Traverse each row from left to right to find the minimum non-background column index in each row. The minimum among them becomes a; Traverse each row from right to left to find the maximum non-background column index. The maximum becomes c; Similarly, column-wise traversal determines b and d.

Figure 2a,b show schematic diagrams of ROI segmentation using the K-means algorithm, and the resulting bounding box is shown in **Figure 2c**.



(**a**) Plain image (**b**) Image segmentation result

(**c**) ROI Results

Figure 2. K-means algorithm for image segmentation and ROI extraction.

3.2. The generation of keystream

This approach not only randomly selects a secret key K of 192 bits, but also adopt SHA-256 algorithm. And the keystreams are generated from above keys. Through this design, the security of the algorithm key is further enhanced, so that the encryption keys of different images are different, and the effect of one encryption at a time is realized. The generation of keystream is as follows:

Input: Plain medical image P, secret Key K consisted of 192 bits

Output: Seven keystreams K_{1-7}.

Method:

Step 1: Get the hash value of image P by SHA-256 function and take it as part of the secret key.

$$HK = hash256(P) \tag{5}$$

Step 2: Read state variables x, y, z, a, b and c of Lorenz chaotic system to compute

the x', y', z', a', b' and c' using Eq. (3):

$$\begin{cases} x' = x + (\dfrac{\sum_{i=1}^{64} K(i) \times 2^{i-1}}{2^{64}} + \dfrac{\sum_{i=1}^{128} HK(i) \times 2^{i-1}}{2^{128}}) \\ y' = y + (\dfrac{\sum_{i=65}^{128} K(i) \times 2^{i-65}}{2^{64}} + \dfrac{\sum_{i=129}^{256} HK(i) \times 2^{i-129}}{2^{128}}) \\ z' = z + (\dfrac{\sum_{i=129}^{192} K(i) \times 2^{i-129}}{2^{64}} + \dfrac{\sum_{i=65}^{192} HK(i) \times 2^{i-65}}{2^{128}}) \\ a' = a + \text{mod}(\sum_{i=1}^{64} K(i) + \sum_{i=1}^{128} HK(i), 192) \Big/ 10^5 \\ b' = b + \text{mod}(\sum_{i=65}^{128} K(i) + \sum_{i=129}^{256} HK(i), 192) \Big/ 10^5 \\ c' = c + \text{mod}(\sum_{i=129}^{192} K(i) + \sum_{i=65}^{192} HK(i), 192) \Big/ 10^5 \end{cases} \tag{6}$$

Step 3: Update the parameters of Lorenz system using x', y', z', a', b' and c' to obtain x'', y'', z'', a'', b'' and c'' using Eq. (4):

$$\begin{cases} x'' = x' + (\dfrac{\sum_{i=1}^{64} (K(i) + HK(i)) \times 2^{i-1}}{2^{68}}) \\ y'' = y' + (\dfrac{\sum_{i=129}^{192} (K(i) + HK(i)) \times 2^{i-1}}{2^{68}}) \\ z'' = z' + \text{mod}(\, x'' + y'', 1) \\ a'' = a' + \text{mod}(\sum_{i=1}^{64} K(i) \oplus \sum_{i=65}^{128} HK(i), 128) \Big/ 10^5 \\ b'' = b' + \text{mod}(\sum_{i=65}^{128} K(i) \oplus \sum_{i=129}^{192} HK(i), 128) \Big/ 10^5 \\ c'' = c' + \text{mod}(\sum_{i=129}^{192} K(i) \oplus \sum_{i=192}^{256} HK(i), 128) \Big/ 10^5 \end{cases} \tag{7}$$

where the operator $\oplus$ represents bit-wise XOR operation.

Step 4: Iterate the Lorenz system $M \times N$ times using the updated x', y', z', a', b', c' and x'', y'', z'', a'', b'', and c'' separately. This iteration will produce six chaotic sequences $Sequence_\varphi$ where $\varphi = 1, 2, 3, 4, 5, 6$. Then generate the $preSequence_\varphi$ as follows:

$$\begin{cases} preSequence_\varphi(i) = floor\left(mod\left(\left((abs(Sequence(i)) - floor(abs(Sequence(i)))) * 10^{14}\right), N\right)\right) + 1; i = 1, 2, \ldots, MN; \varphi = 1, 2 \\ preSequence_\varphi(i) = floor\left(mod\left(\left((abs(Sequence(i)) - floor(abs(Sequence(i)))) * 10^{14}\right), M\right)\right) + 1; i = 1, 2, \ldots, MN; \varphi = 3, 4 \\ preSequence_\varphi(i) = floor\left(mod\left(\left((abs(Sequence(i)) - floor(abs(Sequence(i)))) * 10^{14}\right), 256\right)\right); i = 1, 2, \ldots, MN; \varphi = 5, 6 \end{cases} \tag{8}$$

Here, the function $abs(X)$ return the absolute value x and $floor(X)$ returns the nearest integer $\leq x$.

Step 5: Construct different keystreams K_{1-7} as follows:

$$K_1 = preSequence_1(1:M) \oplus preSequence_2(M+1:2M)) \oplus preSequence_1(2M+1:3M) \oplus \ldots\ldots \oplus preSequence_2((N-1)M+1:MN)) \tag{9}$$

$$K_2 = preSequenc_1(1:N) \oplus preSequenc_2(N+1:2N)) \oplus preSequenc_1(2N+1:3N) \oplus \ldots\ldots \oplus preSequenc_2((M-1)N+1:MN)) \tag{10}$$

$$K_2 = preSequence_1(1:N) \oplus preSequence_2(N+1:2N)) \oplus preSequence_1(2N+1:3N) \oplus \ldots\ldots \oplus preSequence_2((M-1)N+1:MN)) \tag{11}$$

$$K_4 = cat(preSequence_3(\frac{MN}{4}+1:\frac{MN}{2}), preSequence_4(1:\frac{MN}{2}), preSequence_3(\frac{MN}{2}+1:\frac{3MN}{4})) \tag{12}$$

$$K_6 = cat(preSequenc_1(\tfrac{MN}{4}), preSequenc_2(\tfrac{MN}{2}), preSequenc_3(\tfrac{3MN}{4}), preSequenc_4(MN), preSequenc_5(\tfrac{MN}{4}), preSequenc_5(\tfrac{MN}{2}), preSequenc_5(\tfrac{3MN}{4}), preSequenc_5(MN)) \tag{13}$$

$$K_s = preSequence_5; K_7 = preSequence_6 \tag{14}$$

Here, the function $cat(x, y)$ represents the concatenation of x and y.

3.3. Permutation process of the proposed scheme

3.3.1. Pixel-level scrambling

Input: ROI image IMG, K_1, K_2, K_3 and K_4

Output: Scrambled image $S1\_IMG$

Process:

Step 1: Take the ROI image IMG from original medical image P with sized of $c \times d$ and perform the following steps.

Step 2: Take the keystream K_1 as the first column of the image IMG, and take keystream K_2 as the last column of the image IMG.

Step 3: For each row, compare the values of K_1 and K_2 at the corresponding positions, which are $K_1[i]$ and $K_2[i]$, respectively.

$$\begin{cases} left = \min(K_1[i], K_2[i]) \\ right = \max(K_1[i], K_2[i]) \\ R\mathbb{I}[i] = left \end{cases} \tag{15}$$

Step 4: Flip the values in the corresponding left and right intervals in each row.

Step 5: Compare the difference between $K_1[i]$ and $K_2[i]$ with 0, $R_1[i]$ cyclic shifts are performed for each row.

$$\begin{cases} K_1[i] - K_2[i] > 0, cyclic\ shift\ right\ R1[i] position \\ K_1[i] - K_2[i] \le 0, cyclic\ shift`left\ R1[i] position \end{cases}, i = 1, 2, ..., c \tag{16}$$

Step 6: For each column, compare the values of K_3 and K_4 at the corresponding positions, which are $K_3[j]$ and $K_4[j]$, respectively.

$$\begin{cases} up = \min(K_3[j], K_4[j]) \\ down = \max(K_3[j], K_4[j]) \\ R_2[j] = up \end{cases} \tag{17}$$

Step 7: Flip the values in the corresponding up and down intervals in each column.

