PAPER

A plaintext-related and ciphertext feedback mechanism for medical image encryption based on a new one-dimensional chaotic system

Physica Scripta

PAPER

A plaintext-related and ciphertext feedback mechanism for medical image encryption based on a new one-dimensional chaotic system

Jianwu Xu[1], Kun Liu[1], Qingye Huang[2], Quanjun Li[2] and Linqing Huang[2]

[1] School of Automation Science and Engineering, South China University of Technology, Guangzhou 510641, People's Republic of China
[2] School of Advanced Manufacturing, Guangdong University of Technology, Guangzhou 510006, People's Republic of China

E-mail: aulkun@mail.scut.edu.cn

RECEIVED
10 June 2024

REVISED
21 October 2024

ACCEPTED FOR PUBLICATION
28 October 2024

PUBLISHED
7 November 2024

Keywords: medical image encryption, lightweight, 1D-SAM, permutation-diffusion, PRCFM

Abstract

In recent years, Plaintext-Related Image Encryption (PRIE) algorithms have been introduced, demonstrating a commendable level of plaintext sensitivity to resist chosen plaintext attack (CPA). However, these approaches suffer from several drawbacks, including inability to fully reconstruct the original image, limited practical value and excessive computational demands etc.. Moreover, the exponential expansion of medical data necessitates the formulation of more secure and efficient encryption algorithms. In this paper, firstly, a novel one-dimensional chaotic map, designated as 1D-SAM, which strikes an excellent balance between structural complexity and chaotic performance is proposed. The 1D-SAM achieve a larger chaotic range and an elevated Lyapunov exponent, signifying enhanced dynamical complexity. Subsequently, we devise a lightweight medical image encryption system leveraging the 1D-SAM and an innovative diffusion architecture, termed the plaintext-related and ciphertext feedback mechanism(PRCFM). This encryption system is a symmetric-key cryptosystem, eliminating the need for transmitting supplementary data beyond the secret keys to the recipient. Notably, the encrypted image maintains identical dimensions to its original counterpart and is fully recoverable. Complete simulation experiments were conducted on a personal computer equipped with *MATLAB R*2021*a*, *OS Windows* 11, 2.60 GHz *CPU* and 16*GB RAM*. The experimental results indicate that our encryption system, employing a single permutation-diffusion round, efficiently encrypts a 512×512 image in approximately 0.2854 seconds. Leveraging the advantages of the PRCFM, our approach demonstrates superior plaintext sensitivity, achieving an average number of pixels changing rate (NPCR) of 99.6051% and a unified average changed intensity (UACI) of 33.4452%. In summary, our work addresses key limitations of contemporary encryption frameworks, exhibiting acceptable performance in both encryption speed and security strength.

1. Introduction

Digital image stands as a pivotal medium for information dissemination. While transmitting sensitive data, particularly medical images, through public channels or entrusting their storage to third-party entities, the absence of protection might lead to privacy leakage. Encryption technology holds a pivotal position in safeguarding the security of images and has garnered significant research attention over the past few decades. For the fact that, different from textual data, digital image possess larger data capacity and higher correlation, especially for medical images like CT-Scan images. Furthermore, the remarkable proliferation of the smart healthcare industry in recent times has spurred a substantial surge in the generation and transmission of medical images. Consequently, the conventional encryption algorithms tailored for textual data i.e., Data Encryption Standard(DES), Advanced Encryption Standard(AES) and Rivest-Shamir-Adleman(RSA), are found to be insufficient in delivering satisfactory encryption outcomes [1]. Consequently, the development of cryptosystems that possess both high strength and efficiency has emerged as an increasingly pressing imperative.

Chaotic systems possess some inherent properties like high sensitivity to initial values and complex chaotic behaviour [2]. The realm of chaos-based cryptography, an extensively researched field, has been experimentally demonstrated through lasers [3, 4], circuit system [5] and neural network [6] etc.. This is intimately related to synchronisation in chaotic systems, which is used to remove chaotic backgrounds and reproduce the signal. Algorithmically speaking, in [7], Shannon introduced the modern cryptography architecture, namely permutation-diffusion structure. Within this structure, the permutation operation serves a pivotal role in disrupting the spatial redundancy of images by rearranging the positions of pixels, albeit with a limitation in altering the inherent statistical properties of pixels. Subsequently, the diffusion operation comes into play, modifying the pixel values, thereby complementing the permutation stage and enhancing the overall security of the cryptographic process. In virtually all chaos-based image encryption frameworks, chaotic systems are integral components for generating pseudo-random numbers. Notably, high-dimensional (HD) chaotic systems, characterized by their intricate dynamics and capacity to produce pseudo-random sequences with exceptional randomness properties, have garnered widespread adoption within the realm of image encryption [8–10]. For instance, in [8], a 2D chaotic system was designed and utilized for the generation of a 3D orthogonal Latin square, which is then employed in encryption processes. In [10], a novel memristive hyperchaotic model was introduced and rigorously analyzed. Leveraging this hyperchaotic model, medical images in the Internet of Medical Things are compressed and encrypted by using 3-bit permutation, 5-bit permutation and diffusion operation. Nevertheless, it is noteworthy that the execution time associated with HD systems tends to surpass that of the Low-dimensional(LD) chaotic systems. Consequently, numerous image encryption schemes opt for LD chaotic systems, such as Chebyshev Map [11] and Sine map [12] to generate pseudo-random numbers. However, these conventional LD maps fall to offer larger chaotic range and more intricate dynamical behaviors. To reconcile the trade-off between chaotic performance and computational efficiency, numerous refined LD chaotic systems have been devised [13–15]. In [13], a new 1D chaotic system based on the fraction of cosine over sine(1-DFCS) is proposed. Subsequently,, the chaotic sequences generated by 1-DFCS are employed within a new sensitive function to diffuse the original images.

In general, image encryption schemes can be categorized into two groups: non-plaintext-related image encryption(NPRIE) schemes and PRIE schemes. For NPRIE schemes [16–18], the encryption procedure and the generation of the keystream exhibit an independence from the original image. This implies that, regardless of the diversity in the original images being encrypted, the encryption process and the corresponding keystream remain unaltered. In [17], Cao *et al* introduced an innovative image cryposystem based on a new 2D chaotic map. The proposed scheme incorporates two rounds plaintext-related confusion-diffusion operations. This characteristic renders NPRIE encryption schemes vulnerable to CPAs or differential attacks(DA). Illustratively, the algorithms presented in [16, 17] have been cracked by DA in [19] and CPA in [20], respectively.

To resist various CPAs or DAs, PRIE encryption technologies have been widely studied. In PRIE schemes, the inherent information of the original image is intricately integrated into the generation of the keystream or the process of encryption. Consequently, even when two original images with subtle differences are subjected to the cryptosystem, the resulting cipher images are completely different. This feature frustrate attempts by adversaries to leverage CPA or DA for cryptanalysis. In works [15, 21, 22], enhancing plaintext sensitivity involves utilizing the value of a previously encrypted pixel to influence the subsequent pixel's encryption. Specifically, [21] introduces a method where the original image is initially permuted using the Rubik's cube method, followed by a two-dimensional diffusion process. Notably, during each dimensional diffusion step, the previously encrypted pixels from various directions contribute to encrypting the current pixel, effectively propagating subtle alterations in the original image across the entire encrypted counterpart. In 2023, Lai *et al* [22] proposed a medical image encryption scheme that incorporates a single round of permutation coupled with multi-directional substitution to guarantee high security. However, to attain satisfactory plaintext sensitivity, iterative permutation-diffusion procedures are necessary, potentially compromising the encryption speed of the system. Recognizing that permutation operations alone are insufficient in altering statistical properties, researchers have capitalized on this feature to devise PRIE encryption algorithms [23–25]. A notable instance is [24], where a Deoxyribonucleic acid(DNA) coding based image cryptosystem is introduced, leveraging the peculiarity of plaintext to enhance plaintext sensitivity. This approach exploits the base count in DNA-encoded images to generate pseudo-random sequences for permutation. However, the statistical characteristics of the original image remain insufficiently sensitive to modifications, allowing adversaries to manipulate the image without altering its statistical features, thus facilitating cryptanalytic strategies like CPAs and DAs. In [26], the traditional permutation and diffusion operations are fused into a single integrated process and executed simultaneously. Furthermore, a plaintext-related parameter, which is highly sensitive to the original image and initiates the encryption of the first pixel. The first encrypted pixel then sequentially secures the rest of the image. Although this design fosters heightened plaintext sensitivity and encryption efficiency, it poses a challenge at the receiver end, where the inability to decrypt the first pixel potentially introduces security vulnerabilities. To tackle this security concern, researchers have innovatively conceived a multitude of encryption architectures[10,

