Hindawi
Security and Communication Networks
Volume 2023, Article ID 9781068, 1 page
https://doi.org/10.1155/2023/9781068

Retraction

Retracted: Medical Image Encryption Based on 2D Zigzag Confusion and Dynamic Diffusion

Security and Communication Networks

Received 26 December 2023; Accepted 26 December 2023; Published 29 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] S. Li, L. Zhao, and N. Yang, "Medical Image Encryption Based on 2D Zigzag Confusion and Dynamic Diffusion," *Security and Communication Networks*, vol. 2021, Article ID 6624809, 23 pages, 2021.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 6624809, 23 pages
https://doi.org/10.1155/2021/6624809

Research Article

Medical Image Encryption Based on 2D Zigzag Confusion and Dynamic Diffusion

Shanshan Li, Li Zhao, and Na Yang

College of Information Engineering, Chang'an University, Xi'an, Shanxi 710064, China

Correspondence should be addressed to Shanshan Li; sputnik@126.com and Li Zhao; 2019124043@chd.edu.cn

Received 31 December 2020; Revised 13 March 2021; Accepted 22 April 2021; Published 8 May 2021

Academic Editor: Chi-Hua Chen

For the security of medical image, a new algorithm of medical image encryption is designed. The novel algorithm is based on a chaotic system composed of the two-dimensional Sine Logistic modulation map (2D-SLMM) and the two-dimensional Hénon-Sine map (2D-HSM). The main encryption procedure includes zigzag scan scramble, pixel grey value transformation, and dynamic diffusion. On the pixel grey value transformation stage, a password feedback is added. This makes the relationship between password and key more complicated. The proposed scheme is lossless for medical image encryption and decryption. It avoids the problems of low-dimensional chaotic map such as narrow interval and few parameters, as well as the problem of the special texture and contour of medical images. The key space of the novel algorithm is big enough, and the encryption and decryption processing are sensitive to the key. Simulation and experiments validate the effectiveness and efficiency of the novel algorithm. Security analysis proves the algorithm is resistant to common attacks.

1. Introduction

Medical images contain important personal privacy information of patients. To protect the confidential content, medical images are usually encrypted. The conventional encryption methods, such as Advanced Encryption Standard (AES) [1], Data Encryption Standard (DES) [2, 3], International Data Encryption Algorithm (IDEA), and Triple-DES [4], are usually employed to protect the text data. Medical image data have uneven distribution of image pixels, obvious regional features, and high resolution. Traditional encryption methods are not suitable for protecting Digital Imaging and Communications in Medicine (DICOM) images due to the lack of efficiency for bulk data [5]. Chaotic maps have been widely used in several medical image cryptosystems because of the prominent characters, such as tremendous high ergodicity, unpredictability, and sensitivity to initial values [6, 7]. Tremendous chaotic encryption algorithms and various improved methods have been proposed [8–10]. DNA-based coding has also been adopted for image encryption [11]. DNA-based coding had been proved to be inadequate to withstand chosen-cipher attacks and known-plaintext analysis. The main drawback of chaotic systems was their limited accuracy in digital computers. Kumar et al. [12] proposed a new encryption scheme for medical data. It applied the fractional discrete cosine transform (FrDCT) on the image and performed chaotic mapping on the FrDCT coefficients. Ye et al. [13] proposed a new meaningful image encryption algorithm based on compressive sensing and information hiding technology, which reduced the possibility of attack by hiding the presence of a common image. Researchers combined various classical algorithms in chaotic systems. Ye et al. [14] proposed an asymmetric image encryption algorithm based on the RSA cryptosystem and fractional chaotic system. Different keys for encryption and decryption were designed under an asymmetric architecture. The RSA algorithm and fractional chaotic system were combined to encrypt images. The chaotic system was combined with phase-truncated short-time fractional Fourier transform (PTSTFrFT), two-

dimensional linear canonical transform (2D LCT), and quaternion discrete fractional Hartley transform (QDFrHT) [15–17].

The existing medical image encryption methods hardly achieved a balance between security and efficiency. The reason is that most of the algorithm did not consider the medical image texture characteristics. Medical image encryption with hyperchaotic systems and high-dimensional chaotic systems were secure enough while introducing more complexity. This paper proposed a medical image encryption based on 2D zigzag confusion and dynamic diffusion. The chaotic system used in the novel encryption scheme is composed of two-dimensional chaotic map. Compared with high-dimensional chaotic systems, its structure is relatively simple, and the time complexity is reduced. Compared with the low-dimensional chaotic map, its structure is more complex, so it is more difficult to predict and analyse. These characters of the system balance security and effectiveness of the proposed method. The algorithm could be used to encrypt grayscale images of any size. And it is easy to be implemented for colorful images when they are represented by different color channels.

The rest of this article is organized as follows. Section 2 will introduce the related concepts applied in the proposed algorithm and analyse the contribution of the proposed algorithm. In Section 3, we will introduce the encryption process and decryption process of the scheme in detail. Section 4 will provide simulation results and safety analysis, and Section 5 will present conclusions.

2. Related Concepts

In this section, we introduce the two-dimensional zigzag confusion, random selection chaotic system, and improved cat map involved in the proposed scheme.

2.1. Two-Dimensional Zigzag Confusion. The 2D zigzag scan [18, 19] was used to scramble the pixel positions of the medical image to destroy the high correlation between adjacent pixels. The operation started from the first pixel of the medical image matrix, the subsequent pixels were traversed in 2D zigzag mode [20], and the traversing process stretched the two-dimensional matrix into a one-dimensional sequence; the specific process is shown in Figure 1. For example, for a matrix of size5 × 5, the starting position is $(1, 1)$, and the scrambling matrix starts at element 45. The original matrix and one-dimensional sequence after 2D zigzag scan are shown in Figure 2.

2.2. Chaotic System. This paper chooses two two-dimensional chaotic maps to form a random selection system for image pixel grey value disturbance and diffusion: 2D Sine Logistic modulation map (2D-SLMM) and 2D Hénon-Sine map (2D-HSM). Their parameter settings determine the nonlinear systems' behaviour.

2.2.1. Two-Dimensional Sine Logistic Modulation Map. The 2D-SLMM is composed of two typical one-dimensional Logistic map [21–23] and Sine map. The Logistic and Sine

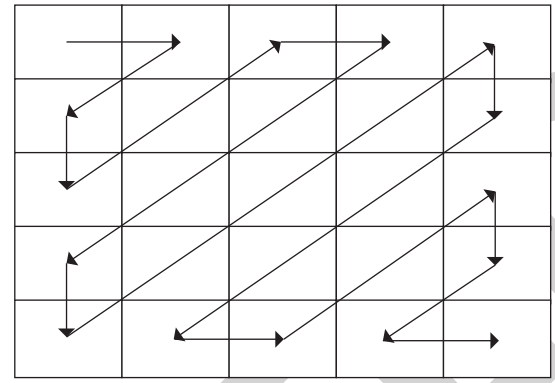


Figure 1: The zigzag path.

chaotic maps are nonlinear transformations with simple structure. Therefore, they are easy to be analysed and predicted. Researchers have confirmed that it has security problems [24]. In order to solve this problem, Hua et al. [25] designed a 2D Sine Logistic modulation map and further proved it has greater advantages in security and efficiency than other high-dimensional chaotic systems. The two-dimensional Sine Logistic modulation map is defined as follows:

$$\begin{cases} x_{i+1} = \alpha\left(\sin\left(\pi y_i\right) + \beta\right) x_i\left(1 - x_i\right), \\ y_{i+1} = \alpha\left(\sin\left(\pi x_{i+1}\right) + \beta\right) y_i\left(1 - y_i\right), \end{cases} \tag{1}$$

where $x_i, y_i \in [0, 1]$, $\alpha \in [0, 1]$, and $\beta \in [0, 3]$. When parameter $\alpha \in [0.905, 1]$ and β is close to be 3, the 2D Sine Logistic map will be hyperchaotic.

2.2.2. Two-Dimensional Hénon-Sine Map. Wu et al. [26] proposed a 2D Hénon-Sine map consisting of Hénon map and Sine map by studying two-dimensional Hénon map and one-dimensional Sine map. Compared with the original two chaotic maps, the 2D Hénon-Sine map has more complex trajectories, which makes it more unpredictable. Its mathematical expression is defined as follows:

$$\begin{cases} x_{i+1} = \left(1 - \varphi \sin^2\left(x_i\right) + y_i\right) \bmod 1, \\ y_{i+1} = \gamma x_i \bmod 1, \end{cases} \tag{2}$$

where the value ranges of parameters φ and γ are extended to $(-\infty, +\infty)$. When parameter$\varphi \in [-\infty, -0.71) \cup [0.71, +\infty)$ and $\gamma = 0.7$, or $\varphi \in R$ and $\gamma \notin [-1, 1]$, the 2D Hénon-Sine map is chaotic, and the chaotic range is larger.

2.2.3. Improved Cat Map. Cat map [27, 28] was proposed by Russian mathematician Vladimir Igorevich Arnold, also known as Arnold map. Because the image of cats is often used as an example, it is called "cat map." This is a chaotic map method that performs repeated folding and stretching transformation in a limited area and is generally applied to multimedia chaotic encryption. In order to better hide the statistical characteristics of medical images, the cat map is improved to make it nonlinear. Assuming the size of the

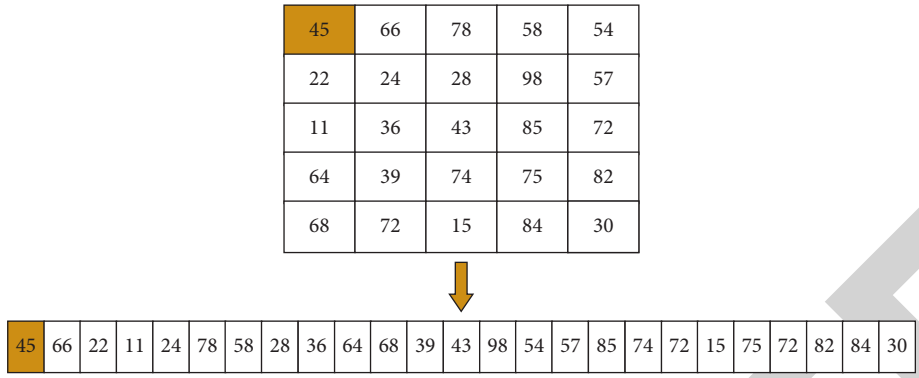


Figure 2: Zigzag confusion result with the starting position $(1, 1)$.

medical image matrix is $M \times N$, the improved cat map is defined as

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ bq & abq+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} + \begin{bmatrix} 0 \\ x_{i+1}^2 \end{bmatrix} \bmod \begin{bmatrix} M \\ N \end{bmatrix}, \quad (3)$$

where $a, b, c, d \in Z_+$, and $q = (N/\gcd(M, N))$, Z_+ represents the positive integer, and $\gcd(\cdot)$ represents the greatest common divisor. (x_i, y_i) is the pixel position before mapping. According to the theorem that the reversible transformation of the finite integer transformation must have a transformation period, the improved cat map has periodic reversibility. The original image can be restored according to this characteristic.

2.3. Performance Evaluation. The proposed chaotic system possesses good chaotic behaviours. In this subsection, the trajectory and Lyapunov exponent are used to evaluate the chaotic performance of the chaotic system.

2.3.1. Trajectory. We set the initial values of 2D-SLMM and 2D-HSM to be the same as the 2D Logistic map [25], Hénon map [26], two-dimensional logistic tent modular map (2D-LTMM) [29], and improved Hénon map [30], and the initial value is set to $(0.528, 0.135)$. Their parameters are set to the values that ensure six maps to have excellent chaotic behaviours. Figures 3(c)–3(f) show the trajectories of 2D-SLMM, 2D-HSM, improved Hénon map, and 2D-LTMM, respectively. Compared with the phase diagrams of the 2D Logistic map and Hénon map shown in Figures 3(a) and 3(b), 2D-SLMM and improved Hénon have a larger distribution area. 2D-HSM and 2D-LTMM are distributed across the entire phase plane. This observation shows that 2D-SLMM, 2D-HSM, improved Hénon, and 2D-LTMM have better ergodicity and more random output.

2.3.2. Lyapunov Exponent. An important feature of chaos is that a small uncertainty of the initial state will cause the high-speed output to increase exponentially. In a nonchaotic system, trajectories close to each other converge exponentially or diverge at an exponential rate. The rate of convergence or divergence of the system's trajectory can be described by Lyapunov exponent (LE) λ [31, 32]. Lyapunov exponent of 2D-SLMM and 2D-HSM is calculated in this subsection. Positive LE means that even if the initial state changes slightly, the final output is completely different. Therefore, when $\lambda > 0$, the dynamic system is chaotic and has hyperchaotic behaviors when it has more than one positive LE values. Figures 4(a)–4(f) show the LE spectrum of 2D Logistic map, Hénon map, 2D-SLMM, 2D-HSM, improved Hénon map, and 2D-LTMM with their corresponding parameters, respectively. 2D-HSM has chaotic behavior when $\gamma \notin [-1, 1]$, $\varphi \in \mathrm{R}$. The maximum Lyapunov exponent of 2D-HSM is greater than 0. When $\alpha \in [0.78, 0.89]$, 2D-SLMM has chaotic behaviors because its LE value is positive. And when $\alpha \in [0.89, 1]$., 2D-SLMM has hyperchaotic behaviors because its two LE values are positive. Both values become greater when α is close to 1. Compared with the LE values of other 2D chaotic maps shown in Figure 4, the 2D-HSM and 2D-SLMM have wider chaotic range, a larger LE value, and therefore a more complex trajectory. Its output is also more unpredictable.