Step 8: Compare the difference between $K_3[j]$ and $K_4[j]$ with 0, $R_2[j]$ cyclic shifts are performed for each column, and denote the addressed image as $S1\_IMG$

$$\begin{cases} K_3[j] - K_4[j] > 0, cyclic\ shift\ up\ R_2[j] position \\ K_3[j] - K_4[j] \le 0, cyclic\ shift\ down\ R_2[j] position \end{cases} \tag{18}$$

The above process can be shown by an example matrix in **Figure 3**.

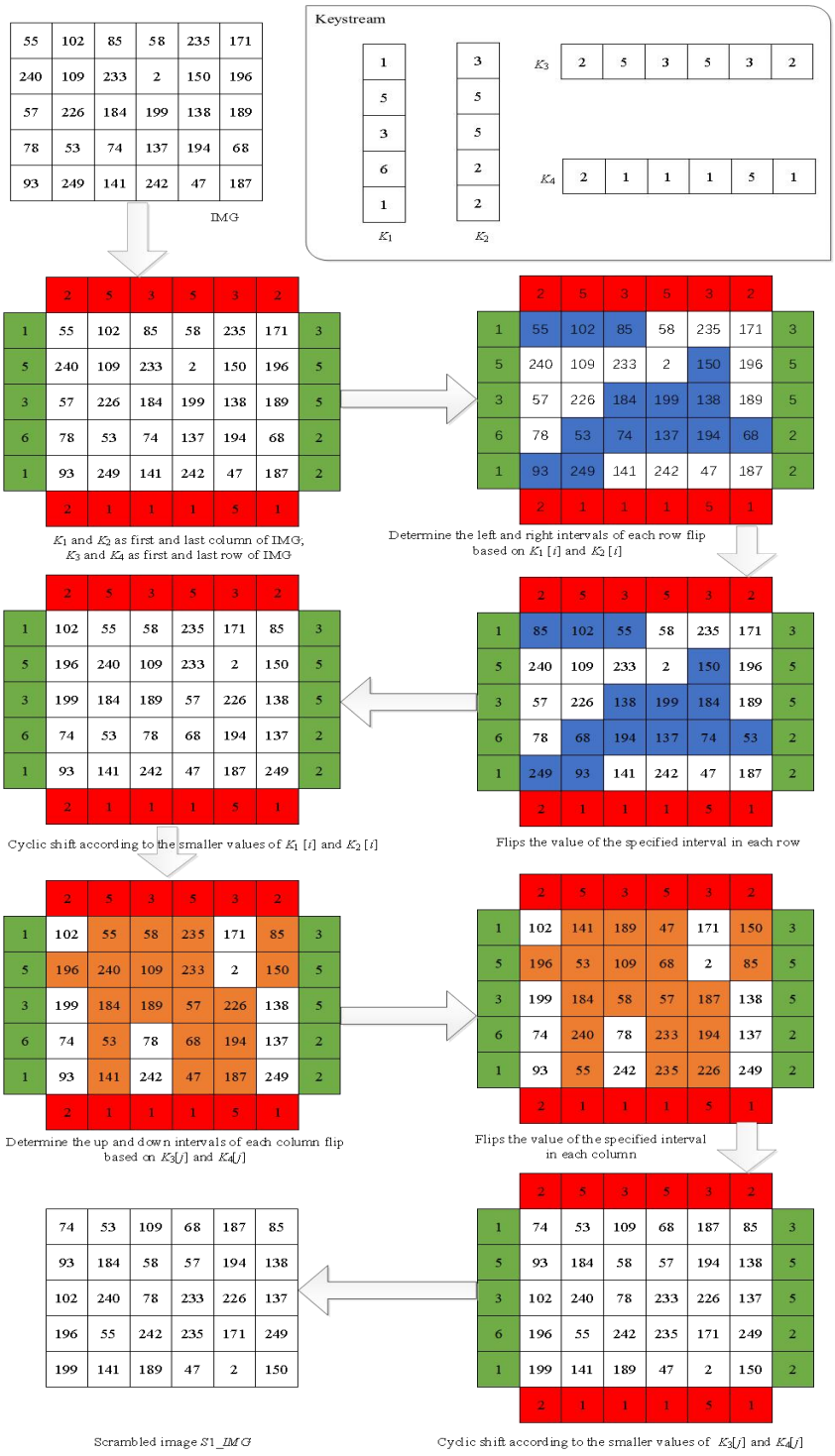


Figure 3. Pixel level scrambling.

3.3.2. Bit-level scrambling

Input: $S1\_IMG$, K_5 and K_6

Output: Final scrambled image $S2\_IMG$

Process:

Step 1: Consider the matrix $S1\_IMG$ of dimensions $M \times N$. For each pixel location (i, j), count the number of zero bits in its binary representation. Store the result in matrix $S1\_ZEROS$.

Step 2: Let K_5 of be a keystream matrix of the same size $M \times N$. Calculate the total number of one bits in the corresponding binary value. Denote the resulting matrix as $K5\_ONE$.

Step 3: Compute the matrix S_DIFF using the modulo operation:

$$S\_DIFF = \text{mod}(S\_ZEROS, 2) \tag{19}$$

Step 4: Calculate the value of $S\_ROTATION$ using the following equation:

$$S\_RATATION = (K5\_ONE + (8 - S1\_ZEROS), 8) + 1 \tag{20}$$

Here $8 - S\_ZEROS$ represents the 1's numbers in each (i, j) pixel of $S1\_IMG$.

Step 5: Perform rotation on $S1\_IMG$ based on the above three matrices as specified below:

$$\begin{cases} S\_DIFF(i,j) == 0, \ cyclic\ shift\ right\ S\_ROTATION\ (i,j)\ position\ on\ pixel\ S1\_IMG(i,j) \\ S\_DIFF(i,j) == 1, \ cyclic\ shift\ left\ S\_ROTATION\ (i,j)\ position\ on\ pixel\ S1\_IMG(i,j) \end{cases} \tag{21}$$

Step 6: Decompose $S1\_IMG$ into 8-bit planes and reshape them into size of $M \times N \times 8$.

Step 7: Sort K_6 and save the sorted subscripts as $Index$. Then, we sort the obtained 8-bit plane in Step 6 based on $Index$ to obtain the bit-level scrambled image $S2\_IMG$.

Step 8: Replace $S2\_IMG$ at the original position of image in medical image P.

The bit-level scrambling process is illustrated with an example of a 5×6 matrix in **Figure 4**.

3.4. Diffusion process of the proposed scheme

In this phase, a bit-level diffusion mechanism is introduced. The keystream K_7, generated by the Lorenz chaotic system, is first converted into its binary representation, denoted as CM, with a dimensional size of $M \times N \times 8$. Simultaneously, the image matrix $S2\_IMG$ also has a size of $M \times N \times 8$. The bit-wise diffusion procedure is defined by the following equation:

$$C(i,j,k) = \begin{cases} CM(i,j,k) \oplus S2\_IMG(i,j,k), k = 1 \\ CM(i,j,k) \oplus C(i,j,k-1) \oplus S2\_IMG(i,j,k), k \neq 1 \end{cases} \tag{22}$$

Then, Transform the obtained bit-level C matrix to the final cipher-image. The

overall encryption process can be viewed as a dynamic state-control sequence, where the Lorenz system serves as the central chaotic generator, evolving over time and modulating the structure of both permutation and diffusion phases. This dynamic control mechanism ensures that the encryption outcome is not only complex and unpredictable but also highly sensitive to the underlying state trajectory, reinforcing security against statistical and differential attacks.