27–30]. Specifically, the encrypted image's dimensions are enlarged, followed by the insertion of plaintext-related parameters into the ciphertext. This augmented ciphertext, along with the accompanying parameters, is then transmitted to the receiver. For example, in [30], Chen *et al* harness the statistical properties of a random information source in the wavelet domain to develop a lightweight image encryption scheme. To strike an optimal balance between security and speed, solely the low-frequency components undergo encryption. Upon applying the inverse discrete wavelet transformation, the resulting ciphertext image is obtained, which is then extended to accommodate the transmission of the plaintext-related parameter vector. However, these technologies inevitably alter the size of the ciphertext image, thereby augmenting the bandwidth necessary for its transmission. To ensure robust security, researchers have devised one-time-pad-like cryptosystems, leveraging secret keys derived either directly from the original image [31, 32] or through cryptographic hash functions such as SHA-256 [33–36], SHA-512 [37], etc.. A medical image encryption algorithm [31] innovatively uses chaotic system initial values, which are derived from the original image, as keys. It segments the image into blocks, subjects them to random permutation and diffusion through bitwise XOR operations. In [35], an optimized random sequence scrambles pixel positions, followed by diffusion via the 3D-Lorenz system. Notably, the initial values of the 3D-Lorenz system are derived from the plain image using SHA-256, and serve as the secret keys. Meanwhile, [37] employs a multifaceted encryption scheme incorporating cyclic shifting, inter-bitplane XOR, and substitution-box substitution. To bolster security, SHA-512 processes the original image to yield ultra-sensitive output, which serves as the secret keys. And these 512-bit hashes facilitate the generation of S-boxes through a novel algebraic technique. A pivotal limitation of one-time-pad-like schemes stems from the incessant exchange of secret keys, consequently escalating the intricacies and expenses tied to key dissemination and administration. Moreover, the requirement for a distinct key per image encryption undermines the feasibility of these systems in video encryption or real-time encryption applications.

In this article, we introduce a novel one-dimensional chaotic map, designated as 1D-SAM, which exhibits a parsimonious structure yet harbors intricate chaotic dynamics. This map is meticulously devised to achieve an optimal equilibrium between encryption speed and security when deployed for image encryption tasks. Subsequently, based on the 1D-SAM, a new plaintext-related diffusion architecture PRCFM is proposed for medical image encryption, which addresses the majority of limitations inherent in contemporary encryption schemes.

The remainder of this paper is organized as follows: section 2 introduces the proposed new chaotic system 1D-SAM. Section 3 expounds the image encryption system. Section 4 presents the simulation and security analysis of the proposed encryption system. Section 5 presents the discussion of our work. Section 6 concludes our work.

2. Proposed chaotic map

In this section, we offer a meticulous introduction to the proposed chaotic system 1D-SAM. Its mathematical representation is given by equation (1):

$$x_{n+1} = \sin(r^2 \arcsin(x_n)) \tag{1}$$

where r is the control parameter.

2.1. Lyapunov exponent test

A dynamical system that exhibits nonlinearity, characterized by the manifestation of global boundedness within its state space and possessing a positive Lyapunov exponent, can be rigorously classified as a chaotic system. Notably, as evidenced by equation (1), the system fulfills the essential criterion of global boundedness. Subsequently, to ascertain its chaotic nature further, we proceed to compute the Lyapunov exponent (LE) of this system, alongside those of several recently introduced one-dimensional chaotic systems, utilizing equation (2). The outcomes are then plotted in figure 1 for comparative analysis. As discernible from figure 1, when contrasted with the 1−DFCS [13] and 1−DCP [14], the proposed 1D-SAM exhibits a superior Lyapunov exponent across a considerably wider range of parameter value.

$$\lambda = \lim_{k\to\infty} \frac{1}{k} \ln\left|\frac{f^k(x_0 + \Delta x) - f^k(x_0)}{\Delta x}\right| = \lim_{k\to\infty} \frac{1}{k} \sum_{i=0}^{k-1} \ln\left|\frac{\partial f(x)}{\partial x}\right|_{x=x_i} \tag{2}$$

where k corresponds to the size of the generated time series $f(x_n)$.

2.2. Bifurcation analysis

The phenomenon of period-doubling bifurcation represents an alternative pathway through which nonlinear dynamical systems traverse into a chaotic regime. Figure 2 depicts the bifurcation diagrams corresponding to

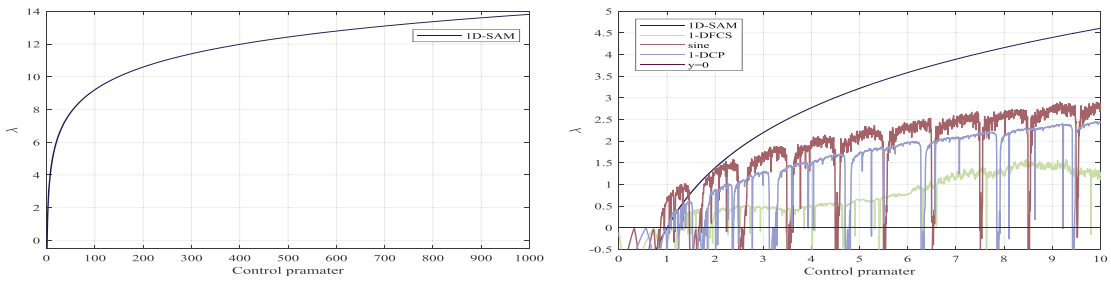
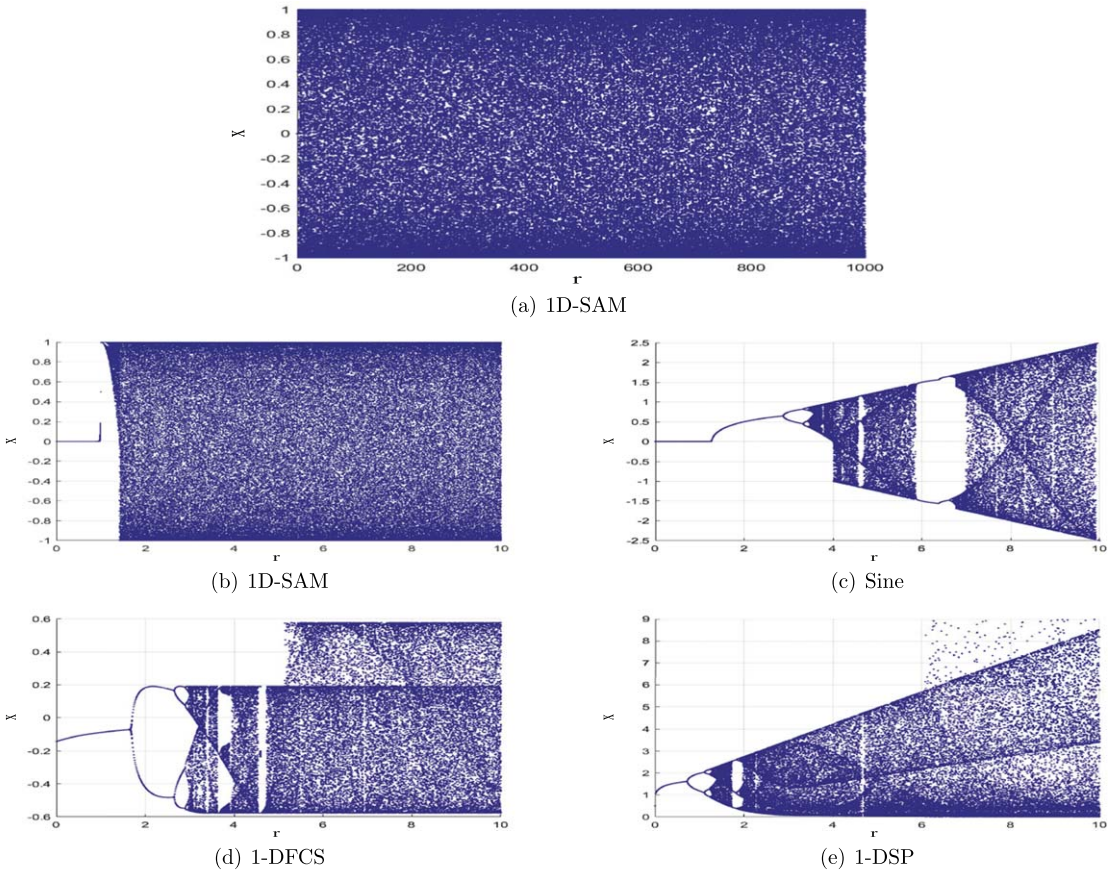


Figure 1. LE analysis result of different maps.