2.4. Major Contribution of the Study. In the proposed encryption algorithm, the chaotic system is composed of two two-dimensional chaotic maps. Compared with the low-dimensional chaotic map, its structure is more complex, so it is difficult to predict and analyse, which improves the security of the system. Compared with the high-dimensional chaotic map, its structure is relatively simple, and the time complexity is therefore reduced, which improves the execution efficiency of the algorithm. A cipher feedback is applied at pixel grey value transformation processing. The coefficient of cat map transformation is generated by chaotic sequence, which makes the relationship between cipher and secret key more complicated. Cipher feedback and chaotic iteration are adopted in diffusion process. The effect of diffusion is related not only to the secret key, but also to the plaintext itself. The proposed algorithm considers the texture characteristics of medical images and chaotic mapping

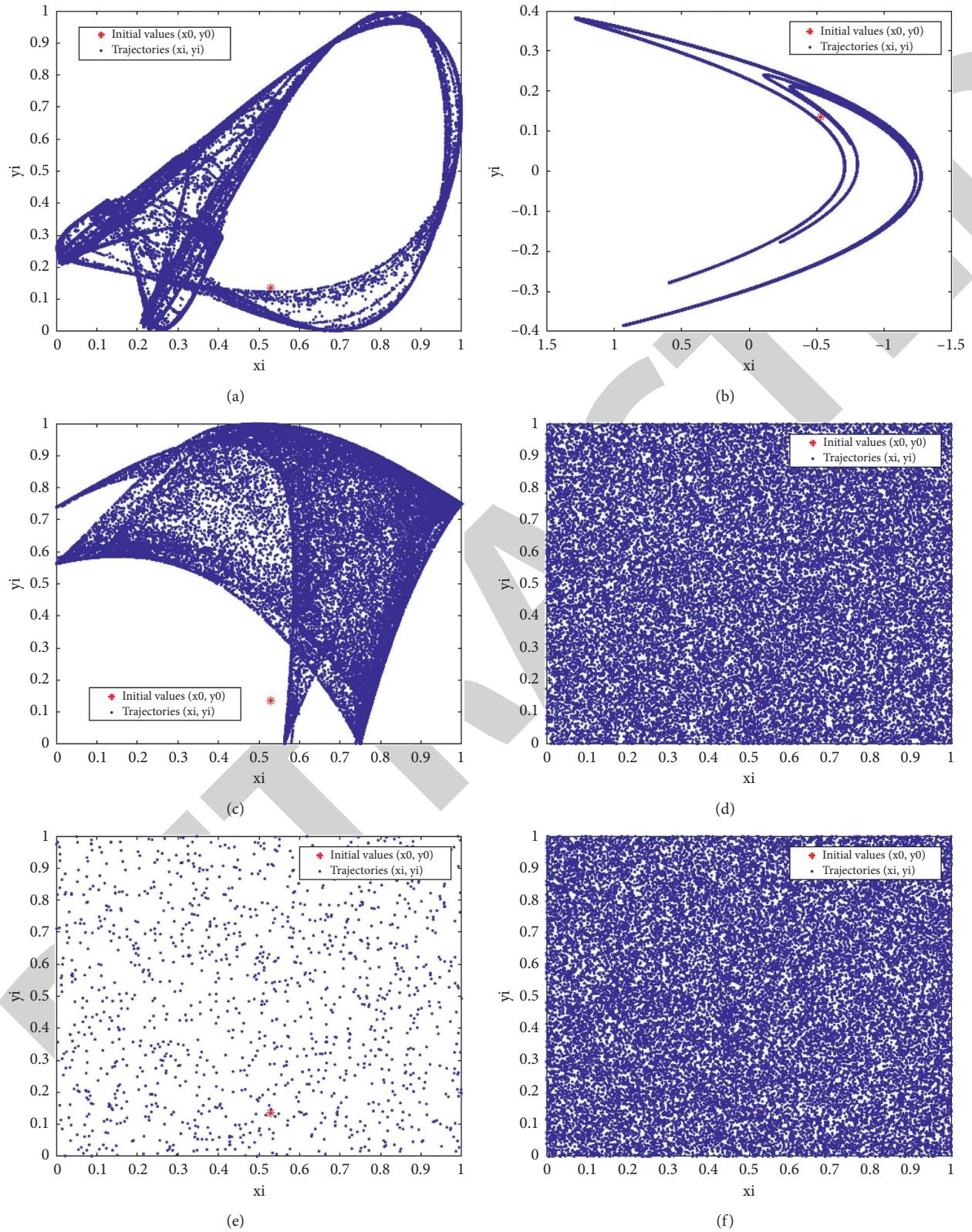


Figure 3: Trajectories of six 2D chaotic maps: (a) the 2D Logistic map with parameters $r = 1.19$, (b) the Hénon map with parameter $a = 1.4$ and $b = 0.3$, (c) the 2D-SLMM with parameter $\alpha = 1$ and $\beta = 3$, (d) the 2D-HSM with parameter $\varphi = 8$ and $\gamma = 3$, (e) the improved Hénon map with parameter $a = 50$ and $b = 50$, and (f) the 2D-LTMM with parameter $a = 50$ and $b = 50$.

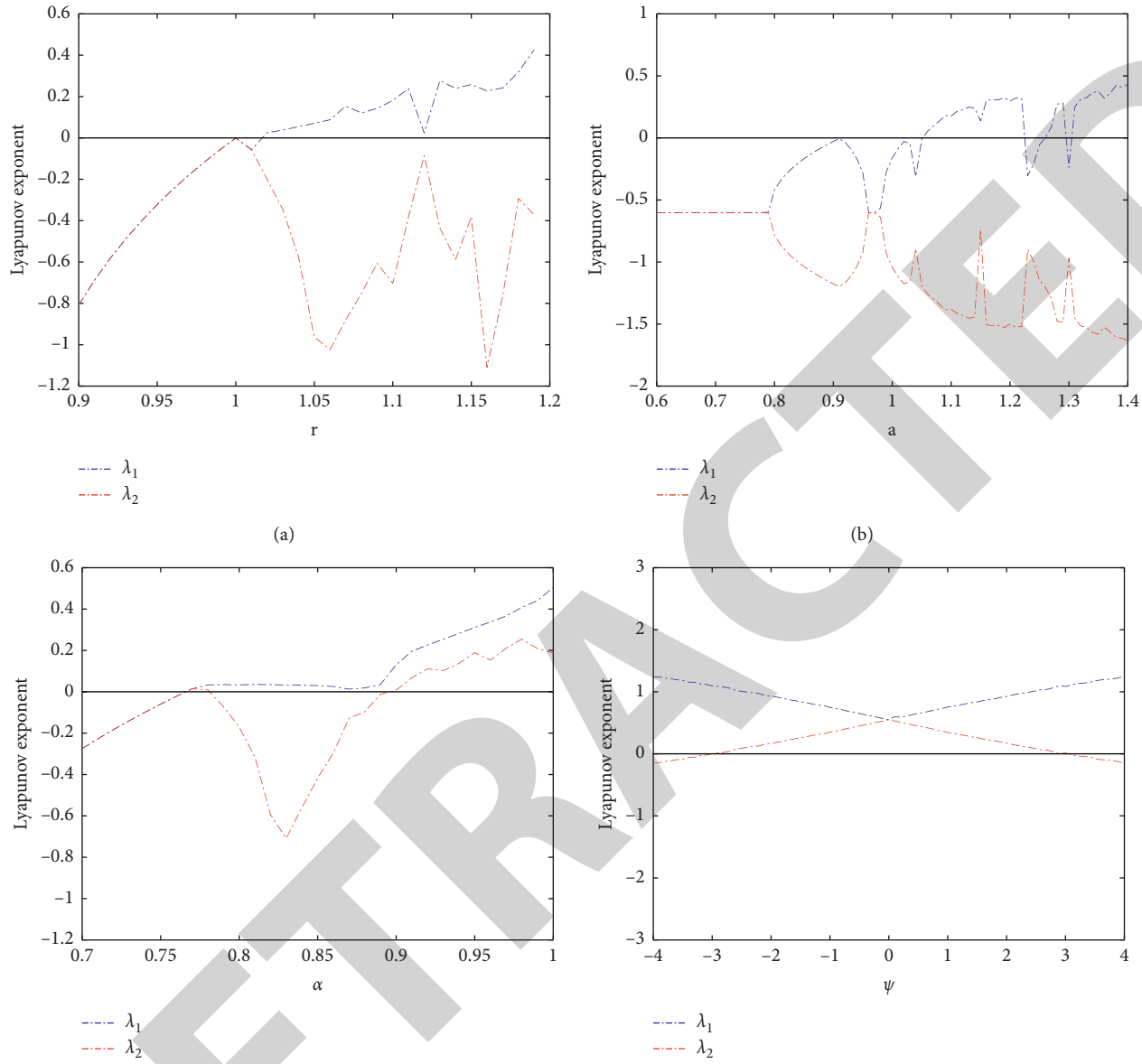


Figure 4: Continued.

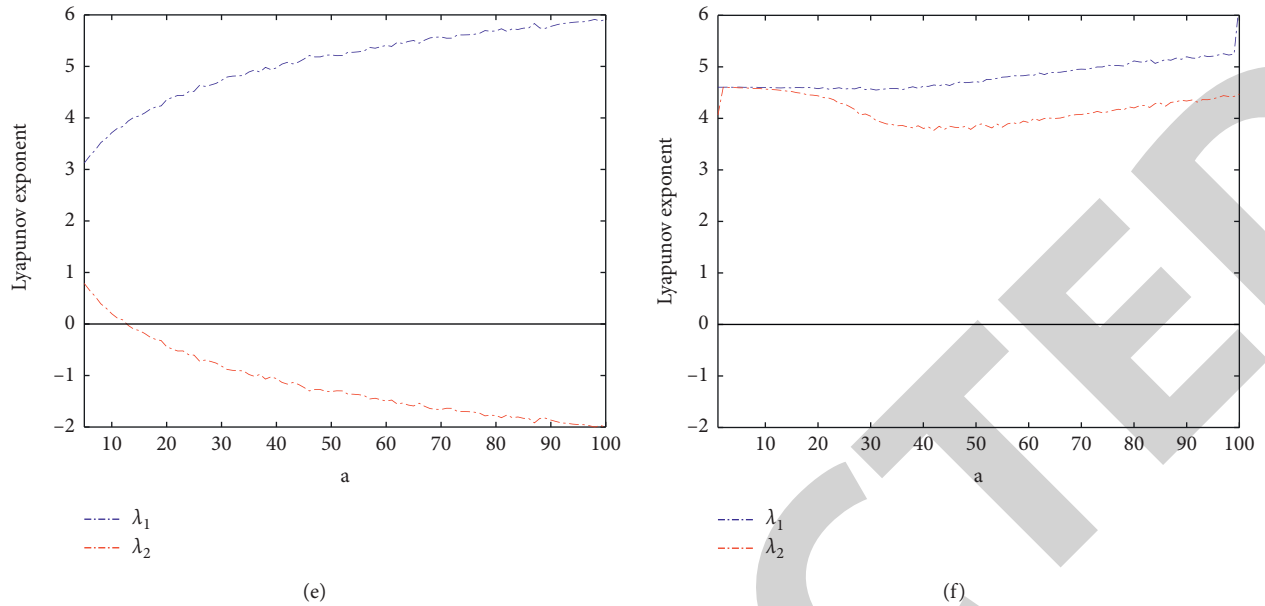


Figure 4: The LE distributions of six 2D chaotic maps: (a) the 2D Logistic map, (b) the Hénon map ($b = 0.3$), (c) the 2D-SLMM ($\beta = 3$), (d) the 2D-HSM ($\gamma = 3$), (e) the improved Hénon map ($b = 50$), and (f) the 2D-LTMM ($b = 50$).

characteristics to achieve a balance between security and effectiveness.

3. Proposed Scheme

3.1. Permutation Process. Image pixel position scrambling refers to the pixel position shuffle and rearrangement. The goal of pixel position scrambling is to destroy the correlation between adjacent pixels of the image and make the scrambling image chaos-like. It makes the algorithm resistant to plaintext attack and cipher attack. In this paper, the medical image pixel position is scrambled according to the following steps:

(i) Step 1: the original medical image is a two-dimensional matrix $\mathbf{P}$. Let us say that the size of the two-dimensional matrix $\mathbf{P}$ is $M \times N$, where $i = 1, 2, 3, \ldots, M$ and $j = 1, 2, 3, \ldots, N$.

(ii) Step 2: separating the even-numbered and odd-numbered rows of the image matrix $\mathbf{P}$ where $i = 1, 2, 3, \ldots, (M/2)$. For elements in even rows, the rule is to exchange the element in row $2i$ with element in row $M + 2 - 2i$. All even-numbered row elements are scrambled according to this rule. For elements in odd row, the rule is to exchange the element in row $2i - 1$ with element in row $M + 1 - 2i$ until all rows of all image matrices are scrambled. Let us call the scrambled two-dimensional matrix $\mathbf{P}_1$.