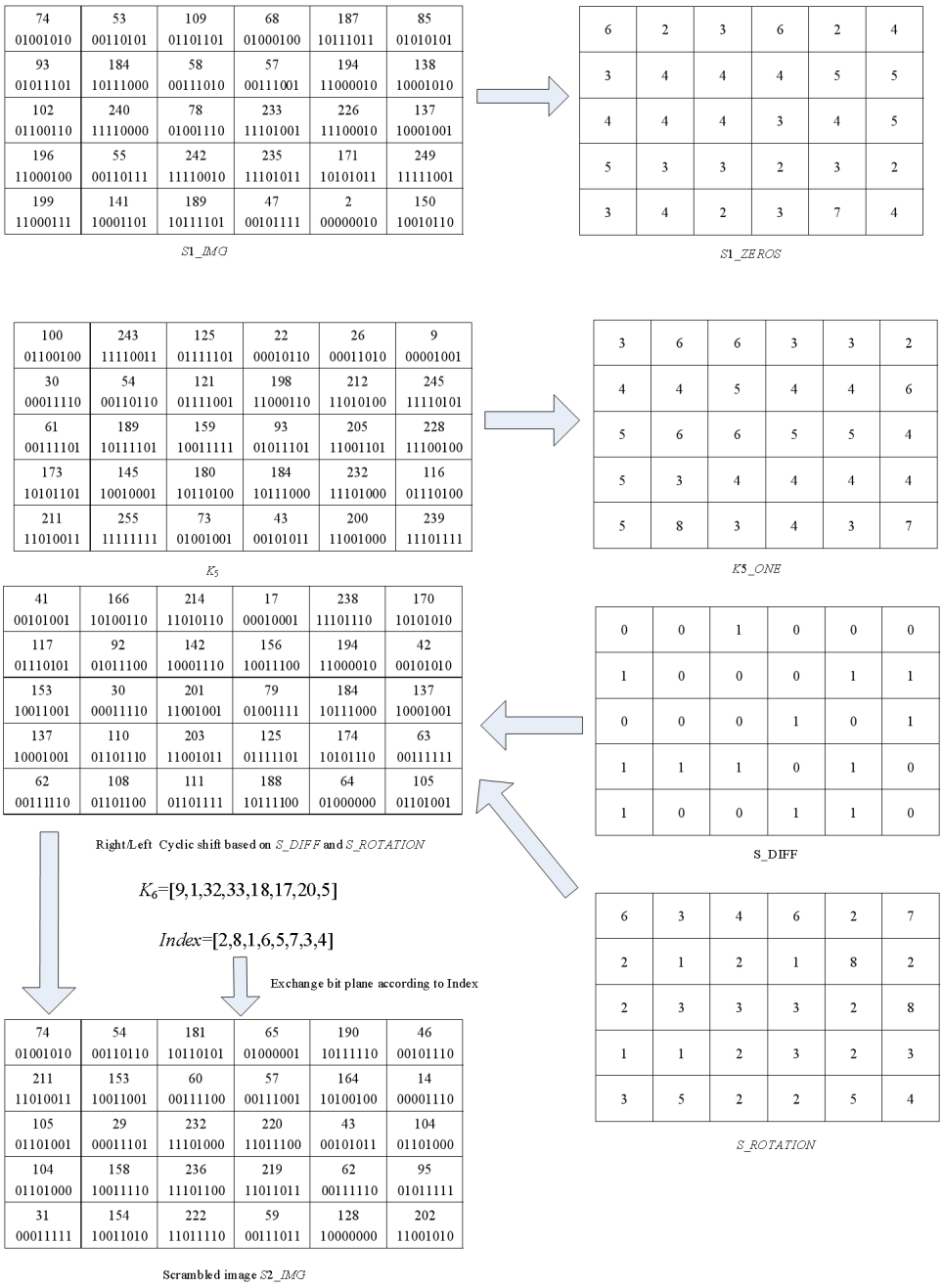


Figure 4. Bit level scrambling.

3.5. Decryption process

The decryption process of the proposed ROI-based hybrid encryption scheme is strictly the inverse of the encryption procedure, ensuring complete reversibility. Given the same secret key and the corresponding image-dependent parameters, the decryption steps can accurately recover the original image without any information loss. The

process can be summarized as follows:

Step 1: Using the identical initial conditions and control parameters of the Lorenz chaotic system, the receiver regenerates the chaotic sequences. The same SHA-256 hash of the encrypted image header or metadata is combined with the secret key to guarantee that the keystreams are identical to those used during encryption.

Step 2: The steps to generate the CM matrix are the same as above, and $S2\_IMG$ is obtained by the following formula:

$$S2_IMG(i,j,k) = \begin{cases} CM(i,j,k) \oplus C(i,j,k), k = 1 \\ CM(i,j,k) \oplus C(i,j,k-1) \oplus C(i,j,k), k \neq 1 \end{cases} \tag{23}$$

Step 3: The bit-level permutation indices are reconstructed from the same chaotic sequences, and the inverse mapping is applied to reorder the bits to their original positions. Similarly, the pixel-level permutation matrix is reversed to restore the spatial arrangement of the ROI and RONI regions. This step completely removes the spatial confusion introduced during encryption.

Step 4: The decrypted ROI is accurately placed back into its original position within the RONI to reconstruct the full medical image. Because ROI extraction was performed deterministically based on pixel intensity or segmentation boundaries, no auxiliary location data is required for reconstruction, thereby maintaining data integrity and avoiding leakage of sensitive metadata.

The above steps can be used to restore the plain medical image P.

3.6. Data transmission between encryption and decryption parties

To ensure successful decryption, the data transmitted from the encrypting party to the decrypting party must be explicitly defined. Only a small set of parameters is required, avoiding any leakage of sensitive image content. Specifically, the receiver needs: (1) the secret key K, securely shared through a private channel; (2) the ROI information $Pos(a,b,c,d)$ embedded in the ciphertext header for accurate reconstruction; (3) the ciphertext image itself, transmitted over the public channel. With these elements, the decrypting party can precisely regenerate the chaotic sequences and perform inverse operations, ensuring complete reversibility and integrity of the proposed scheme.

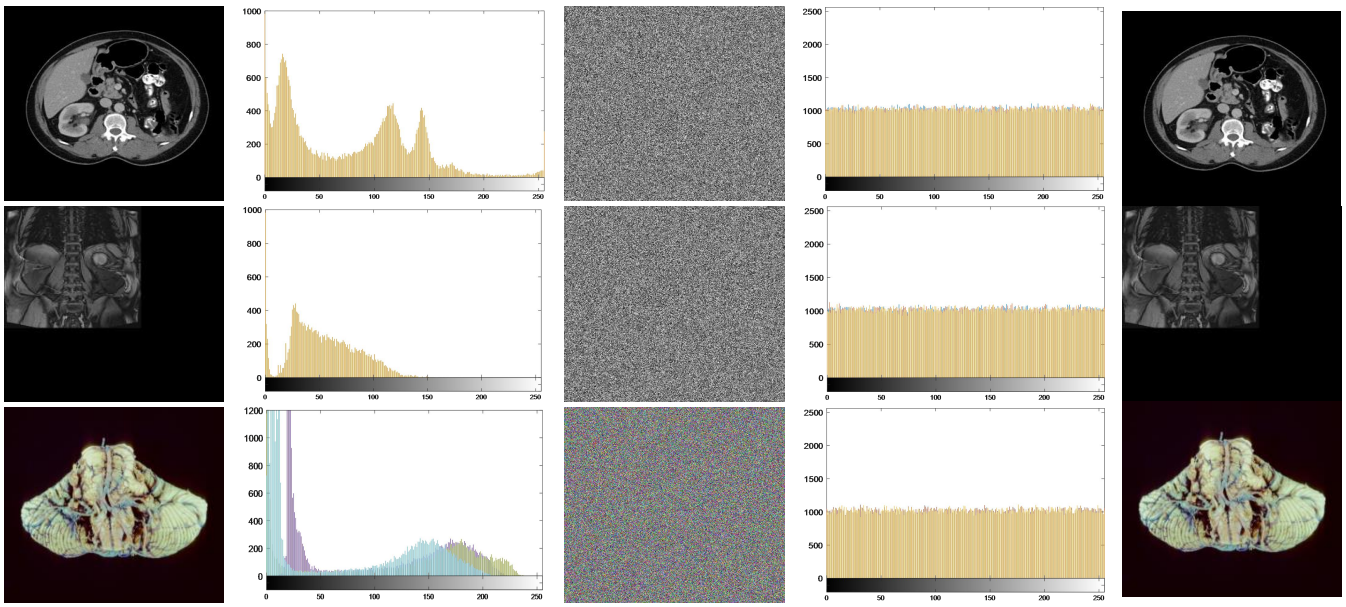
4. Simulation results and security analysis