(a) 1D-SAM

(b) 1D-SAM (c) Sine

(d) 1-DFCS (e) 1-DSP

Figure 2. Bifurcation diagrams of different maps.

various maps. Notably, the analysis reveals that the 1D-SAM exhibits a notably broader range of chaotic behavior.

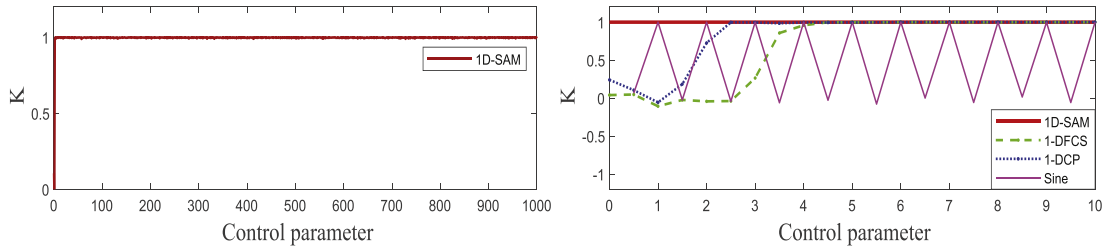
2.3. 0-1 Test

The 0-1 test can be directly applied to time-series data to discern whether a dynamical system exhibits chaotic or non-chaotic behavior. The K can be calculated as follows:

$$s(n) = \sum_{i=1}^{n} X(i)\sin(ir) \tag{3}$$

$$p(n) = \sum_{i=1}^{n} X(i)\cos(ir) \tag{4}$$

$$M(n) = \lim_{N\to\infty} \frac{1}{N}\sum_{i=1}^{n}[p(i+n) - p(i)]^2 + [s(i+n) - s(i)]^2 \tag{5}$$



(a) The 0-1 Test of 1D-SAM with $r \in (0, 1000)$

(b) The 0-1 Test of 1D-SAM, 1-DCP, 1-DFCS and Sine with $r \in (0, 10)$

Figure 3. The 0-1 Test of 1D-SAM, 1-DFCS, 1-DCP and Sine.

Table 1. NIST test results of 1D−SAM.

Test index	p-Value	Result
Frequency	0.816 537	PASS
BlockFrequency	0.534 146	PASS
CumulativeSums	0.419 021	PASS
Runs	0.401 199	PASS
LongestRun	0.971 699	PASS
Rank	0.304 126	PASS
FFT	0.299 251	PASS
NonOverlappingTemplate	0.455 937	PASS
OverlappingTemplate	0.994 250	PASS
universal	0.137 282	PASS
ApproximateEntropy	0.455 937	PASS
RandomExcursions	0.568 055	PASS
RandomExcursionsVariant	0.602 458	PASS
Serial	0.971 699	PASS
LinearComplexity	0.494 392	PASS

$$K = \frac{\log M(n)}{\log n} \tag{6}$$

where X represents a time series of size N, generated by the 1D-SAM. Specifically, with a parameter r set to 2, and when K approaches 1, the dynamical system observed to exhibit chaotic behavior. The comparative test outcomes for the 1D-SAM, alongside the 1-DFCS, 1-DCP, and Sine functions, are presented in figure 3, which demonstrates that 1D-SAM exhibits superior chaotic performance.

2.4. NIST SP 800-22 test

In the realm of image encryption, the level of randomness inherent in the keystream is undeniably a pivotal determinant of the encryption system's security. To rigorously evaluate the randomness of the outputs produced by the 1D-SAM, we employ the NIST SP 800-22, which comprises 15 subtests. Firstly, 125, 000 binary numbers are generated by the 1D-SAM and subsequently subjected to the NIST SP 800-22. Following this, the test results are obtained and presented in table 1. A meticulous analysis of these results reveals that all $P-values$ lie within the acceptable range of (0.01, 1), indicating that the binary numbers have successfully passed the NIST SP 800-22 randomness test. So, the binary sequences generated by the 1D-SAM successfully meet the rigorous randomness criteria outlined in the NIST SP 800-22 standard, rendering them suitable for the development of fast and secure encryption systems.

3. The proposed image cryptosystem

This section delves into the proposed encryption framework, as visually represented in figure 4. The introduced algorithm, a symmetric cryptosystem in essence, incorporates a single round of permutation-diffusion process, which is meticulously outlined in the subsequent paragraphs.

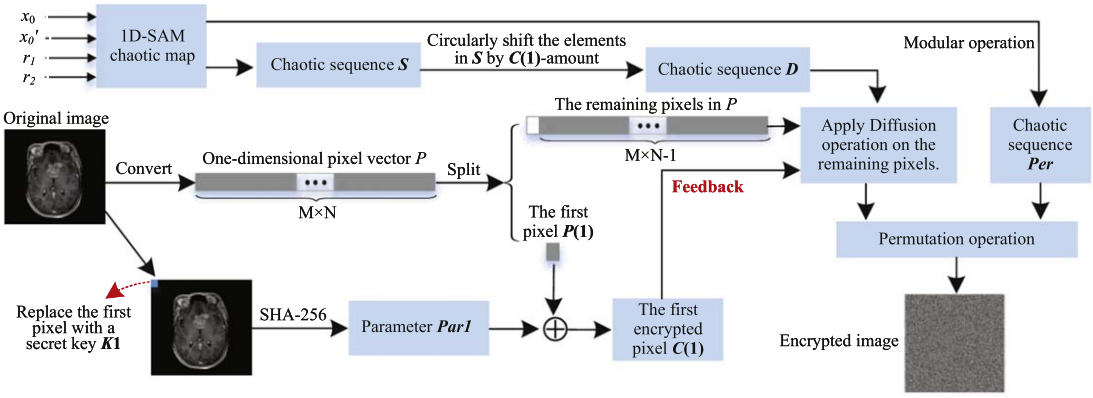


Figure 4. The proposed image cryptosystem.

3.1. Keystream generation

To encrypt a medical image P of dimensions $M \times N$, we employ the proposed 1D-SAM to generate two distinct random sequences, denoted as $X1$ and $X2$ using differing initial values $(x_0,\ x'_0)$ and unique parameter configurations (r_1, r_2), as defined in equation (7).

$$\begin{cases} X1 = \{x_1,\ x_2,\ldots,x_M\} \\ X2 = \{x'_1,\ x'_2,\ldots,x'_N\} \end{cases} \tag{7}$$

And then two keystreams, S and Per, each with a size of $M \times N$, are calculated using equation (8).

$$\begin{cases} S(k) = \mathrm{mod}(\lfloor X1(i) \times 10^{15} + X2(j) \times 10^{15} \rfloor,\ 256),\ k{+}{+} \\ Per(k) = \mathrm{mod}(\lfloor X1(i) \times 10^{15} + X2(j) \times 10^{15} \rfloor,\ M \times N) + 1,\ k{+}{+} \end{cases} \tag{8}$$

where $i = 1, 2, \cdots, M; j = 1, 2, \cdots, N; k = 1, 2, \cdots, M \times N$.

3.2. Encryption prosess

Step 1: Convert the medical image P into a one-dimensional vector $P1$ of length L, where $L = M \times N$.

Step 2: Calculate a plaintext-related parameter par. Firstly, the key ke is employed to substitute the first pixel of the original image P, thereby yielding a modified image denoted as $P2$. Then SHA-256 accepts $P2$ as input, subsequently generates a 256-bit binary hash value, denoted as H. Finally, the obtained hash value H is processed by equation (9) to yield the desired plaintext-related parameter par.

$$\begin{cases} tmp = H(1{:}\ 32) \oplus H(33{:}\ 64) \oplus \ldots \oplus H(225{:}\ 256) \\ par = mod(tmp,\ 256) \end{cases} \tag{9}$$

Step 3: Implement the proposed PRCFM on $P1$ to obtain a one-dimensional vector P_d, which is detailed in algorithm 1.