(iii) Step 3: separating the even and odd columns of the image matrix $\mathbf{P}_1$ where $j = 1, 2, 3, \ldots, (N/2)$. The odd column exchanges the element in column $2j - 1$ with the element in column $N + 1 - 2j$. All odd-numbered column elements are scrambled according to this rule. For elements in even column, the rule is to exchange the element in column $2j$ with element in column $N + 2 - 2j$ until all columns of all image matrices are scrambled. Get a two-dimensional matrix $\mathbf{P}_2$ after a round of scrambling.

(iv) Step 4: the 2D zigzag scan is used to scramble the image matrix $\mathbf{P}_2$ after one round of scrambling. The scrambling method is shown in Figure 1, and the before and after changes of the scrambling are shown in Figure 2. After scrambling, the two-dimensional image matrix $\mathbf{P}_2$ is stretched to the one-dimensional image sequence $\mathbf{S}$.

3.2. Image Pixel Grey Value Disruption Process. The transformation of image pixel grey value can diffuse the pixel value to confuse the relationship between cipher and plaintext, especially to eliminate the texture features of medical images such as the distribution of pixels in the grey histogram of medical images. The more uniform the distribution of pixels, the stronger the ability to resist statistical attacks. The specific process of disruption is described as follows:

(i) Step 1: the chaotic map selected when disturbing the elements in the image sequence $\mathbf{S}$ after scrambling is as described in equation (4). Here, $\mathbf{K}(\mathbf{i})$ is the random selection of the chaotic system map mentioned earlier:

$$\mathbf{K}(\mathbf{i}) = \begin{cases} \alpha(\sin(\pi y + \beta))x(1-x), \\ \alpha(\sin(\pi x) + \beta)y(1-y), \\ \left(1 - \varphi \sin^2(w) + z\right) \bmod 1, \\ \gamma w \bmod 1. \end{cases} \tag{4}$$

(ii) Step 2: the chaotic initial value is input, and four pseudorandom sequences are generated through iteration of equation (4) for $M \times N + 200$ times. In order to eliminate the transient effect, the first 200 numbers of each sequence are discarded to obtain pseudorandom sequences $\mathbf{k}_1$, $\mathbf{k}_2$, $\mathbf{k}_3$, and $\mathbf{k}_4$.

(iii) Step 3: selecting the pseudorandom sequence $\mathbf{k}_1$ and $\mathbf{k}_2$ to combine, and a new pseudorandom sequence $\mathbf{k}_5$ is generated by using equation (6). Two positive integers m_1 and m_2 are input. Equations (5), (6), and (7) are used to select the elements corresponding to the pixels to be scrambled in the image vector from the chaotic sequence $\mathbf{k}_5$ to generate the control coefficient of cat map form the cat map coefficient matrix $\mathbf{E}$ reflected in equation (8), where $i = 1, 2, 3, \ldots, ((M \times N)/2)$, and floor refers to rounding down:

$$\begin{cases} \text{key1} = m1 \bmod 30, \\ \text{key2} = m2 \bmod 30, \end{cases} \tag{5}$$

$$\begin{cases} \mathbf{k}_5(2i-1) = \mathbf{k}_1(2i-1) + \mathbf{k}_2(2i-1) - \text{floor}\left(\mathbf{k}_1(2i-1) + \mathbf{k}_2(2i-1)\right), \\ \mathbf{k}_5(2i) = \mathbf{k}_1(2i) + \mathbf{k}_2(2i) - \text{floor}\left(\mathbf{k}_1(2i) + \mathbf{k}_2(2i)\right), \end{cases} \tag{6}$$

$$\begin{cases} a = \text{floor}\left(\mathbf{k}_5(2i-1) \times 10^{\text{key1}}\right) \bmod 10, \\ b = \text{floor}\left(\mathbf{k}_5(2i) \times 10^{\text{key2}}\right) \bmod 10, \end{cases} \tag{7}$$

$$\mathbf{E} = \begin{bmatrix} 1 & a \\ bq & abq + 1 \end{bmatrix}. \tag{8}$$

(iv) Step 4: equation (9) is used to transform the grey value of the pixels in the one-dimensional image sequence $\mathbf{S}$, until all the pixels are transformed to obtain the transformed one-dimensional image sequence $\mathbf{D}$ where $\mathbf{E}$ is the coefficient matrix of the cat map during the encryption process and L is the grey level:

$$\begin{bmatrix} d_{2i-1} \\ d_{2i} \end{bmatrix} = E \begin{bmatrix} s_{2i-1} \\ s_{2i} \end{bmatrix} + \begin{bmatrix} 0 \\ d_{2i-1}^2 \end{bmatrix} \bmod L. \tag{9}$$

3.3. Diffusion Process. In this paper, the logic of dynamic diffusion is used to carry out diffusion operation on image pixels, and the following is a description of the specific process. The cipher feedback involved can effectively diffuse the influence of the current cipher value to all subsequent cipher values. Based on this idea, it is also possible to associate the current cipher value with a pseudorandom integer sequence and combine chaotic iteration and cipher feedback to diffuse image pixels. In this way, the confusion and diffusion effects of the image are not only related to the characteristics of the image but also related to the encryption key, which further improves the diffusion performance of the algorithm:

(i) Step 1: similarly, the pseudorandom integer sequences $\mathbf{k}_1$ and $\mathbf{k}_3$ are combined, $\mathbf{k}_2$ and $\mathbf{k}_4$ are combined, two positive integers $m3$ and $m4$ are input, and new pseudorandom integer sequences $\mathbf{k}_6$ and $\mathbf{k}_7$ are generated by using equations (10) and (11), where $i = 1, 2, 3, \ldots M \times N$, and floor refers to rounding down:

$$\begin{cases} \text{key3} = m3 \bmod 256, \\ \text{key4} = m4 \bmod 256, \end{cases} \tag{10}$$

$$\begin{cases} \mathbf{k}_6 = \text{floor}\left(\left(\left(\mathbf{k}_1(i) + \mathbf{k}_3(i)\right) - \text{floor}\left(\mathbf{k}_1(i) + \mathbf{k}_3(i)\right)\right) \times 10^{\text{key3}}\right) \bmod 256, \\ \mathbf{k}_7 = \text{floor}\left(\left(\left(\mathbf{k}_2(i) + \mathbf{k}_4(i)\right) - \text{floor}\left(\mathbf{k}_2(i) + \mathbf{k}_4(i)\right)\right) \times 10^{\text{key4}}\right) \bmod 256. \end{cases} \tag{11}$$

(ii) Step 2: when $i = 1$, the first pixel of the image sequence is encrypted according to equation (12), and $\oplus$ represents bitwise XOR operation:

$$\begin{cases} \text{sum1} = \sum_{i=2}^{M\times N} d(i), \text{sum2} = 0, c(1) = d(1) \oplus k6(1) \oplus k7((1) \oplus \text{mod}(\text{sum1} + k6(1), 256). \end{cases} \tag{12}$$

(iii) Step 3: when $i = i + 1$, the i-th pixel of the image sequence is encrypted according to

$$\begin{cases} \text{sum1} = \text{sum1} - d(i), \\ \text{sum2} = \text{sum2} + c(i-1), \\ c(i) = d(i) \oplus \text{mod}(\text{sum1} + k6(i), 256) \oplus \text{mod}(\text{sum2} + k7(i), 256). \end{cases} \tag{13}$$

(iv) Step 4: if $i < M \times N$, return to step 9 to continue execution. Otherwise, the final encrypted one-dimensional sequence $\mathbf{C}$ is obtained. The one-dimensional sequence $\mathbf{C}$ is reconstructed into a two-dimensional matrix $\mathbf{C}_1$ with size $M \times N$ in a column-by-column manner which is the encrypted image, and the encryption process ends.

3.4. Procedures of Proposed Schemes

3.4.1. Encryption Process. The encryption process of the proposed scheme is shown in Figure 5. The specific process of encryption is presented in Algorithm 1.

3.4.2. Decryption Process. The decryption process of the proposed scheme is shown in Figure 6. The specific process of decryption is presented in Algorithm 2.

4. Experimental Results and Security Analysis

Three digital medical images of ultrasound, CT, and MRI $k7$with size 512×512 involved in the experiment are collected from the National Library of Medicine's Open Access Biomedical Images Search Engine (https://openi.nlm.nih.gov). The two medical images of X-ray and CT-kidney with size 1024×1024 are from AI studio (https://aistudio.baidu.com/aistudio). The configuration environment of the experimental host is CPU of Intel Core I7-6700, with 8 GB RAM, 3.40 GHz processor, and 64 bit Windows 7 operating system. The experiment uses MATLAB (R2019b) software to realize the simulation test. In the experiment, the initial value of the chaotic system reflected by equation (4) is $x_0 = 0.106$, $y_0 = 0.204$, $w_0 = 0.301$, and$z_0 = 0.203$, and the parameter setting values used in equations (5) and (10) are $m1 = 2$, $m2 = 3$, $m3 = 4$, and $m4 = 3$.

4.1. Encryption and Decryption Effect and Analysis. The algorithm presented in this paper is used to encrypt the test image. The encryption and decryption results are shown in Figure 7. The first column is plaintext images, the second is cipher image, and the third is decryption image. It can be seen the second column of Figure 7 that the cipher images appear noise-like. It also can be observed that the algorithm presented by this paper can effectively solve the obvious contour problem. From the third column of Figure 7, when the encryption and decryption keys are the same and the image is not tampered, the decryption algorithm can restore the original medical image without distortion.

4.2. Statistical Attack. Statistical attack mainly refers to illegal intruder trying to predict and analyse plaintext image and their encryption and decryption keys based on the distribution of pixel grey value. The analysis of statistical attack could be performed as correlation coefficient analysis and grey histogram analysis.

4.2.1. Correlation Coefficient Analysis. The correlation of adjacent pixels in an image refers to the relationship between two adjacent elements in the three directions of horizontal, vertical, and diagonal. It is specifically reflected by the covariance, with a range in interval $[-1, 1]$. The correlation of adjacent pixels is proportional to the value of correlation coefficient. The closer the value of correlation coefficient to 1 indicates stronger correlation between image pixels. Otherwise the correlation is weak. The calculation of correlation coefficient is defined by

$$\begin{cases} D(x) = \dfrac{1}{n\sum_{i=1}^{n}(x_i - E_x)^2}, \\ \text{cov}(x, y) = \dfrac{1}{n\sum_{i=1}^{n}(x_i - E_x)(y_i - E_y)}, \\ r = \dfrac{\text{cov}(x, y)}{(\sqrt{D(x)}\sqrt{D(y)})}, \end{cases} \tag{14}$$

where E_x and E_y are the mathematical expectations of x and y, respectively, n is the number of pixels, $\text{cov}(x, y)$ is the covariance of x and y, and r is the correlation coefficient.

Table 1 shows the correlation coefficients of adjacent pixels of plaintext and cipher of some medical images. The correlation coefficients of adjacent pixels of plaintext of medical images are close to 1, while the correlation coefficients of adjacent pixels of cipher images tend to 0. It indicates that the adjacent pixels of plaintext image have strong correlation, and the adjacent pixels of cipher image

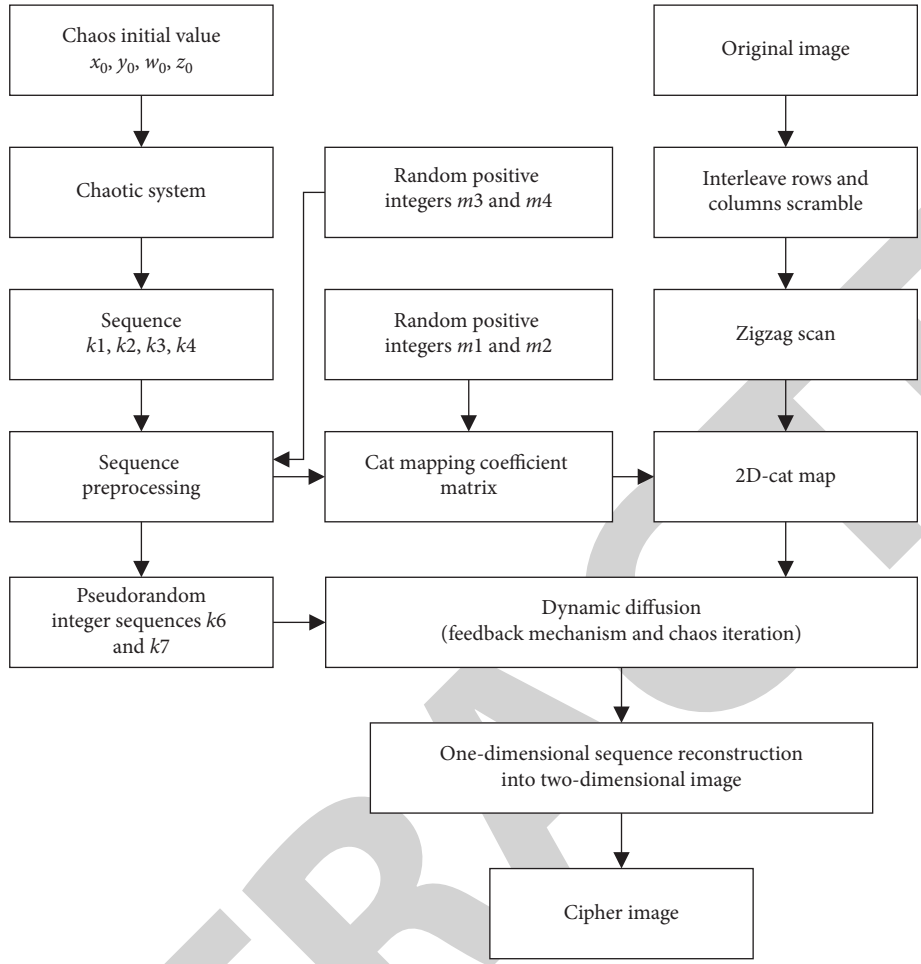


Figure 5: The encryption process of the proposed algorithm.