To validate the proposed method, a series of simulations and security evaluations were conducted. All experiments were performed in MATLAB 2016a on a computer configured with an Intel Core i5-5257U processor running at 2.70 GHz and 8 GB of memory. The test images are carried out according to medical images provided by TCGA database (cancerimagingarchive.net), and several medical images of different size and type are selected as a group of test cases to demonstrate the applicability of the algorithm. Six CT images were selected from the "TCGA-B9-4114 \09-19-2004-NA-CT" dataset and numbered "001" to "006". Initial conditions and parameters for the chaotic system were randomly initialized. As an example, the values are set as: $x = 0.012814140114$, $y = 0.198213531431$, $z = 0.328193629108$,

$a = 10.000000001234$ $b = 2.666666109273$, $c = 20.000000002863$. Chaotic system parameters and initial values are randomly chosen, along with a 192-bit secret key. For illustration, a 384-bit hexadecimal key such as K = D31098A43CF109EA10 ABD376EF4690BCA25403CDEF0426EF can be employed to generate personalized initial values.

4.1. Simulation

In this experiment, eight medical images were encrypted and subsequently decrypted to evaluate the performance of the proposed method. **Figure 5** presents selected examples labeled from "001" to "003", along with their corresponding histograms before and after encryption, and the results after decryption. As illustrated in **Figure 5**, the histogram of the original images demonstrates clear data patterns, indicating the presence of structured content. In contrast, the histograms of the encrypted images exhibit a nearly uniform distribution, revealing no discernible information. This confirms that the encryption process effectively conceals image details. After decryption, the original content is successfully recovered. These results suggest that the proposed algorithm maintains both high security and reliable reversibility, thereby achieving good practical performance.



(**a**) Plain image (**b**) Histogram of (**a**) (**c**) Encrypt image (**d**) Histogram of (**c**) (**e**) Decrypt image

Figure 5. Simulation results.

4.2. Secere key analysis

Since the key consists of 192 bits, the key space is 2192, which is sufficient to resist brute force attacks. Furthermore, an effective image encryption algorithm should be highly sensitive to its secret key. Even a minimal alteration in the key value is expected to produce drastically different encrypted or decrypted outputs [35]. To verify this property, we conducted two experiments assuming machine precision of 10^{-11}.

In the first test (**Figure 6**), we encrypted the same image using keys with slight numerical differences and compared the results through pixel-wise subtraction. The distinct outputs confirm that even minimal key changes produce vastly different cipher

images. In the second, we decrypted the cyphertext using similarly varied keys. Only the exact original key could successfully recover the plaintext; all others failed (**Figure 7**). These results clearly demonstrate the strong key sensitivity.

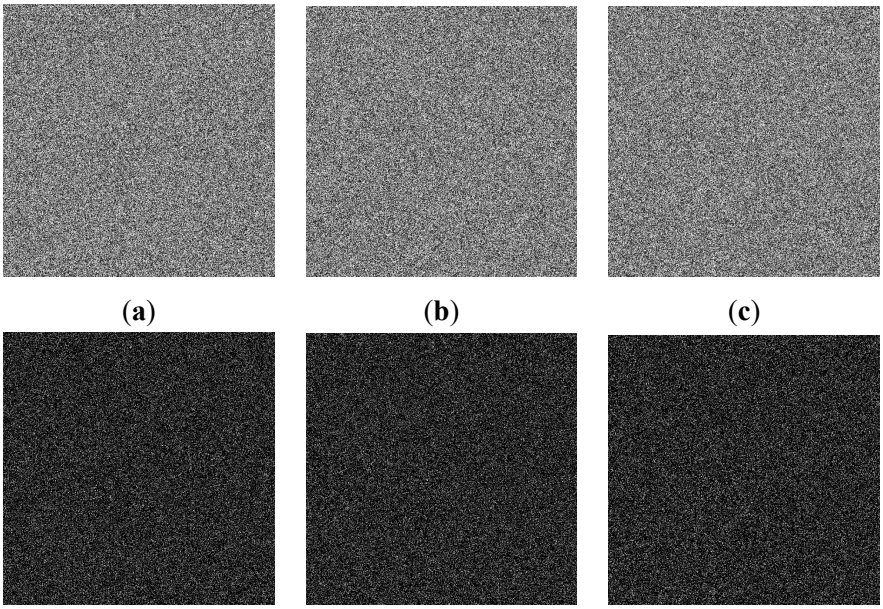


Figure 6. Key sensitivity in encryption. (a) encrypted image of Figure 6a using original x', y'; (b) encrypted image of **Figure 6a** using $x' = x' + 10^{-11}$; (c) encrypted image of **Figure 6a** using $y' = y' + 10^{-11}$; (d) difference between **Figure 6a** and **Figure 6b**; (e) difference between **Figure 6a** and **Figure 6c**; (f) difference between **Figure 6b** and **Figure 6c**.

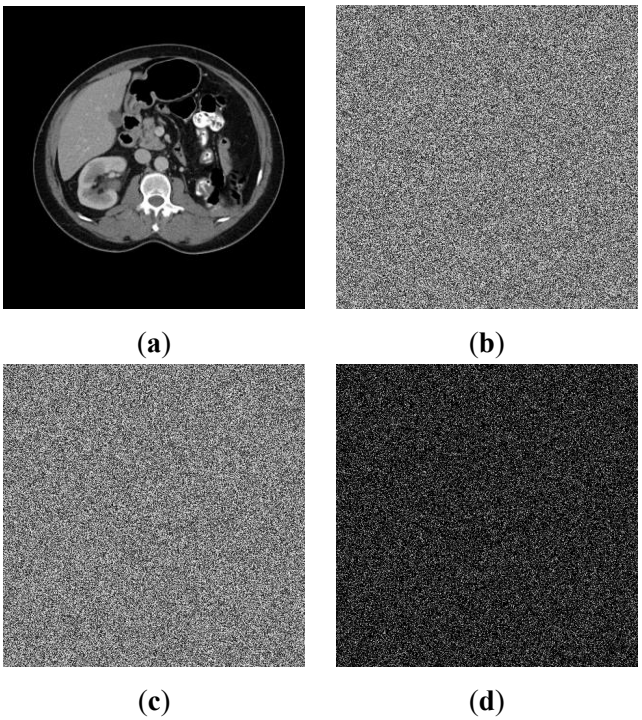


Figure 7. Key sensitivity in decryption. (**a**) decrypted image of **Figure 7a** using original x', y'; (**b**) decrypted image of **Figure 7a** using $x' = x' + 10^{-11}$; (**c**) decrypted image of **Figure 7a** $y' = y' + 10^{-11}$; (**d**) difference between **Figure 7b** and **Figure 7c**.