Algorithm 1. PRCFM

Require: A one-dimensional pixel vector $P1$, secret key ke, keystream S and plaintext-related parameter par.
Ensure: Diffused one-dimensional pixel vector P_d.
1: $P_d(1) = P1(1) \oplus par$
2: $pre = P_d(1)$
3: $num1 = mod(pre \times ke,\ M \times N) + 1$
4: $D = circshift(S,\ num)$
5: **for** $i = 2{:}\ M \times N$ **do**
6: $\quad P_d(i) = mod(P(i) \oplus D(i) + pre,\ 256)$
7: $\quad pre = P_d(i)$
8: **end for**

Step 4: Scramble the diffused one-dimensional pixel vector P_d using the keystream Per according to equation (10), resulting in an encrypted one-dimensional pixel vector, labeled as C.

$$P_d(i) \leftrightarrow P_d(Per(i)) \tag{10}$$

where $i = 1, 2, \cdots, M \times N$.

Step 5: The encrypted one-dimensional pixel vector C is transformed into an encrypted grayscale image of dimensions $M \times N$.

3.3. Decryption prosess

In symmetric encryption systems, Alice and Bob share an identical secret key. Initially, Bob employs the keys to generate the keystreams D and Per. Subsequently, the cipher image C is converted into a one-dimensional vector $C1$, with a length of $L = M \times N$. By executing the inverse permutation operation specified in equation (11) on $C1$, the diffused one-dimensional pixel vector P_d is obtained.

$$\begin{cases} C1(i) \leftrightarrow C1(Per(i)) \\ P_d = C1 \end{cases} \tag{11}$$

where $i = 1, 2, \cdots, M \times N$.

Finally, Bob performs the reverse process of PRCFM detailed in algorithm 2 on P_d to restore the original image P.

Algorithm 2. Reverse process of PRCFM

Require: Diffused one-dimensional pixel vector P_d, secret key ke and keystream D.
Ensure: A one-dimensional pixel vector $P1$.
1: $pre = P_d(1)$
2: $num1 = mod(pre \times ke, M \times N) + 1$
3: $D = circshift(D, num)$
4: **for** $i = 2: M \times N$ **do**
5: $P1(i) = mod(P_d(i) + 256 - pre, 256) \oplus D(i)$
6: $pre = P_d(i)$
7: **end for**
8: $P2 = P1$
9: $P2(1) = ke$
10: $H = SHA256(P2)$
11: $tmp = H(1: 32) \oplus H(33: 64) \oplus ... \oplus H(225: 256)$
12: $par = mod(tmp, 256)$
13: $P1(1) = P_d(1) \oplus par$

4. Results and analysis

In this section, a series of experiments have been conducted, with their outcomes being thoroughly analyzed and deliberated upon, aiming to rigorously assess the performance of the proposed encryption scheme. Four medical images about different body regions with a uniform size of 512×512 were selected from the Pseudo-PHI DICOM-Database(cancerimagingarchive.net). This images, designated as 'IMG1', 'IMG2', 'IMG3' and 'IMG4' respectively, served as test images. Without loss of generality, we arbitrarily set the secret key as $x_0 = 0.9$, $x'_0 = 0.65$, $r_1 = 16.49$, $r_2 = 33.56$, $ke = 150$ and $N_0 = 1280$. Subsequently, the test images and their corresponding encrypted counterparts were visually presented in figure 5.

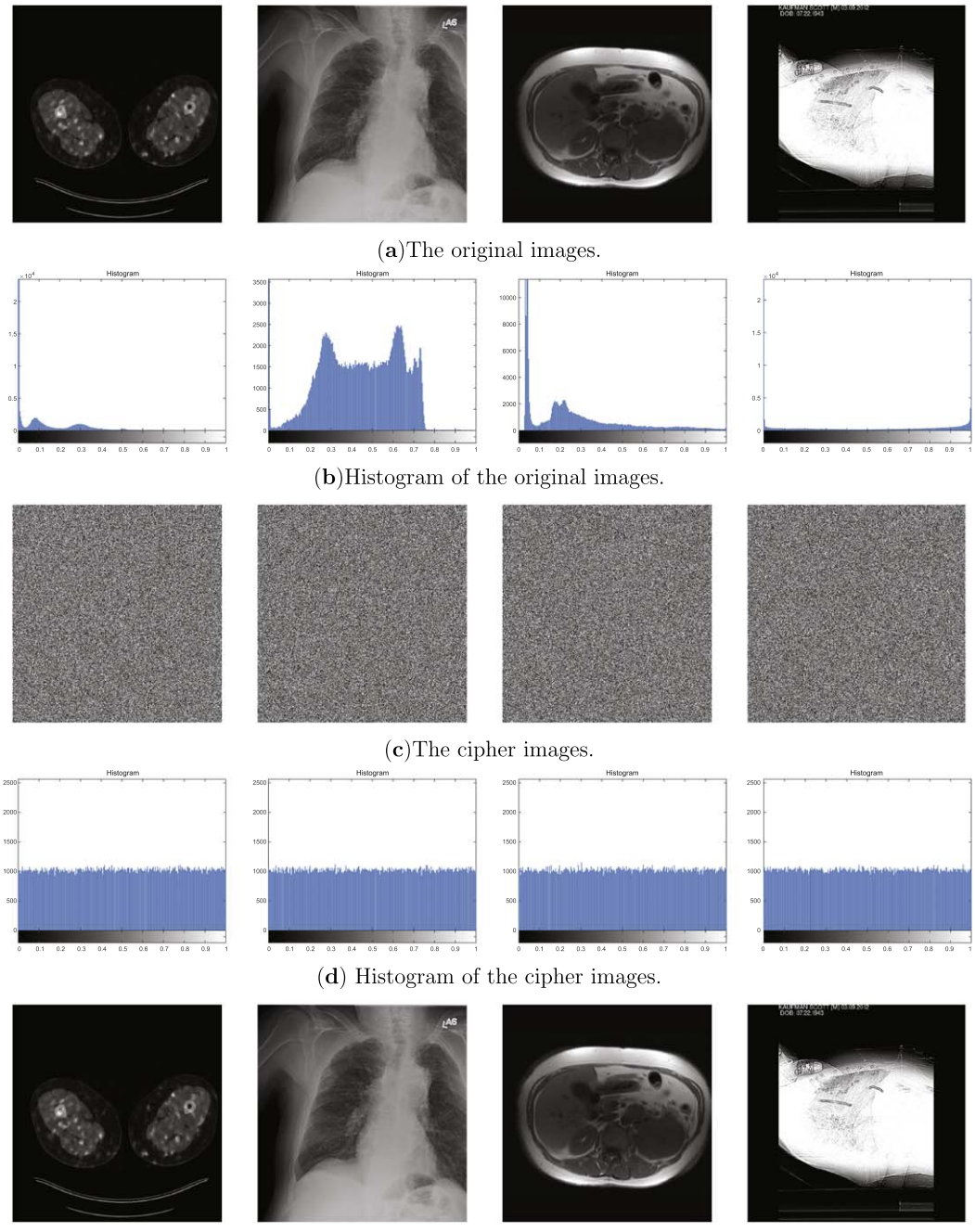
Moreover, we employ the Peak Signal-to-Noise Ratio (PSNR), which is mathematically defined in equation (12) rigorously evaluate the encryption quality.

$$PSNR = 10 \times \log \frac{255^2}{MSE}(dB) \tag{12}$$

where $MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(P(i, j) - C(i, j))^2$, M and N represent the dimensions of the image, P and C are the plaintext image and the cipher image, respectively. Table 2 presents the analysis results of PSNR values, which exhibit low magnitudes, thereby conclusively demonstrating the exceptional encryption quality.

4.1. Key space

To ensure resilience against brute-force attacks, it is imperative that the encryption system possesses a sufficiently vast key space. In light of contemporary computing capabilities, the key space of any encryption algorithm ought to exceed 2^{100}. Our proposed cryptosystem consists of six keys: $x_0 \in (0, 1)$, $x'_0 \in (0, 1)$, $r_1 > 2$, $r_2 > 2$, $ke \in [0, 255]$ and $N_0 \in [1000, 2500]$. The precision of the two initial values x_0, x'_0, as well as the two



(a)The original images.

(b)Histogram of the original images.

(c)The cipher images.

(d) Histogram of the cipher images.

(e) The decrypted images.

Figure 5. Encryption effect of our scheme.

Table 2. PSNR analysis results.