Input: the original medical image $\mathbf{P_o}$ of size $M \times N$, the secret keys x_0, y_0, w_0, z_0, $m1$, $m2$, $m3$, $m4$.
Output: the cipher image $\mathbf{P_c}$
(1) $\mathbf{S} \leftarrow$ Permute $\mathbf{P_o}$ with the rules in Section 3.1.
(2) Obtain pseudorandom sequences $\mathbf{k}_1$, $\mathbf{k}_2$, $\mathbf{k}_3$, and $\mathbf{k}_4$ using equation (4) with initial values x_o, y_o, w_o, z_o.
(3) $q \leftarrow (N/\gcd(M, N))$
  key1,key2 $\leftarrow$ use equation (5) with control parameters $m1$, $m2$.
  for i from 1 to $((M \times N)/2)$
  $\mathbf{k}_5 \leftarrow$ use equation (6) with pseudorandom sequences $\mathbf{k}_1$, $\mathbf{k}_2$.
  $a, b \leftarrow$ use equation (7) with $\mathbf{k}_5$ and key1,key2.
  $\mathbf{S_e}(2i-1) \leftarrow (\mathbf{S}(2i-1) + a\mathbf{S}(2i)) \bmod 256$.
  $\mathbf{S_e}(2i) \leftarrow (bq\mathbf{S}(2i-1) + (abq+1)\mathbf{S}(2i) + \mathbf{S_e}^2(2i-1)) \bmod 256$.
  end for
(4) key3,key4 $\leftarrow$ use equation (10) with control parameters m_3, m_4.
(5) Cipher image $\mathbf{P_e} \leftarrow$ Diffuse $\mathbf{S_e}$ with the steps in Section 3.3.

Algorithm 1: The proposed encryption algorithm.

are basically no longer correlated. The algorithm is effective for scrambling.

Figure 8 shows the adjacent pixel distribution of the CT image and its encrypted image in the horizontal, vertical, and diagonal directions. It can be found that the pixels of the plaintext image are basically distributed around the diagonal, indicating that the correlation between adjacent pixels of the plaintext image is very strong, while the distribution of pixels of the cipher image is irregular. The correlation between adjacent pixels of the cipher image is low.

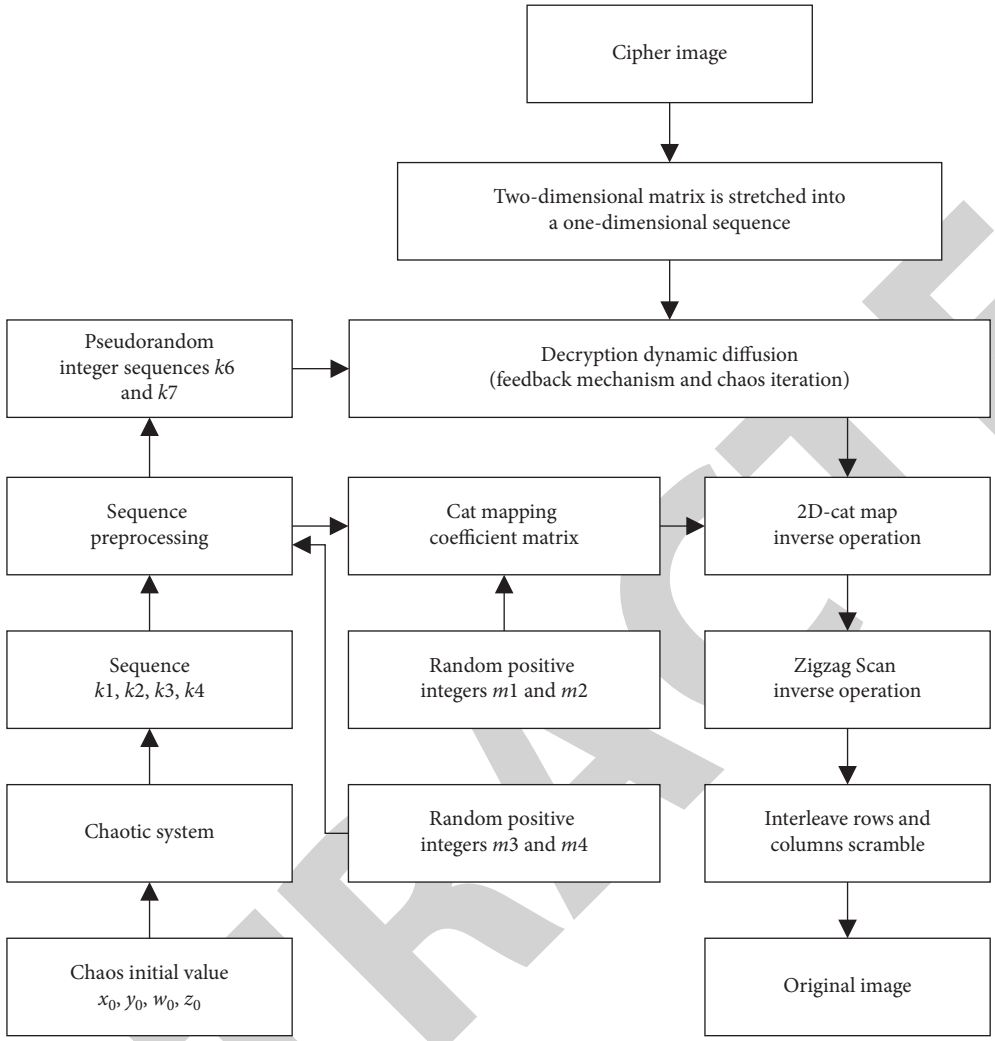


Figure 6: The decryption process of the proposed algorithm.

Input: the cipher image $\mathbf{P_c}$ of size $M \times N$, the secret keys $m1$, $m2$, $m3$, $m4$, x_0, y_0, w_0, z_0.
Output: the decrypted image $\mathbf{P_d}$
(1) $\mathbf{S_c} \leftarrow$ Stretch $\mathbf{P_c}$ in a column-by-column manner.
(2) Obtain pseudorandom sequences $\mathbf{k}_1$, $\mathbf{k}_2$, $\mathbf{k}_3$, and $\mathbf{k}_4$ using equation (4) with initial values x_o, y_o, w_o, z_o.
(3) key3, key4$\leftarrow$ use equation (10) with control parameters m_3, m_4.
for i from $M \times N$ to 1
$\mathbf{k}_6, \mathbf{k}_7 \leftarrow$ use equation (11) with pseudorandom sequences $\mathbf{k}_1$, $\mathbf{k}_2$, $\mathbf{k}_3$, $\mathbf{k}_4$, and key3,key4.
if $i \leftarrow M \times N$
sum1$\leftarrow$0, sum2$\leftarrow\sum_{i=2}^{M\times N} S_c(i)$
$\mathbf{S_d}(M \times N) \leftarrow \mathbf{S_c}(M \times N) \oplus \mathrm{mod}(\mathrm{sum1} + k6(M \times N), 256) \oplus \mathrm{mod}(\mathrm{sum2} + k7(M \times N), 256)$
else if $i \leftarrow 1$
sum1$\leftarrow$sum1 + $\mathbf{S_d}(i+1)$, sum2$\leftarrow\sum_{i=2}^{M\times N} \mathbf{S_c}(i)$
$\mathbf{S_d}(1) \leftarrow \mathbf{S_c}(1) \oplus k6(1) \oplus k7(1) \oplus \mathrm{mod}(\mathrm{sum1} + k6(1), 256)$
else
sum1$\leftarrow$sum1 + $\mathbf{S_d}(i+1)$,sum2$\leftarrow$sum2 $-$ $\mathbf{S_c}(i)$
$\mathbf{S_d}(i) \leftarrow \mathbf{S_c}(i) \oplus \mathrm{mod}(\mathrm{sum1} + k6(i), 256) \oplus \mathrm{mod}(\mathrm{sum2} + k7(i), 256)$
end if
end for
(4) $q \leftarrow (N/\gcd(M, N))$
key1,key2 $\leftarrow$ use equation (5) with control parameters $m1$, $m2$.

Algorithm 2: Continued.

for i from 1 to $((M \times N)/2)$
$\mathbf{k}_5$.← use equation (6) with pseudorandom sequences $\mathbf{k}_1$, $\mathbf{k}_2$.
a,b.← use equation (7) with pseudorandom sequences and control parameters $\mathbf{k}_5$ and key1,key2.
$\mathbf{S}_{\mathbf{d}1}(2i-1) = ((abq+1)\mathbf{S}_{\mathbf{d}}(2i-1) - a(\mathbf{S}_{\mathbf{d}}(2i) - \mathbf{S}^2_{\mathbf{d}}(2i-1)))\text{mod}256$
$\mathbf{S}_{\mathbf{d}1}(2i) = (-bq\mathbf{S}_{\mathbf{d}}(2i-1) + \mathbf{S}_{\mathbf{d}}(2i) - \mathbf{S}^2_{\mathbf{d}}(2i-1) + 256)\text{mod}256$
end for
(5) $\mathbf{C}_{\mathbf{d}} \leftarrow$ Permute $\mathbf{S}_{\mathbf{d}1}$ with the inverse process of 2D zigzag scan.
(6) Decrypted image $\mathbf{P}_{\mathbf{d}} \leftarrow$ Permute $\mathbf{C}_{\mathbf{d}}$ with the rules of step 2 and step 3 in Section 3.1.

Algorithm 2: The proposed decryption algorithm.

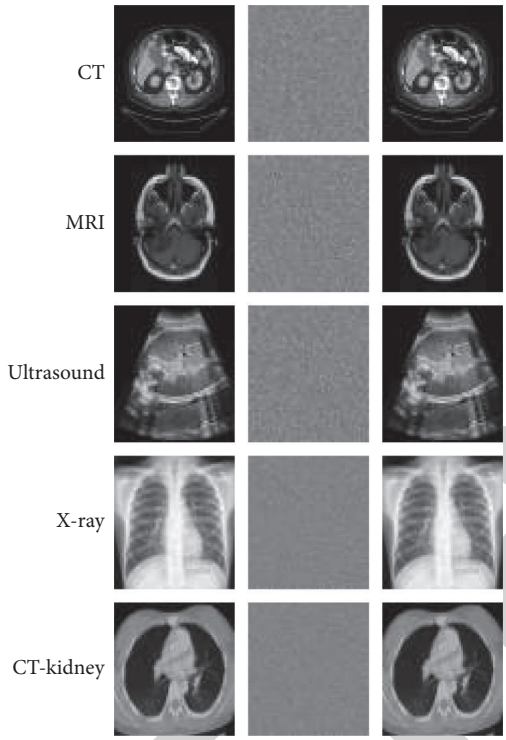


Figure 7: Samples of the original digitized image on the left, the cipher image on the middle, and the decrypted digitized medical image on the right.

4.2.2. Histogram Analysis. Image histogram is one of the commonly used metrics for evaluating the robustness of the cipher algorithm against statistical attacks. The histogram is a graph drawn according to the frequency of each grey value in the image, which reflects the most basic statistical characteristics of the image. The histogram of encrypted images should be different from the histogram of original images and have uniform level grayscale values to resist the statistic attack. The first column of Figure 9 is the original image of 4 medical images, the second column is the grey histogram of the original image, the third column is the grey histogram corresponding to the encrypted image, and the fourth column is the grey histogram corresponding to the decrypted image. The pixel distribution of the original medical image is uneven, while the pixel distribution of the encrypted medical image is uniform. The histogram of the original medical image is the same as that of the decrypted medical image, but they are completely different from that of the encrypted medical image. The histogram of encrypted images is resistant to statistical attack.

Table 1: Correlation coefficient of the original images and its encrypted image.

Images	Direction	Correlation coefficient	
		Original image	Encrypted image
CT (512 × 512)	Horizontal	0.9809	0.0012
	Vertical	0.9597	−1.8721e-04
	Diagonal	0.9493	4.3539e-04
MRI (512 × 512)	Horizontal	0.9913	0.0027
	Vertical	0.9907	−4.8855e-04
	Diagonal	0.9829	−7.9588e-04
Ultrasound (512 × 512)	Horizontal	0.9966	3.4296e-04
	Vertical	0.9889	6.9743e-04
	Diagonal	0.9858	8.5018e-04
X-ray (1024 × 1024)	Horizontal	0.9956	−1.7713e-04
	Vertical	0.9944	0.0015
	Diagonal	0.9914	0.0016
CT-kidney (1024 × 1024)	Horizontal	0.9984	−0.0009
	Vertical	0.9987	−0.0017
	Diagonal	0.9972	0.0006

The histogram of encrypted image can also be analysed quantitatively by calculating the variance of original, encrypted, and decrypted images. The low value of variance shows high grayscale uniformity, and inversely, the high value of variance shows low grayscale uniformity. The variance can be calculated as

$$\text{Var}(V) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\left(v_i - v_j\right)^2}{2}, \tag{15}$$

where V is the vector of all v_i's and v_j's, $M \times N$ is the size of the image, v_i and v_j are the number of pixels for a particular grayscale values i, and j is the testing image which are the values of the i-th and j-th bins of the corresponding histogram. $\text{Var}(V)$ is the variance of array V.