4.3. Correlation analysis

Plain images typically exhibit strong spatial correlation, as neighboring pixels tend to have similar intensity values [36]. **Figure 8** displays the test results after randomly choosing 5000 pixels in three directions before and after the "001" image. As observed in **Figure 8**, the encrypted image displays a random and uniform distribution of pixel values, which leads to a marked decrease in correlation and improved security.

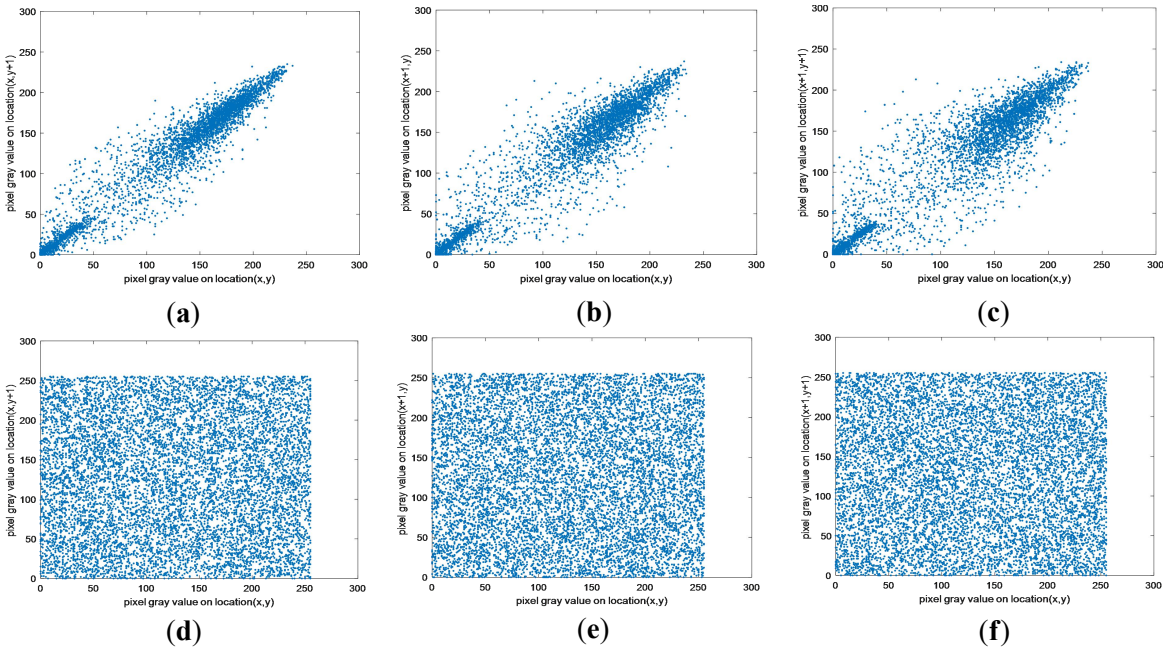


Figure 8. The correlation distribution of 003 (**a**) H of plain image; (**b**) V plain image; (**c**) D plain image; (**d**) H encrypt image; (**e**) V encrypt image; (**f**) D encrypt image.

For a more intuitive digital presentation, the correlation coefficient γ_{xy} is employed as a metric for evaluating the relationship between adjacent pixels. The calculation formula is provided as follows:

$$\begin{cases} \gamma_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}} \\ \mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \\ D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \\ E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \end{cases} \tag{24}$$

where x and y denote the gray-level intensities of two neighboring pixels, N represents the total number of samples, $E(x)$, $D(x)$ and $\mathrm{cov}(x,y)$ are the expected value, variance value and covariance value respectively.

The experimental outcomes are summarized in **Table 1**. **Table 2** provides a comparative analysis involving other encryption methods. For consistency, all values are converted to absolute form before averaging. The results demonstrate that the original image exhibits a high level of correlation between adjacent pixels. In contrast, the encrypted image produced by the proposed scheme shows significantly reduced correlation, with values approaching zero. This behavior suggests that the method

is effective in breaking spatial predictability and provides strong protection against statistical attacks.

Table 1. Correlation analysis between adjacent pixels.

Image	Plain image			Encrypted image		
	H	V	D	H	V	D
001	0.9757	0.9751	0.9589	−0.0012	0.0006	0.0017
002	0.9776	0.9753	0.9620	0.0014	−0.0011	−0.0009
003	0.9793	0.9737	0.9611	−0.0015	0.0016	−0.0010
004	0.9725	0.9845	0.9628	0.0013	−0.0008	0.0012
005	0.9793	0.9841	0.9680	0.0010	−0.0017	−0.0006
006	0.9804	0.9834	0.9683	0.0014	−0.0007	−0.0011

Table 2. Comparison of correlation coefficients.

Average	Proposed	Ye et al. [37]	Farah et al. [38]	Jithin et al. [39]	Hoang et al. [40]	Li et al. [41]
H	0.0013	0.0016	0.0693	0.0012	0.0034	−0.0015
V	0.0011	0.0057	0.0610	0.0011	0.0020	0.0023
D	0.0011	0.0189	0.0242	0.0043	0.0032	0.0021

4.4. Information entropy

Information entropy is a quantitative metric used to assess the uncertainty or randomness inherent in a source of data [42]. If s represents an image, its information entropy is calculated as follows:

$$H(s) = -\sum_{i=1}^{2^i-1} p(s_i) \log_2 p(s_i) \tag{25}$$

where s_i denotes the i-th pixel intensity in the image, with values ranging from 0 to 255. Here, $L = 8$ corresponds to the number of bits in a grayscale pixel, and $p(s_i)$ represents the probability of occurrence of each pixel value. In this experiment, six medical images were evaluated, and the results are summarized in **Table 3**. The analysis indicates that the encrypted images achieved information entropy values exceeding 7.9993, which is nearly identical to the ideal value. **Table 4** further compares these results with other existing algorithms. It can be observed that the proposed method consistently achieves higher entropy, demonstrating its effectiveness in producing ciphertext with superior randomness.

Table 3. Information entropy test.

Image	001	002	003	004	005	006
Plaintext	4.05234	4.13325	3.96646	3.87695	3.50317	3.47619
Ciphertext	7.99940	7.99934	7.99933	7.99928	7.99935	7.99942

Table 4. Comparison of information entropy.

Algorithm	Proposed	Hu et al. [43]	Hu et al. [44]	Alawida et al. [45]	Kamal et al. [46]	Zhao et al. [47]
Mean	7.99935	7.9993	7.9997	7.9992	7.9993	7.9993

4.5. Local entropy analysis

In addition to the global information entropy, local entropy provides a more detailed characterization of the spatial distribution of information. Specifically, local entropy evaluates the randomness within small neighborhoods, thereby revealing whether the encryption process achieves uniform randomness across different image regions. The local entropy (LE) is calculated as:

$$\overline{H_{l,K_d}}(C) = \sum_{j=1}^{l} \frac{R(C_j)}{l} \tag{26}$$

where l and K_d represent the number of randomly selected local regions and the number of pixels in each region, respectively, and $R(C_j)$ represents the information entropy of the block C_j consisting of K_d pixels in the jth local region. The LE theoretical standard range is [7.9019, 7.9031]. **Table 5** shows the LE calculation results of each test image and whether they meet the evaluation criteria. As shown in **Table 5**, all test results fall within the theoretical range, indicating that the algorithm in this chapter effectively blocks the possibility of attacks based on local statistical features.

Table 5. Local entropy analysis.