Image	IMG1	IMG2	IMG3	IMG4
PSNR	5.3314	9.0316	6.5401	5.2236

chaotic system parameters r_1, r_2 is 10^{15}. The key space of our scheme could be $(10^{15})^4 \times 1500 \times 256 > 2^{217}$, so the proposed cryptosystem can effectively resist force attack.

4.2. Histogram analysis

The histogram serves as a visual tool for elucidating the distribution pattern of pixel intensities within an image. For an encrypted image, the randomization of pixel values leads to a flattened histogram, indicative of a uniform distribution. This characteristic fortifies the encryption system against a broad spectrum of statistical attacks.

Table 3. The results of VIH analysis.

Image	Original image				Cipher image			
	IMG1	IMG2	IMG3	IMG4	IMG1	IMG2	IMG3	IMG4
VIH	8.69×10^7	9.83×10^5	1.96×10^7	8.49×10^7	1048.58	1045.74	1201.18	883.62

Table 4. The results of correlations analysis.

Image	Original image				Cipher image			
	V	H	D	A	V	H	D	A
IMG1	0.9522	0.9873	0.9463	0.9445	−0.0021	0.0006	−0.0036	−0.0018
IMG2	0.9927	0.9938	0.9898	0.9897	0.0003	0.0007	0.0015	0.0031
IMG3	0.9959	0.9980	0.9943	0.9939	0.0003	0.0009	0.0019	0.0009
IMG4	0.9757	0.9767	0.9659	0.9653	−0.0012	0.0002	0.0026	0.0013

Figure 4 showcases the comparative histograms of four test images, both in their original and encrypted forms It can be observed that all histograms corresponding to the encrypted images exhibit a uniform distribution.

Furthermore, we incorporate the Variance of Image Histogram (VIH) [26], as formalized in equation (13), as a quantitative metric to assess the degree of flatness within the image histogram

$$VIH = \frac{1}{256}\sum_{i=0}^{255}(h_i - e)^2 \tag{13}$$

where h_i represents the count of pixels that exhibit a specific gray level i and $e = \frac{M \times N}{256}$. The comparative analysis of VIH values between the original and ciphered images is presented in table 3. Notably, the VIH outcomes for the encrypted images exhibit a substantial decrement in comparison to their original counterparts, unequivocally attesting to the exceptional encryption performance and quality achieved by our proposed algorithm.

4.3. Correlation analysis

In comparison to common natural images, medical images possess a heightened degree of correlation among neighboring pixels. To ensure resilience against attacks that exploit such correlations, this strong correlation must be completely eliminated after encryption. Herein, we utilize correlation coefficients (cc) as a rigorous analytical tool to quantify the correlation between adjacent pixels across four cardinal directions within the image. The mathematical formula utilized for calculating c.c. is given as follows:

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{14}$$

$$cov(x, y) = \frac{1}{n}\sum_{i=0}^{n}(x_i - E(x))(y_i - E(y)) \tag{15}$$

$$E(x) = \frac{1}{n}\sum_{i=0}^{n} x_i \tag{16}$$

In this experimental procedure, a total of n randomly sampled pairs of adjacent pixels were extracted from the image. The ensuing test results, tabulated in table 4, convincingly demonstrate a substantial reduction in the pronounced correlation observed within the original images, following the application of the encryption algorithm. Furthermore, we plotted the pixel values of adjacent pixels on a two-dimensional plane, using one as the horizontal coordinate and the other as the vertical coordinate. The resulting graph is depicted in figure 6. Specifically, the upper row of figure 6 showcases the correlation analysis of the original image, analyzed in four distinct directions, while the lower row reveals that the correlation in the encrypted images has been significantly diminished, which approaches negligible levels.

4.4. Information entropy

Information entropy, as quantified by equation (17), serves as a metric for evaluating the degree of randomness inherent within information sources. For an image with 256 gray level, upper bound for the information entropy value is precisely 8.

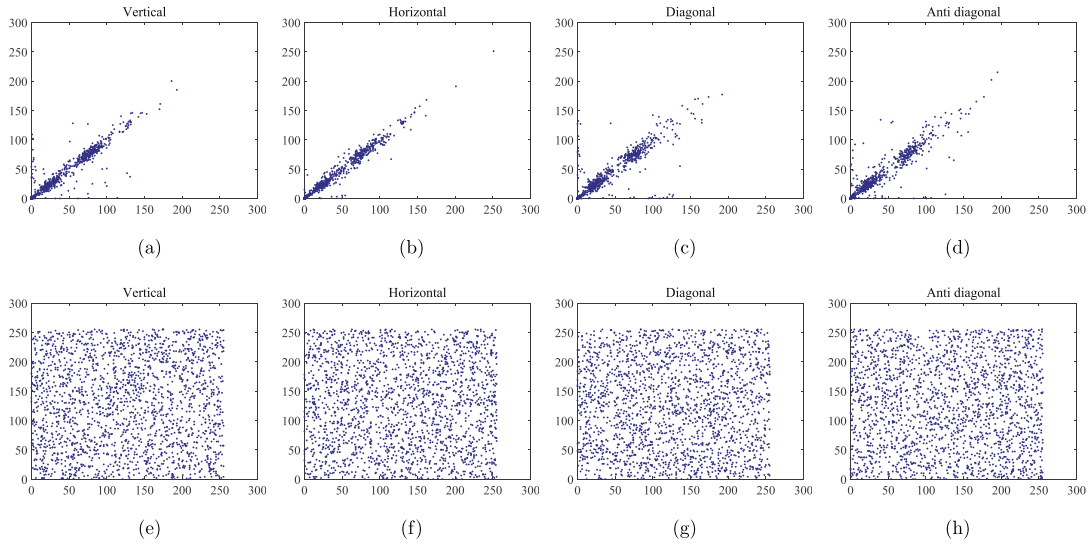


Figure 6. Correlation analysis result of 'IMG1'.

Table 5. The results of information entropy analysis.

image	original image				cipher image			
	IMG1	IMG2	IMG3	IMG4	IMG1	IMG2	IMG3	IMG4
Information entropy	3.4976	7.2993	5.8698	3.6129	7.9993	7.9994	7.9992	7.9992
Local information entropy	2.5068	5.0661	4.2708	3.3185	7.9039	7.9012	7.9002	7.9051

$$E(m) = \sum_{i=0}^{2^N-1} P(m_i)\log\frac{1}{P(m_i)} \tag{17}$$

where $P(m_i)$ is the probability of occurrence for each grayscale value m_i, 2^N is the total number of distinct grayscale values. Beyond assessing the overall information entropy of the entire image, we employ local information entropy as an additional metric to further assess the randomness of encrypted images. Specifically, we randomly extract 46×46 pixel blocks from the image and independently compute the information entropy for each of these local blocks. This approach allows us to capture the variability in randomness across different regions of the image. As evidenced in table 5, the results of both the global information entropy and the average local information entropy analysis, conducted on various test images, exhibit a remarkable proximity to the ideal value.

4.5. Sensitivity analysis

To resist the powerful CPA, an image cryptosystem must exhibit exceptional plaintext sensitivity and key sensitivity. In this section, the number of pixels changing rate (NPCR) and the unified average changed intensity (UACI) are used to rigorously evaluate the sensitivity performance of our scheme. These metrics are formally defined as follows:

$$\begin{cases} NPCR = \sum_{i=0}^{H}\sum_{j=0}^{W} D(i,j) \times 100\% \\ UACI = \dfrac{1}{W \times H}\sum_{i=0}^{H}\sum_{j=0}^{W}\dfrac{|P_1(i,j) - P_2(i,j)|}{255} \times 100\% \end{cases} \tag{18}$$

where

$$D(i,j) = \begin{cases} 0 & P_1(i,j) = P_2(i,j) \\ 1 & P_1(i,j) \neq P_2(i,j) \end{cases} \tag{19}$$

Table 6. NPCR and UACI results of key sensitivity analysis.