Table 2 compares the variance of different plain images, the corresponding cipher images, and decryption images. In Table 2, the encrypted image variance is greatly differed from the original image. This shows that the histograms of encrypted images are different from the original. For each row, the variance of the encrypted image is much smaller than that of the original image. It shows that the histogram of the encrypted image has greater consistency. The

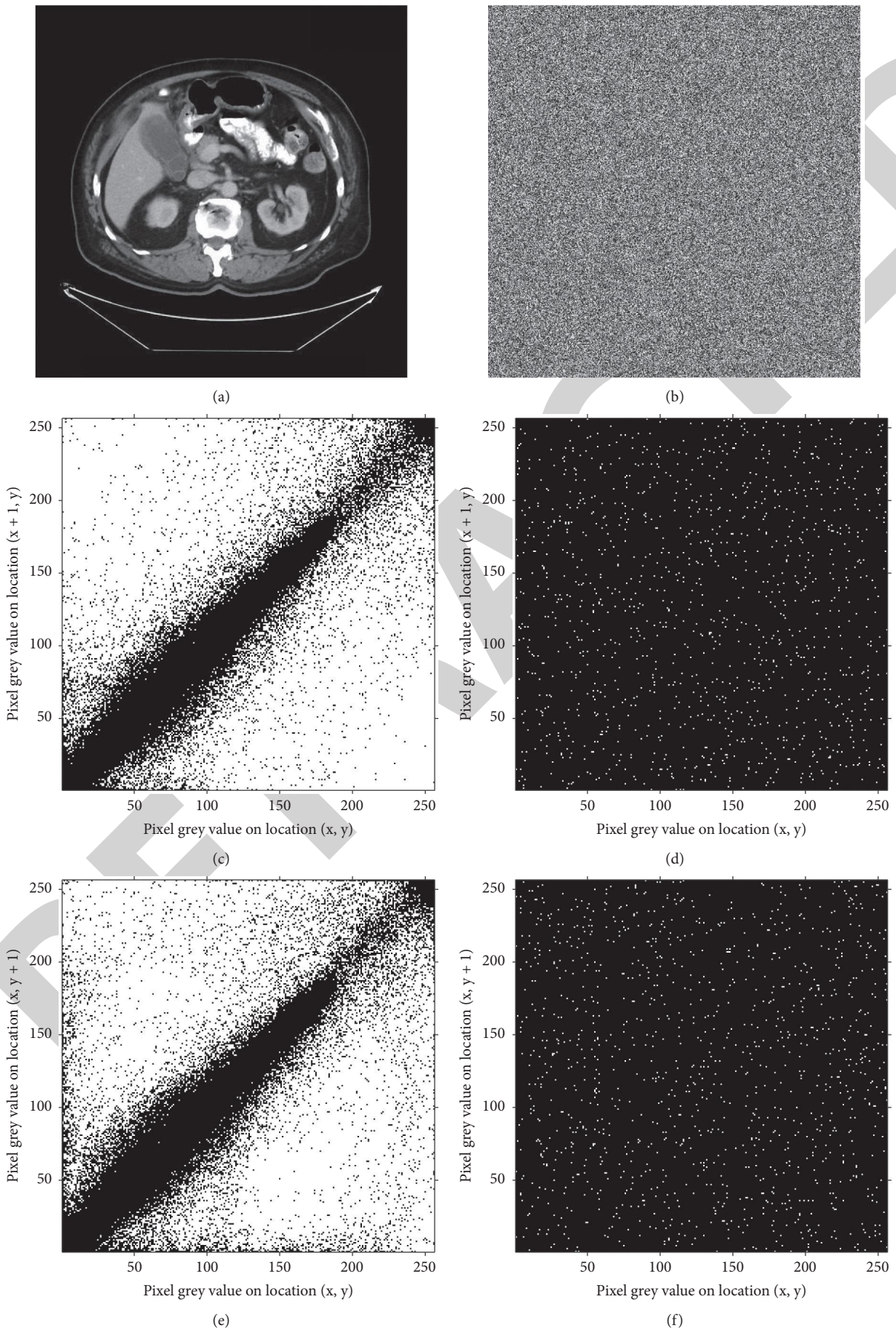


Figure 8: Continued.

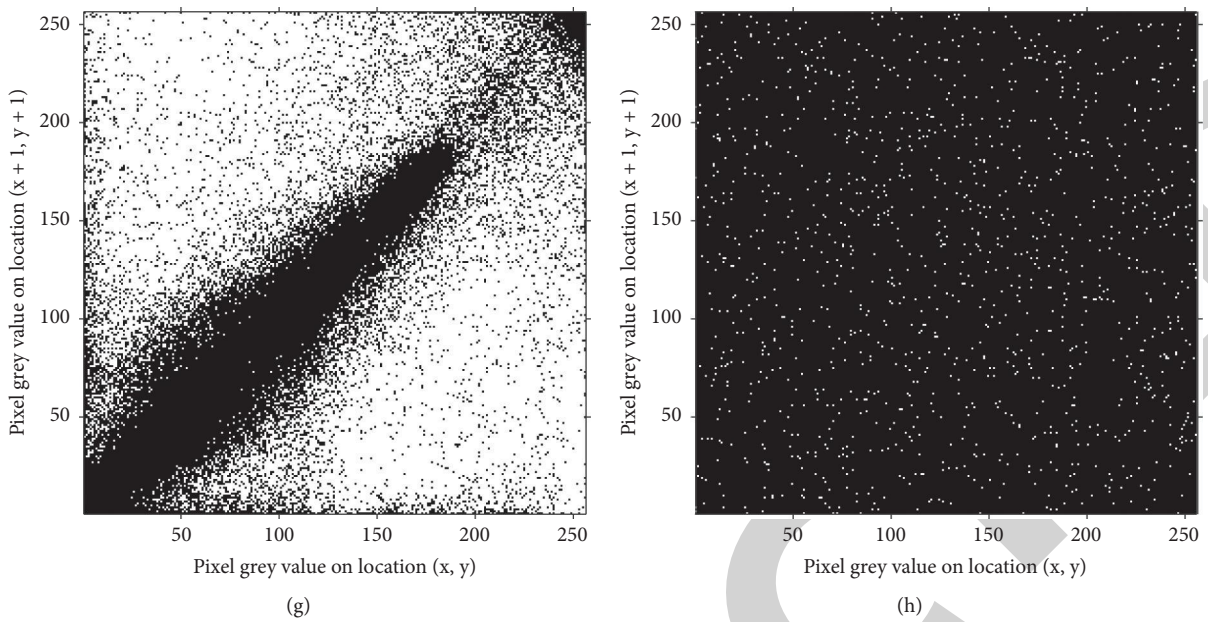


Figure 8: (a, b) Original images and cipher images, (c, d) horizontal correlation of original images and cipher images, (e, f) vertical correlation of original images and cipher images, and (g, h) diagonal correlation of original images and cipher images.

decrypted image variance is equal to the original image. This shows that the original image and the decrypted image are the same, and there is no information loss during the encryption and decryption process. From this discussion, it could be concluded that the proposed algorithm is resistant to statistical attack.

We further verify the uniformity of grayscale value distribution of encrypted images using the chi-square test. The low value of chi-square shows high uniformity. It is defined as

$$\begin{cases} X^2 = \sum_{i=1}^{L} \dfrac{(\text{obs}_i - \text{exp}_i)^2}{\text{exp}_i}, \\ \text{exp}_i = \dfrac{M \times N}{L}, \\ \text{obs}_i(i) = \dfrac{n_i}{M \times N}, \end{cases} \tag{16}$$

where obs_i is the observed frequency of i, n_i is the total number of occurrences of i, exp_i is the expected frequency of i, $M \times N$ is the size of the image, and L is the grey level. Small value of X^2 shows that the pixel distribution is uniform. The chi-square values for the test images are tabulated in Table 3. It is obvious that $X^2 < X^2_{\text{th}}(256, 0.05) = 293.247893$ [33], reflecting the efficiency of the proposed cipher to conceal the spatial redundancy of the plain image.

4.3. Global Information Entropy Analysis. Global information entropy is an important index used to measure whether the grey value distribution is uniform in an image. The greater the global information entropy of the image, the more uniform the grey value distribution of the image, and the greater the possibility of resisting entropy attacks. The theoretical global entropy value of the original random image with 256 grey levels is 8. The global information entropy of the image in the algorithm is calculated by [34]

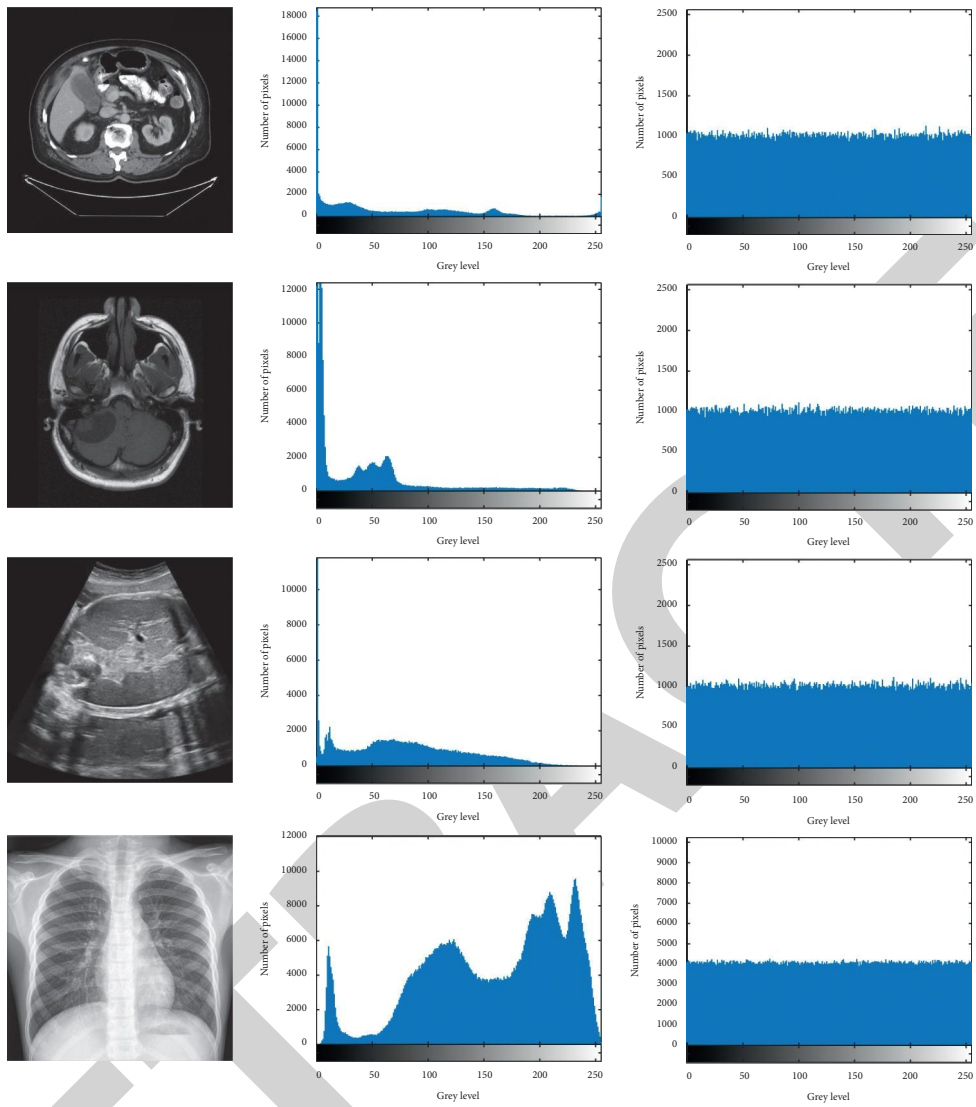
$$H(G) = \sum_{i=1}^{L-1} P(G_i) \log_2 \frac{1}{P(G_i)}, \tag{17}$$

where G_i is the grey value of the image pixels, $P(G_i)$ is the probability of G_i appearing in the image, and L is the grey level.

Table 4 shows the global entropy values of different medical plaintext images and the corresponding global entropy values of encrypted cipher images. The global entropy values of original images are in the 4-th column. All of them are smaller than 8, which means that the original images are meaningful. The last column of Table 4 presents the global entropy values of encrypted images by the proposed algorithm. The values are close to 8, which means that the encrypted images are more random-like.