Images	**001**	**002**	**003**	**004**	**005**
LE	7.9025	7.9030	7.9028	7.9022	7.9025
Result	Pass	Pass	Pass	Pass	Pass

4.6. Differential attack analysis

Two indicators are usually used to evaluate the ability of an algorithm to resist differential attacks [47]: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). Let C_1 and C_2 represent the original ciphertext image and the ciphertext image obtained after slight modification of the plaintext, respectively. Then NPCR and UACI can be calculated as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{27}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{Q}\right] \times 100\% \tag{28}$$

$$D(i) = \begin{cases} 1, & C_1(i,j) \neq C_2(i,j) \\ 0, & C_1(i,j) = C_2(i,j) \end{cases} \tag{29}$$

where ^{M} and N are the width and height of the image, respectively. Based on previous research, Wu et al. [48] proposed a standard for judging whether an algorithm can resist differential attacks. For a significance level α, if the result is higher than $NPCR_a^*$ and falls into the critical interval $(UACI_a^{*-}, UACI_a^{*+})$, the method passed the test.

$NPCR_a^*$ and $(UACI_a^{*-}, UACI_a^{*+})$ are calculated as follows:

$$NPCR_\alpha^* = (F - \Phi^{-1}(\alpha)\sqrt{\frac{F}{M \times N}})\Big/(F+1) \tag{30}$$

$$\begin{cases} UACI_\alpha^* = \frac{F+2}{3F+3} - \Phi^{-1}(\alpha/2)\sqrt{\frac{(F+2)(F^2+2F+3)}{18(F+1)^2MNF}} \\ UACI_\alpha^{*+} = \frac{F+2}{3F+3} + \Phi^{-1}(\alpha/2)\sqrt{\frac{(F+2)(F^2+2F+3)}{18(F+1)^2MNF}} \end{cases} \tag{31}$$

According to Wu et al. [48], $\alpha = 0.05$ is set to evaluate the difference attack. The critical interval defined is shown in **Table 6**.

Table 7 presents the NPCR and UACI results for six test images of size 512×512. All NPCR values exceed 99.59%, and UACI values fall within the critical interval, meeting the expected theoretical thresholds for differential attack resistance. These results indicate that the proposed algorithm can effectively withstand small perturbations in the plaintext, producing significantly different ciphertexts. In addition, **Table 8** provides a comparative analysis of the proposed method against several existing algorithms under two resolution settings (256×256 and 512×512). The average NPCR and UACI values of the proposed scheme are consistently higher or comparable to those of competing methods. Notably, the proposed algorithm maintains excellent performance across different image sizes, with NPCR values close to or exceeding 99.60% and UACI values close to 33.45. These results demonstrate that the proposed encryption scheme exhibits strong resistance to differential attacks. It ensures that even a minimal change in the plaintext leads to substantial and unpredictable alterations in the ciphertext, thereby satisfying the security requirements for sensitive image data protection.

Table 6. Critical values ($\alpha = 0.05$).

Size	$NPCR_{0.05}^*$	$(UACI_{0.05}^{*-}, UACI_{0.05}^{*+})$
256×256	99.5693	(33.2824, 33.6447)
512×512	99.5893	(33.3730, 33.5541)
1024×1024	99.5994	(33.4183, 33.5088)

Table 7. Differential attack analysis.

Test image	001	002	003	004	005	006
NPCR	99.6213	99.6118	99.6068	99.5996	99.6311	99.6846
UACI	33.4314	33.4413	33.4614	33.5023	33.4208	33.4148

Table 8. Comparison of NPCR and UACI.

Algorithm	NPCR		UACI	
	256×256	512×512	256×256	512×512
Avg. of proposed	99.6002	99.6259	99.5894	33.4453
Enayatifar et al. [49]	99.1841	99.6184	33.5284	33.5739
Manikandan et al. [50]	99.571	99.362	33.518	33.485
Zhang et al. [51]	99.6139	99.6077	33.5349	33.3624

4.7. Robustness analysis

Robustness refers to the ability of an algorithm to resist various attacks and abnormal situations, and is one of the important criteria for evaluating the performance of encryption algorithms [51]. In a network communication environment, image transmission will inevitably be affected by uncontrollable factors or malicious attacks and destruction. A robust algorithm should be able to function stably and reliably in various environments to minimize the impact.

To evaluate the robustness of the proposed scheme, simulation experiments were conducted under two typical attack scenarios: random noise interference and data block loss. The results are illustrated in **Figure 9**, where the corresponding PSNR values between the decrypted and original images quantitatively reflect the reconstruction quality.

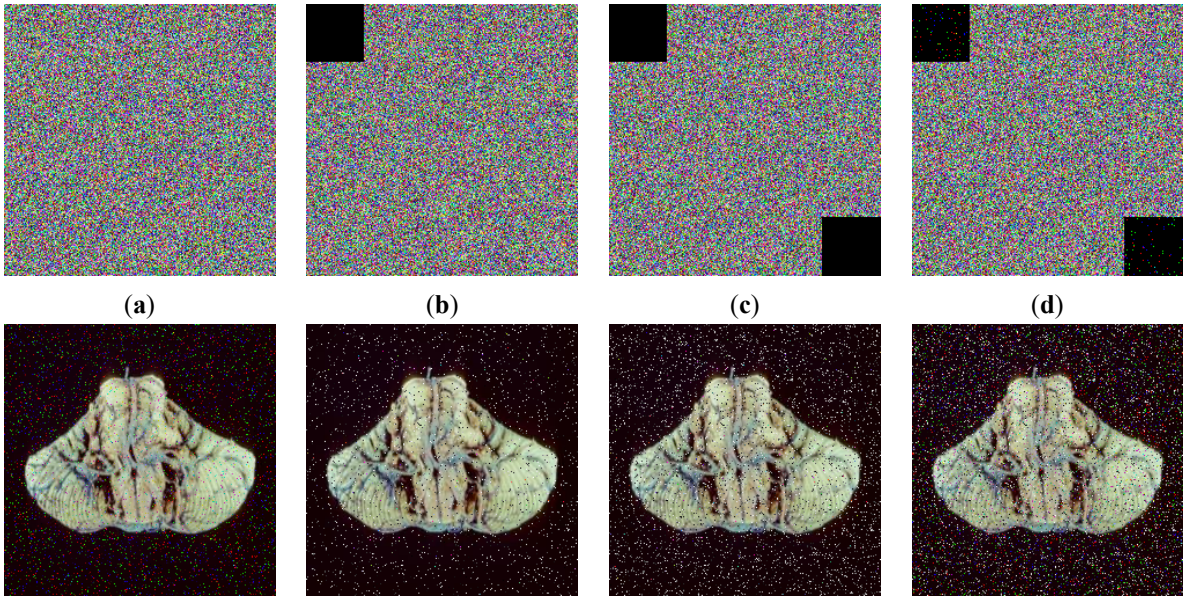


Figure 9. Noise attack: (**a**) ciphertext image of 5% noise; (**b**) ciphertext image of 50×50 data block lost; (**c**) ciphertext image of 100×100 data block lost; (**d**) ciphertext image of 5% noise mixed 100×100 data block lost; (**e**) the decrypted image of **Figure 9a**; (**f**) the decrypted image of **Figure 9b**; (**g**) the decrypted image of **Figure 9c**; (**i**) the decrypted image of **Figure 9d**.

First, a 5% random noise was added to the ciphertext image (**Figure 9a**), and the decrypted result achieved a PSNR of 38.25 dB, indicating that the algorithm can effectively resist moderate noise disturbance with minimal perceptual degradation. Second, block loss attacks were simulated by removing fixed-size regions from the ciphertext image: a 50×50 block (**Figure 9b**), a 100×100 block (**Figure 9c**), and a combination of 5% noise and 100×100 block loss (**Figure 9d**). The corresponding decrypted images (**Figure 9f–h**) achieved PSNR values of 41.28 dB, 34.58 dB, and 28.04 dB, respectively. These results demonstrate that, although structural artifacts appear with increasing distortion, the main diagnostic details and overall visual semantics of the image remain recognizable.