Image	Index	$x_0 + 10^{-15}$	$x'_0 + 10^{-15}$	$r_1 + 10^{-15}$	$r_2 + 10^{-15}$	$ke + 1$	$N_0 + 1$
IMG1	NPCR	99.6035	99.6140	99.6101	99.6025	99.6001	99.6181
	UACI	33.4627	33.4325	33.4509	33.4701	33.3979	33.3952
IMG2	NPCR	99.6103	99.5970	99.6131	99.6192	99.6095	99.6213
	UACI	33.4588	33.4197	33.4975	33.4794	33.4714	33.4926
IMG3	NPCR	99.6230	99.6123	99.6142	99.6140	99.6065	99.6110
	UACI	33.4933	33.4673	33.4655	33.4681	33.4722	33.4543
IMG4	NPCR	99.5908	99.6114	99.6260	99.6098	99.5974	99.5968
	UACI	33.4535	33.4869	33.4626	33.4808	33.4707	33.4657

4.5.1. Key sensitivity

Our encryption system incorporates six distinct $(x_0, x'_0, r_1, r_2, ke, N_0)$. To thoroughly assess the sensitivity of these keys, we conduct a rigorous analysis employing the metrics of NPCR and UACI. The detailed process is as follows:

Step 1: Randomly sample a representative set of keys from the predefined key space denoted as $key1 = (x_0, x'_0, r_1, r_2, ke, N_0)$

Step 2: Through marginal modifications applied to a single key, six distinct key sets were derived, each uniquely identified as $key2 = (x_0 + 10^{-15}, x'_0, r_1, r_2, ke, N_0)$, $key3 = (x_0, x'_0 + 10^{-15}, r_1, r_2, ke, N_0)$, $key4 = (x_0, x'_0, r_1 + 10^{-15}, r_2, ke, N_0)$, $key5 = (x_0, x'_0, r_1, r_2 + 10^{-15}, ke, N_0)$, $key6 = (x_0, x'_0, r_1, r_2, ke + 1, N_0)$ and $key7 = (x_0, x'_0, r_1, r_2, ke, N_0 + 1)$.

Step 3: We employ the seven distinct key sets to encrypt the test image to generate the corresponding ciphertext images.

Step 4: Utilizing equation (18), we obtain the values of NPCR and UACI for various key configurations.

Step 5: By executing steps 1 through 4 in an iterative fashion 200 times, the resulting average values of NPCR and UACI are subsequently presented in table 6.

One can see that the test results are all close to the ideal value. Furthermore, test image 'IMG1' is used to measure the key sensitivity in encryption and decryption process, and the simulation results are shown in figure 7. Figures 7(a) through (g) depict the encrypted images, labeled sequentially as $En1$ to $En7$, respectively, utilizing distinct encryption keys ranging from $key1$ to $key7$. Subsequently, figures 7(h) to (n) present the corresponding histograms for each of these encrypted images. Figures 7(o) through (t) gvisually represent the pixel-wise difference maps, specifically $|En2 - En1|$, $|En3 - En1|$, $|En4 - En1|$, $|En5 - En1|$, $|En6 - En1|$ and $|En7 - En1|$ respectively. Furthermore, figures 7(u) to (z) present the corresponding histograms for these difference maps, offering a quantitative assessment of the distribution of pixel differences across the images. Ultimately, we proceed to decrypt the cipher image $E1$ utilizing each of the seven encryption keys, ranging from $key1$ to $key7$, resulting in six decrypted images, which are presented in figures 7(aa) to (ag). Notably, it is evident from the outcomes that only the application of the correct key, among the seven, is capable of accurately reconstructing the original image.

4.5.2. Plaintext sensitivity

The proposed PRCFM leverages the inherent sensitivity of hash algorithms to input variations, ensuring that even the slightest modification in the original image triggers a substantial alteration in the hash output. In our scheme, the hash output serves as the cornerstone for encrypting the initial pixel, with the resulting encrypted value subsequently utilized to derive the keystream D. Consequently, any alteration to either the first pixel or the keystream D triggers a profound transformation in the overall encryption outcome. The detailed procedure for conducting plaintext sensitivity analysis using NPCR and UACI is as follows:

Step 1: A subset of keys was randomly sampled from the defined key space, which is denoted as $key1 = (x_0, x'_0, r_1, r_2, ke, N_0)$

Step 2: Utilizing equation (20), a subtle adjustment was applied to a pixel within the original image P, yielding a modified version denoted as P'.

$$Pixel(x, y) = \mathrm{mod}(Pixel(x, y) + 1, 256) \tag{20}$$

Step 3: Both the original image P and its modified counterpart P' were encrypted utilizing identical key sets $key1$ to produce their respective ciphertext images.

Step 4: Utilizing equation (18), the numerical values of the NPCR and UACI metrics were derived for analysis.

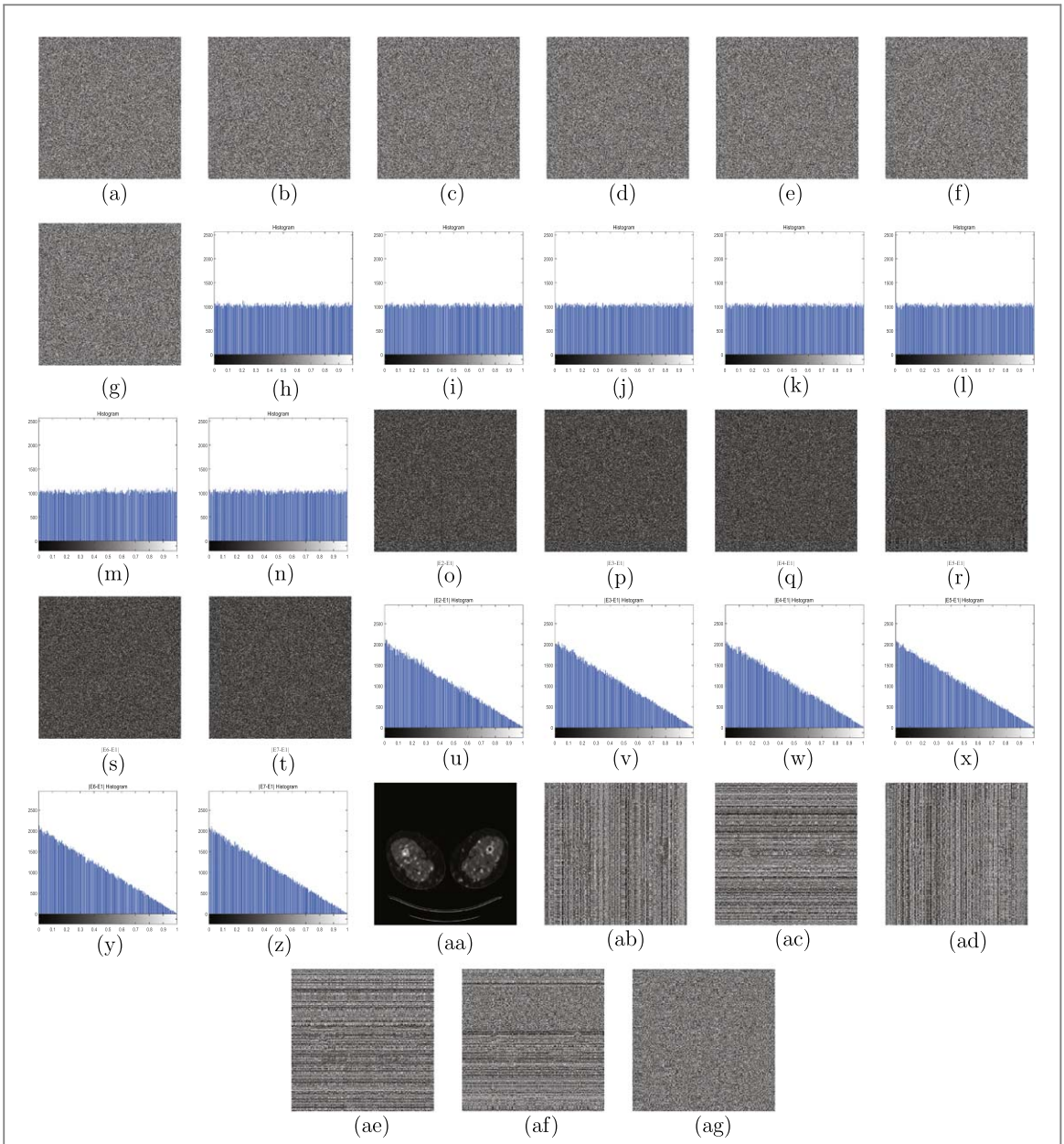


Figure 7. Key sensitivity in encryption process and decryption process.

Table 7. NPCR and UACI results of plaintext sensitivity analysis.

Image	IMG1	IMG2	IMG3	IMG4	Average
NPCR(99.6094)	99.6075	99.5996	99.6052	99.6081	99.6051
UACI(33.4635)	33.4313	33.4760	33.4214	33.4523	33.4452

Step 5: We executed steps 1 through 4 in an iterative fashion, repeating the process a total of 200 times. Subsequently, we computed the average values of NPCR and UACI. As table 7 shown, the outcomes confirm that the PRCFM architecture exhibits a remarkable capability to ensure high plaintext sensitivity.