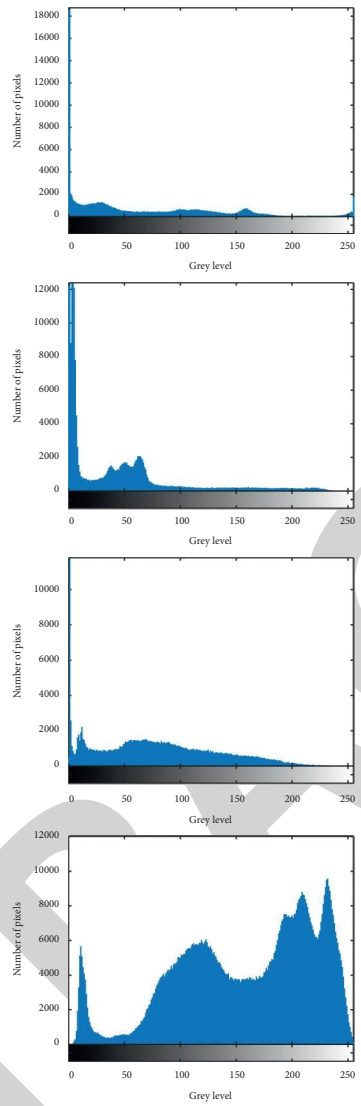
4.3.1. Local Shannon Entropy Analysis. The global information entropy is unfair for the comparisons between images of different sizes, and failure to discern image randomness before and after image shuffling. Local Shannon entropy overcomes these weaknesses of the global Shannon entropy. It measures the exact randomness of pixels in encrypted images [6]. It is the mean value of entropy of several nonoverlapping blocks of the image. The local Shannon entropy is defined as [35]

$$\overline{H_{k,T_B}(S)} = \sum_{i=1}^{k} \frac{H(S_i)}{k}, \tag{18}$$



(a) (b) (c)

Figure 9: Continued.



(d)

Figure 9: (a) Original digitized image, histogram of (b) original digitized image, (c) cipher image, and (d) decrypted digitized medical image.

Table 2: Histogram variance of images using the proposed scheme.

Images (grey)	Original	Encrypted	Decrypted
CT (512 × 512)	55231643.7109	1017.6250	55231643.7109
MRI (512 × 512)	23507412.3359	1031.7422	23507412.3359
Ultrasound (512 × 512)	21233944.1641	1058.0547	21233944.1641
X-ray (1024 × 1024)	6310177.8047	4175.5625	6310177.8047
CT-kidney (1024 × 1024)	24031572.7188	4102.8359	24031572.7188

Table 3: Comparison of the chi-square value between our proposed approach and the other proposals.

Images	Size	Original	Encrypted	Decrypted
CT	512 × 512	13807910.9277	254.4063	13807910.9277
MRI	512 × 512	5876853.0840	257.9355	5876853.0840
Ultrasound	512 × 512	5308486.0410	264.5137	5308486.0410
X-ray	1024 × 1024	394386.1128	260.9727	394386.1128
CT-kidney	1024 × 1024	1501973.2949	256.4272	1501973.2949

Table 4: Global entropy values of different images.

Images	Type	Size	Global entropy values	
			Orig. image	Encrypted image
CT	Grey	512 × 512	4.8150	7.9993
MRI	Grey	512 × 512	5.4672	7.9993
Ultrasound	Grey	512 × 512	6.2947	7.9993
X-ray	Grey	1024 × 1024	7.6744	7.9998
CT-kidney	Grey	1024 × 1024	7.0475	7.9998

where k is the number of nonoverlapping blocks of an information source S, T_B is the total number of pixels in each of the nonoverlapping blocks, and $S_1, S_2, \ldots, S_k$ are the nonoverlapping blocks having information entropies $H(S_1), H(S_2), \ldots, H(S_k)$, respectively.

In this paper, we set the number of nonoverlapping blocks $k = 30$ and the total number of pixels in each of the block $T_B = 1936$. The (k, T_B)-local Shannon entropy is used as the measurement describing the randomness over the entire test image. The local entropy also has optimal value for various significance levels such as 5%, 1%, and 0.1% [36]. Table 5 provides the acceptance interval of the local entropy test under various significance levels of the proposed algorithm. The local Shannon entropy value of all the images is within the range of acceptance interval of 0.05, 0.01, and 0.001 significance levels. This proves the high randomness of pixel values in the encrypted images using the proposed scheme. Table 6 presents the obtained experimental values for different cipher images, and they come from the existing method and our method, respectively. It is obvious that these values are extremely nearby to the maximum value of 8. It indicates the information leakage from the proposed cipher algorithm insignificant.

4.4. Differential Attack. Differential attack means that the attacker can extract the information of the original image through the research of the cipher image. It is analysed and verified by the unified average change intensity (UACI) and the number of changing pixel rate (NPCR). NPCR measures the number of changed pixel values between the two encrypted images by changing one pixel value in the original image. The range of NPCR is $[0, 1]$. It is defined as equation (19). UACI measures the average changing intensity between the two encrypted images by changing one pixel value in the original image. The range of UACI is $[0, 1]$ as well, which is defined in equation (20):

$$\begin{cases} \mathrm{NPCR} = \dfrac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N}, \\ D(i,j) = \begin{cases} 0, c(i,j) = c'(i,j), \\ 1, c(i,j) \neq c'(i,j), \end{cases} \end{cases} \tag{19}$$

$$\mathrm{UACI} = \frac{\sum_{i=1}^{M}\left(\sum_{j=1}^{N}\left|c(i,j) - c'(i,j)\right|/(L-1)\right)}{M \times N}, \tag{20}$$

where M and N are, respectively, the width and height of the medical image, L is the grey level, and $c(i, j)$ and $c(i, j)'$ are the encrypted image and the encrypted image corresponding after changing a pixel grayscale value, respectively.

In this section, we randomly change the value of a pixel in a grayscale image, and Tables 7 and 8 show the NPCR and UACI results of the test image, respectively. The optimal value of NPCR and UACI is related to the size and type of the image. Wu et al. [40] proposed the theoretical critical value of NPCR and UACI. In Tables 7 and 8, the NPCR and UACI values of all images are slightly below the critical value. This indicates that the protection against differential attacks of the proposed scheme is not very strong. We will work on this problem in our future study.

4.5. Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) Analysis. Mean square error (MSE) measures the difference between original and encrypted images. And also it measures the difference between original and decrypted images. Greater value of MSE indicates greater difference between two images [41]. It can be calculated as

$$\begin{cases} \mathrm{MSE}_{\mathrm{OC}} = \dfrac{1}{M \times N}\displaystyle\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[O(i,j) - C(i,j)]^2, \\ \mathrm{MSE}_{\mathrm{OD}} = \dfrac{1}{M \times N}\displaystyle\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[O(i,j) - D(i,j)]^2, \end{cases} \tag{21}$$

where M is the width and N is the height of the image. $O(i, j)$, $C(i, j)$, and $D(i, j)$ represent the pixel grey value of the plaintext image, the cipher image, and the decrypted image in the i-th row and j-th column, respectively.

Peak signal-to-noise ratio (PSNR) measures the fidelity of an image [41]. Smaller value of PSNR indicates greater difference between original and encrypted images [41]. The mathematical expression for the calculation of PSNR is given in

$$\begin{cases} \mathrm{PSNR}_{\mathrm{OC}} = 20 \times \log_{10}\left(\dfrac{\mathrm{MAX}_I}{\sqrt{\mathrm{MSE}_{\mathrm{OC}}}}\right), \\ \mathrm{PSNR}_{\mathrm{OD}} = 20 \times \log_{10}\left(\dfrac{\mathrm{MAX}_I}{\sqrt{\mathrm{MSE}_{\mathrm{OD}}}}\right), \end{cases} \tag{22}$$

where MAX_I represents the pixel grey level of the image. $\mathrm{MSE}_{\mathrm{OC}}$ is the MSE between the original image and the encrypted image, and $\mathrm{MSE}_{\mathrm{OD}}$ is the MSE between the

Table 5: Local Shannon entropy values of different images.

Images (grey)	Size	Local Shannon entropy (reference range) [37, 38]	Local Shannon entropy	Result
CT	512 × 512	$\alpha = 0.05$ (7.901901305,7.903037329)	7.9024	Pass
MRI	512 × 512	$\alpha = 0.01$ (7.901722822,7.903215812) $\alpha = 0.001$ (7.901515698,7,903422936)	7.9030	Pass
Ultrasound	512 × 512		7.9028	Pass
X-ray	1024 × 1024		7.9030	Pass
CT-kidney	1024 × 1024		7.9027	Pass

Table 6: Comparison of information entropy results.

Algorithms	Images	Global Shannon entropy	Local Shannon entropy ($k = 30T_B = 1936$)
Ours	CT	7.9993	7.9024
	MRI	7.9993	7.9030
	Ultrasound	7.9993	7.9028
	X-ray	7.9998	7.9030
Ravichandran et al. [6]	MR_1	7.9992	7.9020
	CT_1	7.9993	7.9023
Chai et al. [39]	Brone	7.9994	7.9015

Table 7: NPCR results for test images.

Tested image size M-by-N 512-by-512		NPCR critical value [40]		
		$N^*_{0.05} = 99.5893\%$	$N^*_{0.01} = 99.5810\%$	$N^*_{0.001} = 99.5717\%$
Name	NPCR (%)	NPCR test results		
		0.05-level	0.01-level	0.001-level
CT	98.6767	Fail	Fail	Fail
MRI	98.2585	Fail	Fail	Fail
Ultrasound	98.6725	Fail	Fail	Fail
Tested image size M-by-N 1024-by-1024		NPCR critical value [40]		
		$N^*_{0.05} = 99.5994\%$	$N^*_{0.01} = 99.5952\%$	$N^*_{0.001} = 99.5906\%$
Name (size)	NPCR (%)	NPCR test results		
		0.05-level	0.05-level	0.05-level
X-ray	98.2576	Fail	Fail	Fail
CT-kidney	98.7677	Fail	Fail	Fail

Table 8: UACI results for test images.

Tested image size M-by-N 512-by-512		UACI critical value [40]		
		$N^{*-}_{0.05} = 33.3730\%$ $N^{*+}_{0.05} = 33.5541\%$	$N^{*-}_{0.01} = 33.3445\%$ $N^{*+}_{0.01} = 33.5826\%$	$N^{*-}_{0.001} = 33.3115\%$ $N^{*+}_{0.001} = 33.6156\%$
Name	UACI (%)	UACI test results		
		0.05-level	0.01-level	0.001-level
CT	32.3884	Fail	Fail	Fail
MRI	31.4729	Fail	Fail	Fail
Ultrasound	32.4262	Fail	Fail	Fail
Tested image size M-by-N 1024-by-1024		UACI critical value [40]		
		$N^{*-}_{0.05} = 33.4183\%$ $N^{*+}_{0.05} = 33.5088\%$	$N^{*-}_{0.01} = 33.4040\%$ $N^{*+}_{0.01} = 33.5231\%$	$N^{*-}_{0.001} = 33.3875\%$ $N^{*+}_{0.001} = 33.5396\%$
Name (size)	UACI(%)	UACI test results		
		0.05-level	0.05-level	0.05-level
X-ray	31.5516	Fail	Fail	Fail
CT-kidney	32.8412	Fail	Fail	Fail

original image and the decrypted image. Table 9 presents the MSE and PSNR results of the test images. The results show that there is a great difference between the original image and the encrypted image, and no difference between the original image and the decrypted image. The large MSE_{OC} value proves that the proposed scheme is secure and robust against different statistical attacks.

4.6. Exhaustive Attack

4.6.1. Key Space Analysis. With the rapid development of computer technology, the key space of encryption algorithms must be large enough to withstand exhaustive attacks, and a key space of 2^{128} or more is required for an algorithm [42]. The secret keys involved in this algorithm have three

Table 9: MSE and PSNR results of the test images using the proposed schemes.

Images	Size	MSE_{OC}	MSE_{OD}	$PSNR_{OC}$	$PSNR_{OE}$
CT	512×512	17124.0626	0	5.7947	∞
MRI	512×512	16892.8865	0	5.8538	∞
Ultrasound	512×512	13338.4275	0	6.8798	∞
X-ray	1024×1024	10290.1876	0	8.0066	∞
CT-kidney	1024×1024	10039.2025	0	8.1138	∞

parts: 4 initial values needed to generate the chaotic sequence, 2 secret keys needed to generate the cat map control coefficient, and 2 initial values used for dynamic diffusion. The whole system is under the condition of double precision, grey value of 256, and 64 bit Windows7 Operating System. According to the IEEE floating point standard, the calculation precision of 64 bit double data is 10^{15} [43]. So, the secret key space of the algorithm can be reached $(10^{15})^8 = 10^{120}$. The algorithm has a large enough secret key space. It is computationally unfeasible to crack the secret key by exhaustive search.

4.6.2. Key Sensitivity Analysis. Secret key sensitivity ensures that the attacker cannot use a secret key close to the actual secret key to decrypt the original image. Any small change in the secret key should get very different encryption results. There are 8 security keys in our scheme, which are the initial values x_0, y_0, w_0, and z_0 of the chaotic system in equation (4), the parameters m_1 and m_2 in equation (5), and the parameters m_3 and m_4 in equation (10). The 8 security keys are slightly changed according to the following rules. One of secret key is updated by Δk and other keys unchanged. Due to the selection of the initial values x_0, y_0, w_0, and z_0 during the test is in the range of $(0, 1)$, Δk is selected as 0.001. Since m_1, m_2, m_3, and m_4 are random positive integers, the Δk is ± 1.