Overall, the proposed encryption scheme maintains acceptable robustness under both random noise and data loss scenarios. The gradual decline in PSNR with higher

disturbance levels quantitatively confirms the scheme's degradation characteristics, while the preservation of key image information verifies its fault tolerance and practical applicability in unreliable or hostile transmission environments.

4.8. Encryption/decryption time

The computational efficiency of the proposed scheme was evaluated by measuring the time required for ROI detection, encryption, and decryption of standard medical images with different sizes. The experiments were conducted in MATLAB 2016a on a computer configured with an Intel Core i5-5257U processor running at 2.70 GHz and 8 GB of memory, and the results are shown in **Table 9**. The ROI detection stage takes about 0.09–0.15 s, while the average encryption and decryption times range from 0.87 s to 1.07 s and 0.74 s to 0.98 s, respectively. For a 512×512 image, the total processing time is within 1.1 s, indicating that the proposed algorithm achieves efficient performance and can meet the requirements of real-time medical image transmission and embedded applications.

Table 9. Encryption/decryption time.

Algorithm	Time consumption (s)		
	Detection	**Encryption**	**Decryption**
001	0.1486	0.8672	0.7436
002	0.0869	0.9624	0.8473
003	0.1147	1.0687	0.9847

5. Discussion

The proposed encryption algorithm demonstrates high security and efficiency, as confirmed by the experimental analyses in Section 4. To further highlight its competitiveness, indirect comparisons are conducted with several recently published algorithms. For example, Li [41] introduced a chaotic-map-based image encryption system that achieves an average information entropy of 7.9993 and NPCR of 99.58%. Similarly, Liu et al. [45] reported an improved cascaded chaotic system obtaining entropy around 7.9992. In contrast, the proposed scheme consistently achieves entropy values of 7.9994 and NPCR of 99.63%, indicating slightly stronger randomness and differential resistance. Moreover, the average correlation coefficient of 0.0011 is lower than that of Ye et al. [37], Farah et al. [38], Jithin et al. [39], and Hoang et al. [40], confirming enhanced decorrelation performance. These results collectively show that the proposed method achieves comparable or better security performance than most state-of-the-art chaotic encryption algorithms while maintaining high computational efficiency.

In addition, the dynamic behavior of the improved Lorenz chaotic system used in this work was analyzed through phase portraits, Lyapunov exponents, and bifurcation diagrams. The calculated largest Lyapunov exponent (LLE > 0) verifies that the system exhibits strong chaotic behavior within the selected parameter ranges. The system also demonstrates wide chaotic intervals, good ergodicity, and high sensitivity to initial

conditions. These characteristics ensure that small variations in parameters or initial values lead to entirely different chaotic sequences, which is essential for secure key generation and effective confusion–diffusion operations.

Overall, the combination of experimental comparisons and verified chaotic characteristics demonstrates that the proposed ROI-based medical image encryption scheme provides a robust, secure, and computationally efficient solution that is competitive with or superior to recent methods.

6. Conclusion

In this paper, a novel medical image encryption algorithm based on ROI perception and chaotic systems has been proposed. By exploiting the spatial structure characteristics of medical images, the algorithm selectively encrypts sensitive areas while leaving thereby improving both security and efficiency. The proposed scheme employs a combination of pixel-level and bit-level scrambling techniques, guided by keystreams generated from the Lorenz chaotic system and a SHA-256-based hash mechanism. Furthermore, a bit-level diffusion strategy is adopted to enhance randomness and ensure strong resistance to differential and statistical attacks. The results demonstrate that the algorithm exhibits high key sensitivity, low pixel correlation in cipher images, near-ideal information entropy, and strong resistance against noise and data loss. Compared with several existing methods, the proposed scheme offers a more secure and efficient solution, particularly suitable for applications in medical data protection where selective confidentiality is essential.

In future work, we plan to further optimize the algorithm by integrating lightweight chaotic systems and compression mechanisms, and to explore hardware implementations for real-time encryption in embedded medical devices.

Author contributions: Conceptualization, HW and XW; methodology, HW; software, XW; investigation, HW; writing—original draft preparation, HW; writing—review and editing, XW. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

1. Sun K, Sprott JC. Dynamics of a simplified lorenz system. International Journal of Bifurcation and Chaos. 2009; 19(04): 1357–1366. doi: 10.1142/S0218127409023688
2. Pecora LM, Carroll TL. Synchronization in chaotic systems. Physical Review Letters. 1990; 64(8): 821–824. doi: 10.1103/PhysRevLett.64.821
3. Chen G. Stability of nonlinear systems. In: Chang K (editor). Encyclopedia of RF and Microwave Engineering. Wiley; 2024. pp. 1–27. doi: 10.1002/0471654507.erfme206
4. Zuo J, Zhang J, Wei X, et al. Design and application of multisroll conservative chaotic system with no-equilibrium, dynamics analysis, circuit implementation. Chaos, Solitons & Fractals. 2024; 187: 115331. doi: 10.1016/j.chaos.2024.115331
5. Sambas A, Zhang X, Moghrabi IAR, et al. ANN-based chaotic PRNG in the novel jerk chaotic system and its application for the image encryption via 2-D Hilbert curve. Scientific Reports. 2024; 14(1): 29602. doi: 10.1038/

s41598-024-80969-z
6. Li C, Gao Y, Lei T, et al. Two independent offset controllers in a three-dimensional chaotic system. International Journal of Bifurcation and Chaos. 2024; 34(01): 2450008. doi: 10.1142/S0218127424500081
7. SaberiKamarposhti M, Ghorbani A, Yadollahi M. A comprehensive survey on image encryption: Taxonomy, challenges, and future directions. Chaos, Solitons & Fractals. 2024; 178: 114361. doi: 10.1016/j.chaos.2023.114361
8. Demirkol AS, Sahin ME, Karakaya B, et al. Real time hybrid medical image encryption algorithm combining memristor-based chaos with DNA coding. Chaos, Solitons & Fractals. 2024; 183: 114923. doi: 10.1016/j.chaos.2024.114923
9. Vijayakumar M, Ahilan A. An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map. Ain Shams Engineering Journal. 2024; 15(4): 102620. doi: 10.1016/j.asej.2023.102620
10. Xian Y, Wang Xingyuan, Yan X, et al. Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion. Optics and Lasers in Engineering. 2020; 134: 106202. doi: 10.1016/j.optlaseng.2020.106202
11. Liu P, Wang X, Su Y. Image encryption via complementary embedding algorithm and new spatiotemporal chaotic system. IEEE Transactions on Circuits and Systems for Video Technology. 2022; 33(5): 2506–2519. doi: 10.1109/TCSVT.2023.3246520
12. Yin F, Li A, Lv C, et al. A new image encryption algorithm with feedback key mechanism using two-dimensional dual discrete quadratic chaotic map. Nonlinear Dynamics. 2024; 112(22): 20417–20435. doi: 10.1007/s11071-024-10099-8
13. Gao S, Wu R, Iu HHC, et al. Chaos-based video encryption techniques: A review. Computer Science Review. 2025; 58: 100816. doi: 10.1016/j.cosrev.2025.100816
14. Liu P, Teng L, Liu H, et al. Enhancing image security with a novel chaotic system: a focus on multiface image encryption in smart applications. IEEE Internet of Things Journal. 2025; 12(12): 20087–20098. doi: 10.1109/JIOT.2025.3542996
15. Wen H, Lin Y. Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. Expert Systems with Applications. 2024; 237: 121514. doi: 10.1016/j.eswa.2023.121514
16. Dehghani R, Kheiri H. Chaotic-based color image encryption using a hybrid method of reversible cellular automata and DNA sequences. Multimedia Tools and Applications. 2023; 83(6): 17429–17450. doi: 10.1007/s11042-023-16118-x
17. Chai X, Gan Z, Yang K, et al. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. Signal Processing: Image Communication. 2017; 52: 6–19. doi: 10.1016/j.image.2016.12.007
18. Lai Q, Liu Y. A family of image encryption schemes based on hyperchaotic system and cellular automata neighborhood. Science China Technological Sciences. 2025; 68(3): 1320401. doi: 10.1007/s11431-024-2678-7
19. Wang M, Fu X, Teng L, et al. A new 2D-HELS hyperchaotic map and its application on image encryption using RNA operation and dynamic confusion. Chaos, Solitons & Fractals. 2024; 183: 114959. doi: 10.1016/j.chaos.2024.114959
20. Wen H, Yang L, Bai C, et al. Exploiting high-quality reconstruction image encryption strategy by optimized orthogonal compressive sensing. Scientific Reports. 2024; 14(1): 8805. doi: 10.1038/s41598-024-59277-z
21. Enayatifar R, Abdullah AH, Isnin IF, et al. Image encryption using a synchronous permutation-diffusion technique. Optics and Lasers in Engineering. 2017; 90: 146–154. doi: 10.1016/j.optlaseng.2016.10.006
22. Gao S, Ho-Ching Iu H, Erkan U, et al. A 3D memristive cubic map with dual discrete memristors: design, implementation, and application in image encryption. IEEE Transactions on Circuits and Systems for Video Technology. 2025; 35(8): 7706–7718. doi: 10.1109/TCSVT.2025.3545868
23. Gao S, Zhang Z, Iu HHC, et al. A parallel color image encryption algorithm based on a 2-D logistic-rulkov neuron map. IEEE Internet of Things Journal. 2025; 12(11): 18115–18124. doi: 10.1109/JIOT.2025.3540097
24. Shi H, Wang Y, Li Y, et al. Region-based reversible medical image watermarking algorithm for privacy protection and integrity authentication. Multimedia Tools and Applications. 2021; 80(16): 24631–24667. doi: 10.1007/s11042-021-10853-9
25. Gao S, Ding S, Ho-Ching Iu H, et al. A three-dimensional memristor-based hyperchaotic map for pseudorandom number generation and multi-image encryption. Chaos: An Interdisciplinary Journal of Nonlinear Science. 2025; 35(7): 073105. doi: 10.1063/5.0270220
26. Hua Z, Yi S, Zhou Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Processing. 2018; 144: 134–144. doi: 10.1016/j.sigpro.2017.10.004
27. Su Y, Teng L, Liu P, et al. Visualized multiple image selection encryption based on log chaos system and multilayer cellular automata saliency detection. IEEE Transactions on Circuits and Systems for Video Technology. 2023; 33(9):