4.6. Encrypted time analysis

In scenarios involving resource-constrained platforms or requiring real-time encryption, the adoption of a cryptosystem featuring low time complexity becomes paramount. Our proposed encryption scheme addresses this need by incorporating a streamlined encryption process that encompasses a solitary round of permutation-diffusion operation. The consumption time for encrypting the test image 'IMG1' with the size of 512×512 in

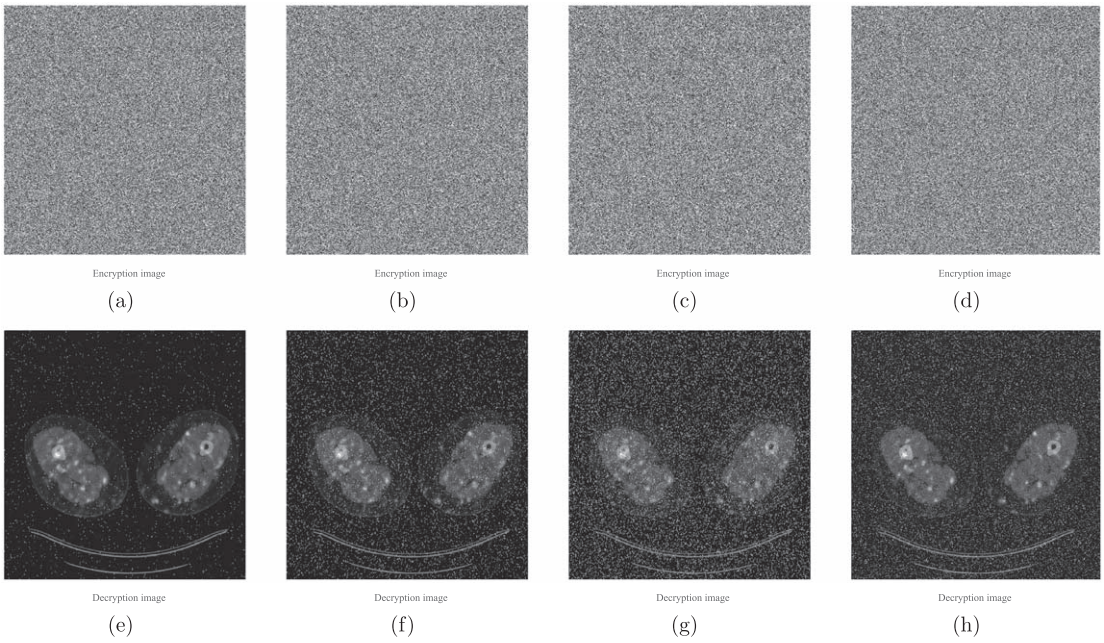


Figure 8. Robustness against noise: (a), (b) and (c) are the encrypted images contaminated by salt and pepper noise with 1%, 5% and 10% density respectively; (d) The encrypted images contaminated by speckle noise with 0.1% density. (e)-(h) are corresponding decrypted images.

MATLAB programming environment is 0.2854s. Obviously, our scheme has a significant advantage in terms of speed.

4.7. Robustness against noise attack and occlusion attack

When transmitting encrypted data over a public channel, it becomes vulnerable to diverse forms of noise interference or deliberate tampering, posing significant challenges to the integrity of the transmitted information. As a result, the design of image cryptosystems necessitates the incorporation of robust mechanisms that can withstand noise attacks and occlusion attacks. In figure 8, the initial row shows the encrypted image 'IMG1' , subjected to a diverse array of noise patterns with varying intensities. The subsequent row depicts the corresponding decrypted images. Subsequently, figure 9 presents a scenario where portions of varying sizes are excised from the encrypted 'IMG1' image, and the resultant decrypted images are graphically represented in the second row. To quantitatively assess the quality of these decrypted images, we employ the PSNR metric, with the results tabulated in table 8. Notably, our proposed scheme demonstrates robust resilience against both noise attacks and occlusion attacks, as evidenced by the results presented.

5. Discussion

In this section, we delve into the advantages and limitations of our work, followed by a discussion of potential future work. To substantiate the superior encryption performance of our proposed algorithm, we conduct a comparative analysis, juxtaposing our proposed scheme against an array of comparable PRIE methodologies. We employ the medical image designated as 'IMG1' as the benchmark test image, ensuring a level playing field by executing all encryption techniques within an identical platform environment. The comparison analysis results are meticulously presented in table 9, offering a quantitative assessment of the performance differentials. Overall, one-time-pad-like cryptosystems [31–34, 36], though capable of achieving commendable encryption outcomes, exhibit significant limitations in terms of practical applicability owing to the exorbitant costs associated with key distribution and management. These systems falter when applied to video encryption or real-time encryption scenarios, underscoring their constrained utility. In the case of other PRIE schemes, the size of the encrypted image typically needs to be expanded, resulting in an escalation in bandwidth requirements for image transmission and encryption time [27–29]. Notably, the approach presented in [30] demonstrates a high plaintext sensitivity and good encryption effects; however, this heightened sensitivity also extends to the ciphertext, making it susceptible to noise and occlusion attacks. Generally, our work demonstrates acceptable performance in terms of encryption speed and security strength. Nevertheless, upon closer examination of individual tests, particularly those assessing encryption speed and resilience against noise and occlusion attacks,

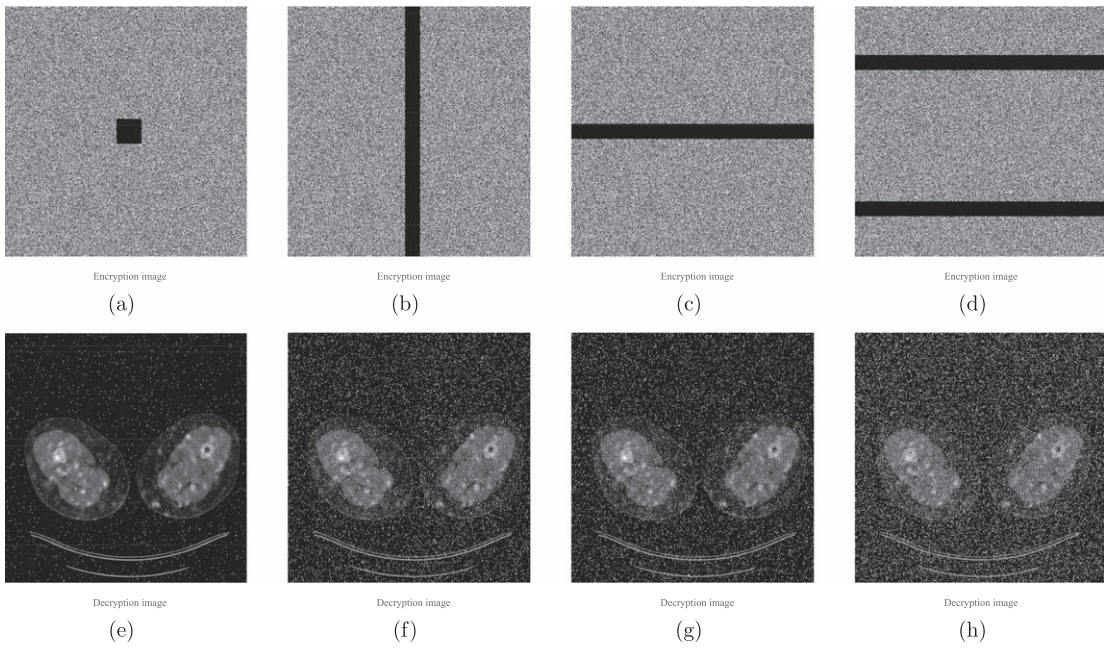


Figure 9. Robustness against cropping attack: (a)–(d) are the encrypted images clipped to different degrees; (e)–(h) are the corresponding decrypted images.

Table 8. Robustness against noise and occlusion attack analysis using PSNR.

Index	Figure 8(e)	Figure 8(f)	Figure 8(g)	Figure 8(h)	Figure 9(e)	Figure 9(f)	Figure 9(g)	Figure 9(h)
PSNR	27.2303	20.2620	17.3397	18.4414	27.1174	19.3889	19.4513	16.5624

our scheme's performance necessitates further refinement. Looking ahead, we envision optimizing the plaintext-related diffusion framework, PRCFM, and exploring the feasibility of integrating parallel computing paradigms into our encryption systems. These endeavors aim to augment encryption speed, thereby addressing identified limitations and advancing the overall performance of our approach.