In order to analyse the key sensitivity, NPCR and UACI are calculated to evaluate the difference between cipher text images. The original medical image is encrypted using the key distributed as the same as before, and the corresponding cipher image is denoted as C. Then, we use the modified keys $k\prime = k + \Delta k$ to encrypt the original image and denote the generated cipher as $C\prime\prime$. Some of the test results are shown in Figure 10, and the NPCR and UACI between the cipher text images generated by two security keys with only 1 bit difference are shown in Table 10. The results clearly show that the proposed image cryptosystem has sufficient key sensitivity.

4.7. Classical Types of Attacks. According to the attacker's acquisition of information, cryptanalysis can be divided into four categories [33]:

Cipher only. The attacker only knows part of the encrypted text.

Known plaintext. The attacker has obtained some given plaintext and corresponding cipher.

Chosen plaintext. The attacker not only knows the encryption algorithm but also can select the plaintext message and can get the corresponding encrypted cipher.

Chosen cipher. The attacker has access to the decryption machine and can construct the plaintext corresponding to any cipher.

The most powerful attack is to chosen plaintext attack. If a cryptographic system is resistant to this kind of attack, then it is resistant other types of attacks.

The sensitivity of the proposed algorithm to the initial parameters (m_1, m_2, m_3, and m_4) and the initial values (x_0, y_0, w_0, z_0) has been verified in detail in Section 4.6.2. If one of them is changed, the chaotic sequence, the cat mapping coefficient matrix, and the pseudorandom integer sequence will be completely different. In addition, in the dynamic diffusion stage, the encrypted value is not only related to the original pixel grey value and the key, but also related to the previous original value and the previous encrypted value. Different encrypted images have different chaotic iterations and cipher feedback. Therefore, the proposed algorithm is resistant to chosen plaintext attack.

4.8. Robustness to Noise and Data Loss. When the encrypted medical images are transmitted or stored via the network, they are easily contaminated by various noises, and data loss is extremely likely to occur. Image encryption algorithms should be robust against noise and data loss. In the proposed algorithm, the encryption and decryption processes are symmetrical. During the encryption process, a change in one pixel in the plaintext image will affect multiple pixels in the ciphertext image. In the decryption process, the change of one pixel in the ciphertext image also affects multiple pixels in the plaintext image. Therefore, the proposed algorithm has an avalanche effect. Figure 11 shows the robustness analysis results of the proposed algorithm against noise and data loss. When the ciphertext image is contaminated by salt and pepper noise or data lost, the decryption process can recover part of the original image. Although there is some noise in the restored image, we can still identify most of the image information. When the ciphertext image is contaminated by Gaussian noise or speckle noise, the decryption process of the proposed algorithm cannot restore the original image. The novel encryption algorithm is sensitive to noise and data loss. We will work on this problem in our future study.

4.9. Computational Complexity Analysis. The time-consuming parts of the proposed encryption algorithm are the generation of chaotic sequences, permutation operations,

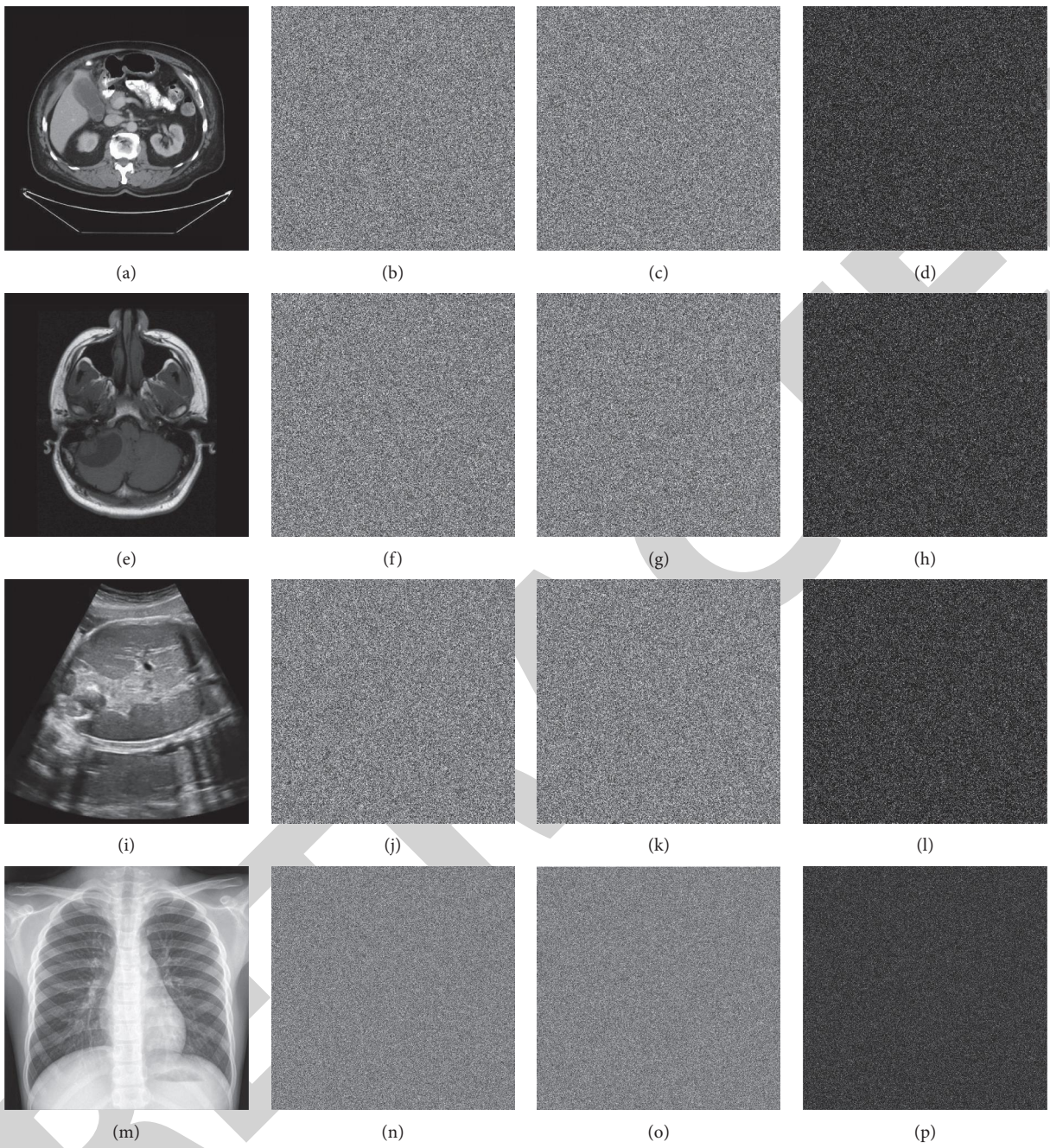


Figure 10: Key sensitivity analysis of x_0. (a), (e), (l), and (o) original images, (b), (f), (m), and (p) cipher images C, (c), (g), (i), and (q) cipher images C'', and (d), (h), (n), and (r) images of $|C - C''|$.

Table 10: Results of NPCR and UACI between cipher text images.

Cipher image		$x_0 = 106$ $x_0' = 107$	$y_0 = 0.204$ $y_0 = 0.205$	$w_0 = 0.301$ $w_0 = 0.302$	$z_0 = 0.203$ $z_0 = 0.204$	$m1 = 2$ $m1 = 3$	$m2 = 3$ $m2 = 4$	$m3 = 4$ $m3 = 5$	$m4 = 3$ $m4 = 4$
CT	NPCR (%)	99.6155	99.6140	99.6086	99.6349	98.6584	98.1796	99.6170	99.6071
	UACI (%)	33.4619	33.4497	33.3950	33.5288	32.5783	31.9500	33.4280	33.4726
X-ray	NPCR (%)	99.6153	99.5949	99.6130	99.5992	98.9952	98.5431	99.6140	99.6110
	UACI (%)	33.4954	33.4653	33.4467	33.4728	33.2973	32.6806	33.4590	33.4543

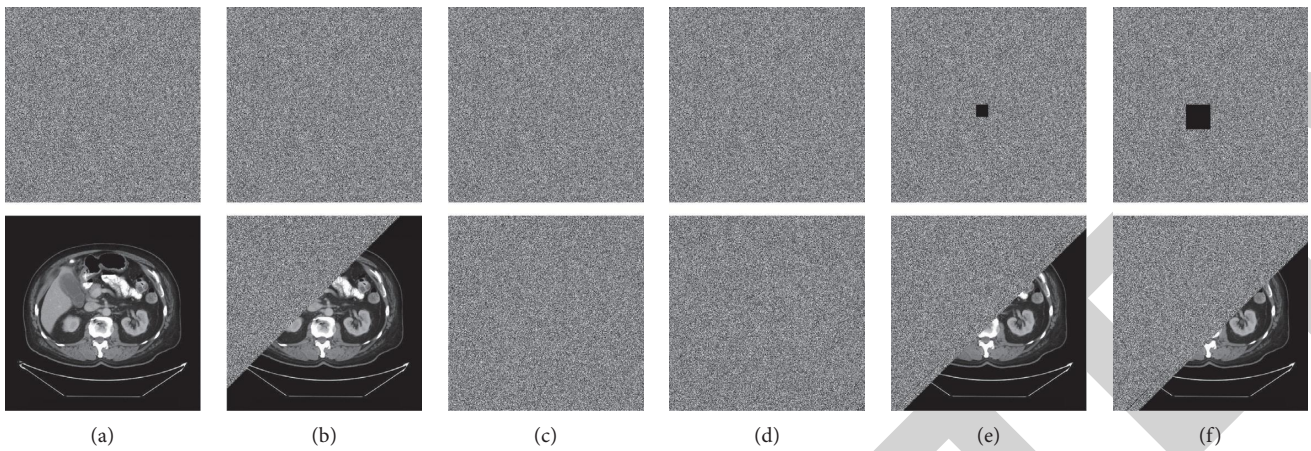


Figure 11: Robustness analysis results of noise and the data loss. (a) The ciphertext image C and its decrypted image; (b) the ciphertext image C_1 with 0.0005% salt and pepper noise and its decrypted result; (c) the ciphertext image C_2 with 0.0005% Gaussian noise and its decrypted result; (d) the ciphertext image C_3 with 0.0005% speckle noise and its decrypted result; (e) the ciphertext image C_4 with 0.390625% data loss and its decrypted result; (f) the ciphertext image C_5 with 1.5625% data loss and its decrypted result.

pixel grey value transformation, and diffusion operations. In the permutation stage, the time complexity of the first round of cross-ranking scrambling is $\Theta(M/2)$ and $\Theta(N/2)$. The time complexity of the second round of scanning using zigzag is $\Theta(M \times N - 1)$. In the chaotic sequence generation stage, two two-dimensional maps are used to form a new chaotic system. The time complexity of generating the chaotic sequence is $\Theta(4 \times M \times N)$. In the phase of pixel grey value transformation, the time complexity of adopting cat mapping transformation is $\Theta((M \times N)/2)$. In the diffusion stage, the dynamic diffusion operation is adopted the same time, and its time complexity is $\Theta(M \times N)$. The total time complexity of the proposed algorithm is $\Theta(4 \times M \times N)$.

4.10. Computational Time Analysis. The efficiency of an encryption algorithm refers to the running speed of the algorithm. Table 11 shows the time taken for the encrypting and decrypting of 5 test images, and the data of which are the average value obtained by performing 11 times on the image. The data in Table 11 reflect that the time required for the proposed algorithm to encrypt a medical image with a size of 512×512 is about 1.3s, and the time it takes to encrypt a size of 1024×1024 is about 5s.

4.11. Random Analysis. In the proposed method, a chaotic system is used to iteratively generate sequences for pixel grey value transformation and dynamic diffusion. In order to prove the effectiveness of the algorithm, a comprehensive statistical randomness test is performed on this subsection. The National Institute of Standards and Technology (NIST) statistical test suite [44] and the standard randomness test FIPS 140-2 [45] are employed for analysis.

4.11.1. NIST Analysis. The National Institute of Standards and Technology (NIST) is a United States (US) based company that provides guidelines for the protection of data. The NIST has outlined 15 significant statistical tests for cryptographic applications, which are used to determine the strength of any cryptographic algorithm and estimate the actual randomness produced by the system [46, 47]. The test was applied to the chaotic system of the proposed algorithm. And the results are shown in Table 12. All of the randomness tests have been passed. Hence, the chaotic system of the proposed scheme is chaotic enough.

4.11.2. NISTFIPS 140-2 Test Analysis. The test uses coin toss equation (23) proposed by Li et al. [48] to construct a bit sequence. Table 13 lists the randomness test results of the bit stream generated by the following different mappings and equation (23). For the bit stream generated by the chaotic map used by the algorithm, the mono bit test is 10,001. When the driving length is less than or equal to 2 or greater than or equal to 6, the run test cannot be satisfied. Other tests are satisfied. The algorithm used for pixel grey value transformation and the dynamic diffusion sequence is basically random:

$$b_i = \begin{cases} 1, & e_i \geq \text{average}(\mathbf{E}), \\ 0, & \text{else}, \end{cases} \tag{23}$$

where $\mathbf{E}$ is a chaotic sequence generated by chaos iteration, e_i is the i-th element in $\mathbf{E}$, and average$(\mathbf{E})$ denotes average value of all elements in $\mathbf{E}$.

4.12. Comparison Analysis. The proposed algorithm is compared with other existing algorithms to verify its performances. The comparison is based on the entropy, correlation coefficient, NPCR, UACI, and key space. The performance of algorithms is tabulated in Table 14. By analysing the algorithms, the key space of the proposed algorithm is larger, and the maximum entropy is greater than some existing encryption algorithms [5, 11, 12, 36, 39, 49, 50]. The proposed method has achieved a strong resistance to differential, statistical, and brute force attack.