4689–4702. doi: 10.1109/TCSVT.2023.3246520
28. Zhang B, Rahmatullah B, Wang SL, et al. A plain-image correlative semi-selective medical image encryption algorithm using enhanced 2D-logistic map. Multimedia Tools and Applications. 2023; 82(10): 15735–15762. doi: 10.1007/s11042-022-13744-9
29. 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. 2020; 8: 122210–122228. doi: 10.1109/ACCESS.2020.3007550
30. Ping P, Zhang X, Yang X, et al. A novel medical image encryption based on cellular automata with ROI position embedded. Multimedia Tools and Applications. 2022; 81(5): 7323–7343. doi: 10.1007/s11042-021-11799-8
31. Liu P, Wang X, Zhao X, et al. Target-based image encryption via infinite interval chaotic system with Ill-conditioned parameter and 3DBDM. Expert Systems with Applications. 2023; 232: 120811. doi: 10.1016/j.eswa.2023.120811
32. Gao S, Liu J, Ho-Ching Iu H, et al. Development of a video encryption algorithm for critical areas using 2D extended Schaffer function map and neural networks. Applied Mathematical Modelling. 2024; 134: 520–537. doi: 10.1016/j.apm.2024.06.016
33. Gao S, Iu HHC, Mou J, et al. Temporal action segmentation for video encryption. Chaos, Solitons & Fractals. 2024; 183: 114958. doi: 10.1016/j.chaos.2024.114958
34. Liu H, Teng L, Zhang Y, et al. Mutil-medical image encryption by a new spatiotemporal chaos model and DNA new computing for information security. Expert Systems with Applications. 2024; 235: 121090. doi: 10.1016/j.eswa.2023.121090
35. Niu Y, Zhou H, Zhang X. Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators. Scientific Reports. 2024; 14(1): 7033. doi: 10.1038/s41598-024-57756-x
36. Li Q, Chen L. An image encryption algorithm based on 6-dimensional hyper chaotic system and DNA encoding. Multimedia Tools and Applications. 2024; 83(2): 5351–5368. doi: 10.1007/s11042-023-15550-3
37. Ye H-S, Zhou N-R, Gong L-H. Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion. Signal Processing. 2020; 175: 107652. doi: 10.1016/j.sigpro.2020.107652
38. Farah MAB, Guesmi R, Kachouri A, et al. A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. Optics & Laser Technology. 2020; 121: 105777. doi: 10.1016/j.optlastec.2019.105777
39. Jithin KC, Sankar S. Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set. Journal of Information Security and Applications. 2020; 50: 102428. doi: 10.1016/j.jisa.2019.102428
40. Hoang TM. A novel design of multiple image encryption using perturbed chaotic map. Multimedia Tools and Applications. 2022; 81(18): 26535–26589. doi: 10.1007/s11042-022-12139-0
41. Li L. A novel chaotic map application in image encryption algorithm. Expert Systems with Applications. 2024; 252: 124316. doi: 10.1016/j.eswa.2023.124316
42. Wang X, Liu P. A new full chaos coupled mapping lattice and its application in privacy image encryption. IEEE Transactions on Circuits and Systems I: Regular Papers. 2022; 69(3): 1291–1301. doi: 10.1109/TCSI.2021.3133318
43. Hu L-L, Chen M-X, Wang M-M, et al. A multi-image encryption scheme based on block compressive sensing and nonlinear bifurcation diffusion. Chaos, Solitons & Fractals. 2024; 188: 115521. doi: 10.1016/j.chaos.2024.115521
44. Alawida M. A novel DNA tree-based chaotic image encryption algorithm. Journal of Information Security and Applications. 2024; 83: 103791. doi: 10.1016/j.jisa.2024.103791
45. Liu P, Teng L, Iu HHC, et al. High sensitivity image encryption algorithm based on cascaded chaotic system. Journal of Information Security and Applications. 2025; 93: 104153. doi: 10.1016/j.jisa.2025.104153
46. Kamal ST, Hosny KM, Elgindy TM, et al. A new image encryption algorithm for grey and color medical images. IEEE Access. 2021; 9: 37855–37865. doi: 10.1109/ACCESS.2021.3063237
47. Zhao M, Li L, Yuan Z. An image encryption approach based on a novel two-dimensional chaotic system. Nonlinear Dynamics. 2024; 112(22): 20483–20509. doi: 10.1007/s11071-024-10053-8
48. Wu Y, Noonan JP, Agaian S. NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT). 2011; 1(2): 31–38. Available online: http://www.cyberjournals.com/Papers/Apr2011/05.pdf
49. Enayatifar R, Guimarães FG, Siarry P. Index-based permutation-diffusion in multiple-image encryption using DNA sequence. Optics and Lasers in Engineering. 2019; 115: 131–140. doi: 10.1016/j.optlaseng.2018.11.017

50. Manikandan N, Muthaiah R, Teekaraman Y, et al. A novel random error approximate adder-based lightweight medical image encryption scheme for secure remote monitoring of health data. Security and Communication Networks. 2021; 2021: 1–14. doi: 10.1155/2021/3570904
51. Zhang B, Rahmatullah B, Wang SL, et al. A variable dimensional chaotic map-based medical image encryption algorithm with multi-mode. Medical & Biological Engineering & Computing. 2023; 61(11): 2971–3002. doi: 10.1007/s11517-023-02874-3