6. Conclusion

In this paper, we propose a novel one-dimensional chaotic map, designated as 1D-SAM, which boasts a simple structure while demonstrating commendable chaotic properties, validated through rigorous testing. Subsequently, we introduce a groundbreaking plaintext-related diffusion architecture, PRCFM, designed to achieve high plaintext sensitivity, thereby bolstering resilience against various powerful CPAs.

In contrast to existing plaintext-related image encryption frameworks, PRCFM offers two distinct advantages. Firstly, it maintains a high degree of plaintext sensitivity while concurrently demonstrating resilience against noise interference and occlusion attacks. Secondly, PRCFM refrains from utilizing the hash value of the original image as the secret keys, thereby circumventing the limitations of a one-time-pad-like cryptosystem. Furthermore, the unique architecture of PRCFM ensures that the recipient can accurately reconstruct the original image, with the ciphertext image preserving identical dimensions to the original. Building upon the strengths of 1D-SAM and PRCFM, we present a lightweight medical image encryption scheme that incorporates solely a single round of permutation-diffusion operation, optimizing for both security and computational efficiency.

The outcomes of our simulations and comprehensive security analysis underscore the exceptional performance of this scheme, demonstrating its prowess in both security and encryption speed. These findings suggest the promising applicability of our proposed method for safeguarding sensitive medical images, addressing the pressing need for secure data transmission and storage in the healthcare sector.

Table 9. Comparison analysis result of correlation schemes.

Algorithm	Correlation coefficients			Information entropy	time(s)	NPCR	UACI	Key space	Comments
	H	V	D						
Proposed	0.0021	−0.0006	0.0036	7.9993	0.2854	99.6075	33.4313	2^{217}	Exceptional performance in security and encryption efficiency
[27]	−0.0006	0.0038	−0.0018	7.9994	0.9256	99.6099	33.4511	2^{170}	Expanded encrypted image size
[28]	0.0024	0.0071	0.0043	7.9991	3.3449	99.6170	33.4828	2^{305}	Expanded encrypted image size and long execution time
[29]	0.0010	−0.0062	0.0068	7.9993	0.5043	100	33.4653	2^{227}	Expanded encrypted image size
[30]	−0.0006	0.0036	−0.0016	7.9978	0.1158	99.6171	33.5426	2^{126}	Low robustness against noise attack and occlusion attack
[31]	0.0105	0.0105	0.0087	7.9992	3.048	99.6210	33.4379	2^{115}	One-time-pad-like cryptosystem and long execution time
[32]	0.0017	0.0018	0.0039	7.9991	0.4990	99.6104	33.4749	2^{325}	One-time-pad-like cryptosystem
[33]	−0.0015	0.0018	0.0054	7.9992	0.7386	99.6209	33.4107	2^{327}	One-time-pad-like cryptosystem
[34]	−0.0006	-0.0066	−0.0017	7.9993	0.4011	99.6338	33.4303	2^{227}	One-time-pad-like cryptosystem
[36]	0.0002	−0.0017	0.0020	7.9984	0.6011	99.6002	33.4454	2^{348}	One-time-pad-like cryptosystem

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Ethical approval

Not applicable.

Competing interests

The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, nor in the decision to publish the results.

Author's contributions

Methodology, Jianwu Xu and Quanjun Li; software, Jianwu Xu and Qingye Huang; validation, Kun Liu and Linqing Huang; investigation, Kun Liu; writing original draft preparation, Jianwu Xu; writing review and editing, Kun Liu and Quanjun Li; funding acquisition Linqing Huang. All authors have read and agreed to the published version of the manuscript.

Funding

This work was supported by the Guangdong University of Technology Educational Reform Project under Grant 211 230 022.

ORCID iDs

Jianwu Xu https://orcid.org/0009-0006-6333-0906
Linqing Huang https://orcid.org/0000-0001-9636-499X

References

[1] Wang R, Deng G Q and Duan X F 2021 *Journal of Information Security and Applications* **58** 102699
[2] Wang L N, Cao Y H, Jahanshahi H, Wang Z S and Jun M 2023 *Optik* **275** 170590
[3] Ashwin P, Terry J R, Thornburg K S and Roy R 1998 *Phys. Rev.* E **58** 7186–9
[4] Li J C, Xiao J L, Yang Y D, Chen Y L and Huang Y Z 2023 *Nanophotonics* **12** 4109–16
[5] Chen M, Xue W, Luo X, Zhang Y and Wu H 2023 *Chaos, Solitons Fractals* **174** 113780
[6] Xiao L, Liu P, He Y, Jia L and Tao J 2022 *Neurocomputing* **491** 197–205
[7] Shannon C E 1949 *The Bell System Technical Journal* **28** 656–715
[8] Hua Z y, Chen Y Y and Zhu Z H 2021 *Nonlinear Dyn.* **104** 4505–22
[9] Zhang Z y, Mou J and Zhou N R 2024 *Nonlinear Dyn.* **112** 5727–47
[10] Lai Q and Hu G 2024 *IEEE Trans. Ind. Inf.* **20** 11262–72
[11] Huang L, Cai S, Xiao M and Xiong X 2018 *Entropy* **20** 535
[12] Shamsa K, Saba I, Fahima H, Omar C, Zainab N, Ayesha W and Majid K 2022 *Security and Communication Networks* **2022** 1
[13] Midoun M A, Wang X and Talhaoui M Z 2021 *Opt. Lasers Eng.* **139** 106485
[14] Talhaoui M Z and Wang X 2021 y and Midoun M A *Vis. Comput.* **37** 541–51
[15] Le Z, Li Q j, Chen H, Cai S, Xiong X M and Xiong L Q 2024 *Phys. Scr.* **99** 055249
[16] Zhang J and Huo D 2019 *Multimed Tools Appl* **78** 15605–21
[17] Cao W J, Mao Y J and Zhou Y C 2020 *Signal Process.* **171** 107457
[18] Kumar K, Roy S and Rawat S M 2022 *Chaos, Solitons Fractals* **158** 111994
[19] Wen H P and Lin Y T 2024 *Expert Syst. Appl.* **237** 121514
[20] Shi G W, Yu S M and Wang Q X 2022 *Entropy* **24** 1023
[21] Zhu H G, Dai L W, Liu Y T and Wu L J 2021 *Math. Comput. Simul* **185** 754–70
[22] Lai Q, Hu G w, Erkan U and Toktas A 2023 *Appl. Math. Comput.* **442** 127738
[23] Cai S, Huang L, Chen X and Xiong X 2018 *Entropy* **20** 282
[24] Kang Y, Huang L, He Y, Xiong X, Cai S and Zhang H 2020 *Symmetry* **12** 1393
[25] Li Z, Peng C G, Tan W J and Li L R 2020 *Symmetry* **12** 1497
[26] Huang L, Cai S, Xiong X and Xiao M 2019 *Opt. Lasers Eng.* **115** 7–20
[27] Huang L, Li W, Xiong X, Yu R, Wang Q and Cai S 2022 *Opt. Commun.* **517** 128365
[28] Huang S, Jiang D, Wang Q, Guo M, Huang L, Li W and Cai S 2022 *Chaos, Solitons Fractals* **163** 112584
[29] Huang S, Jiang D, Wang Q, Guo M, Huang L, Li W and Cai S 2023 *Mathematics* **11** 4411

[30] Chen B, Huang L, Cai S, Xiong X and Zhang H 2024 *Chin. Phys.* B **33** 030501
[31] Kamal S T, Hosny K M, Elgindy T M, Darwish M M and Fouda M M 2021 *IEEE* **9** 37855–65
[32] Wang X Y, Su Y N, Liu L, Zhang H and Di S H 2023 *Vis. Comput.* **39** 43–58
[33] Patro K and Acharya B 2021 *Nonlinear Dyn.* **104** 2759–805
[34] Wang Q Y, Zhang X Q and Zhao X H 2023 *Phys. Scr.* **98** 025211
[35] Singh K, Singh O, Singh A K and Agrawal A K 2022 *ACM Transactions on Multimedia Computing Communications and Applications* **19** 1–19
[36] Iqbal N, Khan M A and Lee S W 2024 *Multimed Tools Appl* **83** 8629–61
[37] Xie H W, Gao Y J and Zhang H 2024 *AIMS Mathematics* **9** 6207–37