Table 11: Results for total encryption time and decryption time using the proposed algorithm.

Images	Type	Size	Encryption time (seconds)	Decryption time (seconds)
CT	Grey	512×512	1.2933	1.1230
MRI	Grey	512×512	1.2706	1.0865
Ultrasound	Grey	512×512	1.2802	1.1032
X-ray	Grey	1024×1024	5.0880	4.4282
CT-kidney	Grey	1024×1024	5.0938	4.4502

Table 12: Test results of the sequences generated by the chaotic system with NIST SP800 suite.

Tests	P value (x_n)	Results
Frequency test	0.5356076801062	Pass
Block frequency test	0.2006251972896	Pass
Cusum-forward test	0.1534611103969	Pass
Cusum-reverse test	0.6665945788960	Pass
Runs test	0.5484500143314	Pass
Longest run test	0.2257749928343	Pass
Rank test	0.2495050092582	Pass
FFT test	0.8695796767915	Pass
Nonoverlapping template test	0.1578386990554	Pass
Overlapping template test	0.8425140482030	Pass
Universal test	0.3708348754012	Pass
Approximate entropy test	0.5610349492218	Pass
Random-excursion test ($x = -1$)	0.7857937272818	Pass
Random-excursion variant test ($x = 1$)	0.2084575927756	Pass
Serial1 test	0.1392589354394	Pass
Serial2 test	0.5800257861316	Pass
Linear complexity test	0.4039596243759	Pass

Table 13: Test results of the sequences generated by the chaotic system with FIPS 140-2 test suite.

FIPS 140-2 test	Theoretical value	2D-SLMM	2D-HSM	Proposed in equation (4)
Mono bit test	9,725–10,725	10,888	10,033	10,001
Poker test	2.16–46.17	466.4896	481.6930	12.9664
Run test of length 1 for '0'	2,315 - 2,685	2874	3665	3285
Run test of length 1 for '1'	2,315 - 2,685	4227	3684	3261
Run test of length 2 for '0'	1,114 - 1,386	1372	1772	1384
Run test of length 2 for '1'	1,114 - 1,386	1813	1778	1389
Run test of length 3 for '0'	527–723	682	909	653
Run test of length 3 for '1'	527–723	1093	972	642
Run test of length 4 for '0'	240–384	414	500	318
Run test of length 4 for '1'	240–384	487	554	327
Run test of length 5 for '0'	103–209	221	291	150
Run test of length 5 for '1'	103–209	333	324	144
Run test of length 6 for '0'	103–209	158	173	78
Run test of length 6 for '1'	103–209	181	195	75
Longest run test	≤ 26	15	15	12

Table 14: Performance comparisons.

Metrics	HC	VC	Dc	NPCR (%)	UACI (%)	Entropy	Keyspace
Banu et al. [5]	0.0019	0.0034	0.0018	99.68	33.47	7.998	10^{128}
Liu et al. [11]	0.0069	0.0216	0.0039	99.60	33.44	7.99929	$< 2^{128}$
Kumar et al. [12]	0.0860	0.0240	0.0204	99.14	32.54	4.7453	10^{60}
Lakshmi et al. [36]	0.0037	−0.0038	0.0006	99.6	33.41	7.99	10^{112}
Chai et al. [39]	−0.0293	0.0079	−0.0160	99.60	33.42	7.9991	10^{98}
Banu et al. [49]	0.00163	0.00225	0.00065	99.6067	33.47	7.9976	10^{206}
Rajagopalan et al. [50]	0.0098	0.0051	−0.0013	—	—	7.9972	$>2^{128}$
Proposed	0.0014	$7.2233e-4$	0.0002	98.536	32.10	7.9993	10^{120}

5. Conclusions

Based on the analysis of existing methods, this paper fully considers the characteristics of medical images. A medical image encryption based on 2D zigzag scan and dynamic diffusion is proposed. This method mainly uses zigzag scan, improved cat map, and dynamic diffusion algorithm. With the help of feedback mechanism and chaotic iteration, the diffusion performance of the algorithm is improved, and the contour problem in the encrypted image is solved. The performance analysis illustrates that the proposed algorithm enhances the security level and it is resistant to differential, exhaustive, and statistical attacks.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no known conflicts of interest regarding the publication of this paper.

Authors' Contributions

S. S. L. conceived and designed the study. L. Z. performed the experiment. L. Z. and N. Y. performed the data analyses and wrote the manuscript. S. S. L., L. Z., and N. Y. helped perform the analysis with constructive discussions.

Acknowledgments

This research was supported by the National Natural Science Foundation of China under grant no. 61402051 and Natural Science Basic Research Plan in Shaanxi Province of China under grant no. 2016JM6076.

References

[1] W. E. Burr, "Selecting the advanced encryption standard," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 43–52, 2003.

[2] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer Science and Business Media, New York, NY, USA, 2012.

[3] F. P. Miller, A. F. Vandome, and J. McBrewster, *Advanced Encryption Standard*, Alpha Press, Orlando, FL, USA, 2009.

[4] D. Coppersmith, D. B. Johnson, and S. M. Matyas, "A proposed mode for triple-DES encryption," *IBM Journal of Research and Development*, vol. 40, no. 2, pp. 253–262, 1996.

[5] A. S. Banu and R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," *Medical & Biological Engineering & Computing*, vol. 58, no. 7, pp. 1445–1458, 2020.

[6] D. Ravichandran, P. Praveenkumar, and J. B. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Computers in Biology and Medicine*, vol. 72, no. 5, pp. 170–184, 2016.

[7] S. Arumugham, S. Rajagopalan, and J. B. B. Amirtharajan, "Networked medical data sharing on secure medium - a web publishing mode for DICOM viewer with three layer authentication," *Journal of Biomedical Informatics*, vol. 86, pp. 90–105, 2018.

[8] N. K. Pareek, V. Patidar, and K. K. Sud, "Cryptography using multiple one-dimensional chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 10, no. 7, pp. 715–723, 2005.

[9] A. Qayyum, J. Ahmad, W. Boulila et al., "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, pp. 140876–140895, 2020.

[10] Z. Li, C. Peng, W. Tan, and L. Li, "A novel chaos-based color image encryption scheme using bit-level permutation," *Symmetry*, vol. 12, no. 9, p. 1497, 2020.

[11] H. Liu, B. Zhao, and L. Huang, "A remote-sensing image encryption scheme using DNA bases probability and two-dimensional logistic map," *IEEE Access*, vol. 7, pp. 65450–65459, 2019.

[12] S. Kumar, B. Panna, and R. K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Medical & Biological Engineering & Computing*, vol. 57, no. 11, pp. 2517–2533, 2019.

[13] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, "Image encryption and hiding algorithm based on compressive sensing and random numbers insertion," *Signal Processing*, vol. 172, p. 107563, 2020.

[14] G. Ye, K. Jiao, H. Wu, C. Pan, and X. Huang, "An asymmetric image encryption algorithm based on a fractional-order chaotic system and the RSA public-key cryptosystem," *International Journal of Bifurcation and Chaos*, vol. 30, no. 15, p. 2050233, 2020.

[15] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," *Optics and Lasers in Engineering*, vol. 124, Article ID 105816, 2020.

[16] Z.-J. Huang, S. Cheng, L.-H. Gong, and N.-R. Zhou, "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform," *Optics and Lasers in Engineering*, vol. 124, Article ID 105821, 2020.

[17] H.-S. Ye, N.-R. Zhou, and L.-H. Gong, "Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion," *Signal Processing*, vol. 175, Article ID 107652, 2020.

[18] H. Wang, D. Xiao, M. Li, Y. Xiang, and X. Li, "A visually secure image encryption scheme based on parallel compressive sensing," *Signal Processing*, vol. 155, pp. 218–232, 2019.

[19] X. L. Chai, H. Y. Wu, Z. H. Gan et al., "An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding," *Optics and Lasers in Engineering*, vol. 124, no. 1, Article ID 105837, 2020.

[20] N. K. Pareek, V. Patidar, and K. K. Sud, "Diffusion-substitution based gray image encryption scheme," *Digital Signal Processing*, vol. 23, no. 3, pp. 894–901, 2013.

[21] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Multiple image watermarking applied to health information management," *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 4, pp. 722–732, 2006.

[22] J. H. K. Wu, R.-F. Chang, C.-J. Chen et al., "Tamper detection and recovery for medical images using near-lossless information hiding technique," *Journal of Digital Imaging*, vol. 21, no. 1, pp. 59–76, 2008.

[23] J. M. Zain and A. R. M. Fauzi, "Medical image watermarking with tamper detection and recovery," *IEEE*, vol. 1, pp. 3270–3273, 2006.

[24] Z. G. Chen, D. Q. Liang, X. H. Deng et al., "Performance analysis and improvement of logistic chaotic map," *Journal of Electronics and Information Technology*, vol. 38, no. 6, pp. 1547–1551, 2016.

[25] Z. Y. Hua, Y. C. Zhou, C.-M. Pun et al., "2D Sine Logistic modulation map for image encryption," *Signal Processing*, vol. 297, pp. 80–94, 2015.

[26] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11–23, 2018.

[27] S. I. Batool and H. M. Waseem, "A novel image encryption scheme based on Arnold scrambling and Lucas series," *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 27611–27637, 2019.

[28] E. Hanouti, H. E. Fadili, and K. Zenkouar, "Breaking an image encryption scheme based on arnold map and lucas series," *Multimedia Tools and Applications*, pp. 1–23, 2020.

[29] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Information Sciences*, vol. 546, pp. 1063–1083, 2021.

[30] Z. Hua, Y. Zhang, and Y. Zhou, "Two-dimensional modular chaotification system for improving chaos complexity," *IEEE Transactions on Signal Processing*, vol. 68, pp. 1937–1949, 2020.

[31] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[32] I. I. Shevchenko, "Lyapunov exponents in resonance multiplets," *Physics Letters. A*, vol. 378, no. 1-2, pp. 34–42, 2014.

[33] S. Amina and F. K. Mohamed, "An efficient and secure chaotic cipher algorithm for image content preservation," *Communications in Nonlinear Science and Numerical Simulation*, vol. 60, pp. 12–32, 2018.

[34] J. Zhou, N.-R. Zhou, and L.-H. Gong, "Fast color image encryption scheme based on 3D orthogonal Latin squares and matching matrix," *Optics & Laser Technology*, vol. 131, p. 106437, 2020.

[35] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.

[36] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan et al., "Neural-assisted image-dependent encryption scheme for medical image cloud storage," *Neural Computing and Applications*, pp. 1–14, 2020.

[37] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Information Sciences*, vol. 222, pp. 323–342, 2013.

[38] T. S. Ali and R. Ali, "A novel medical image signcryption scheme using tent-logistic-tent system and henon chaotic map," *IEEE Access*, p. 1, 2020.

[39] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Computing and Applications*, vol. 31, no. 1, pp. 219–237, 2019.

[40] Y. Wu, J. P. Noonan, and S. Agaian, ""NPCR and UACI randomness tests for image encryption," cyber journals: multidisciplinary journals in science and technology," *Journal of Selected Areas in Telecommunications*, 2011.

[41] E. Yavuz, "A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme," *Optics & Laser Technology*, vol. 114, pp. 224–239, 2019.

[42] A. Kulsoon, D. Xiao, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," *Multimed. Tools Appl*, vol. 75, no. 1, pp. 1–23, 2016.

[43] D. Zuras, M. Cowlishaw, A. Aiken et al., "IEEE standard for floating-point arithmetic," *IEEE Standard*, vol. 754, pp. 1–70, 2008.

[44] R. Ghosh and J. K. M. S. U. Zaman, "Review on fifteen statistical tests proposed by NIST," *Journal of Theoretical Physics and Cryptography*, vol. 1, no. 1, pp. 18–21, 2012.

[45] X. Tong and M. Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically," *Image and Vision Computing*, vol. 26, no. 6, pp. 843–850, 2008.

[46] R. Sivarama, S. Rajagopalan, J. B. B. Rayappan et al., "Ring oscillator as confusion-diffusion agent: a complete TRNG drove image security," *IET Image PA Chaos-Based Image Encryption Algorithm with Simple Logical Functionsrocessing*, vol. 14, no. 13, pp. 2987–2997, 2020.

[47] E. Yavuz, R. Yazıcı, and M. C. Yamaç, "A chaos-based image encryption algorithm with simple logical functions," *Computers & Electrical Engineering*, vol. 54, pp. 471–483, 2016.

[48] S. Li, Y. Zhao, B. Qu, and J. a. Wang, "Image scrambling based on chaotic sequences and Veginère cipher," *Multimedia Tools and Applications*, vol. 66, no. 3, pp. 573–588, 2013.

[49] S. A. Banu and R. Amirtharajan, "Tri-level scrambling and enhanced diffusion for DICOM image cipher- DNA and chaotic fused approach," *Multimedia Tools and Applications*, vol. 79, pp. 28807–28824, 2020.

[50] S. Rajagopalan, S. Poori, M. Narasimhan et al., "Chua's diode and strange attractor: a three-layer hardware-software co-design for medical image confidentiality," *IET Image Processing*, vol. 14, no. 7, pp. 1354–1365, 2020.