Mathematics

AIMS Mathematics, 11(3): 6744–6776.
DOI: 10.3934/math.2026279
Received: 03 January 2026
Revised: 09 February 2026
Accepted: 09 March 2026
Published: 16 March 2026

https://www.aimspress.com/journal/Math

Research article

Secure medical image encryption for healthcare applications: A fractional 4D chaotic system and symmetry-matrix-based approach

Abed Saif Ahmed Alghawli[1,*] and Mohamed M. Darwish[2,3]

[1] Computer Science Department, Prince Sattam Bin Abdulaziz University, Aflaj, Kingdom of Saudi Arabia
[2] Department of Computer Science, University College of Al Wajh, University of Tabuk, Tabuk, Saudi Arabia
[3] Department of Computer Science, Faculty of Computers and Information, Assiut University, Assiut 71516

* **Correspondence:** Email: a.alghauly@psau.edu.sa.

Abstract: Safeguarding medical images against unauthorized access and alteration during storage and transmission is a critical challenge in modern telemedicine systems. This paper introduces a robust method to encrypt medical images in which the confusion stage is driven by a four-dimensional (4D) fractional-order chaotic system, and the diffusion process utilizes a symmetric matrix integrated with a one-dimensional (1D) chaotic map. The fractional 4D chaotic system reveals intricate dynamic behavior and is extremely sensitive to initial conditions, which enhances the confusion capability by thoroughly scrambling pixel positions. The symmetry matrix is combined with a generated chaotic sequence from a 1D chaotic map during the diffusion process that ensures strong pixel intensity diffusion and key dependence. Numerous experiments carried out on a variety of medical images confirm the outstanding performance of the suggested method. The suggested method features a key space exceeding 2^{100}, exhibiting significant robustness to brute-force attacks. It achieves unified average changing intensity (UACI) values above 33% and number of pixels change rate (NPCR) values exceeding 99.6%, confirms robustness to differential attacks, and successfully resists chosen-plaintext and known-plaintext attacks. Additionally, the low pixel correlation and uniform histograms, along with average values of information entropy of 7.9973 and 7.9993 for 256×256 and 512×512 images, respectively, demonstrate strong resilience to statistical attacks. Furthermore, robust evaluations against cropping and noise attacks demonstrate the scheme's practical security, highlighting its suitability for the safe storage and transmission of medical images in healthcare

applications. Compared with related methods, the suggested method offers superior security performance.

Keywords: medical image encryption; confusion process; diffusion process; symmetry matrix; fractional order 4D chaotic system
Mathematics Subject Classification: 94A08

1. Introduction

As medical technologies steadily progress, the use of advanced medical devices becomes more common, and greater attention is given to visualizing medical information. These areas are emerging as key directions for future development in the medical field. Digital images, valued for their clarity and ease of interpretation, have become essential in medical imaging, where they aid healthcare professionals in diagnostics, monitoring diverse diseases, and treatment planning [1]. Medical images including computed tomography (CT), magnetic resonance imaging (MRI), X-rays, and ultrasound provide critical information for assessing patients' medical history and current health status. Because they are stored and shared digitally, they are vulnerable to unauthorized access, manipulation, tampering, data loss, malicious attacks, and other security threats, which can compromise patient privacy and the reliability of healthcare services, especially when transmitted through insecure channels. Thus, encrypting medical images is crucial to protect patients' sensitive data. With the rising risk of data breaches and the increasing emphasis on maintaining patient privacy in today's digital healthcare environment, robust image encryption techniques are more important than ever. Therefore, developing effective medical image encryption techniques has emerged as major research [2–5]. Image encryption converts a digital image into an unintelligible format, safeguarding it from unauthorized access. This is achieved through complex algorithms that securely encode the visual content, which can only be correctly decoded by authorized users [6–8]. Medical images, as digital representations, are attributed by strong pixel correlation, massive data volumes, and considerable redundancy, which require encryption methods suitable for these features. Traditional cryptographic algorithms (e.g., advanced encryption standard (AES), Rivest-Shamir-Adelman (RSA)) are not always well-suited for medical images because of their characteristics. To address these limitations, specialized encryption techniques have been designed for safeguarding the integrity and confidentiality of medical images, with growing emphasis on methods designed specifically for the unique features of medical imagery. Consequently, chaotic-systems-based encryption algorithms have garnered considerable attention owing to their high initial conditions sensitivity, inherent unpredictability, and intricate nonlinear dynamics [9–12]. These characteristics make them serve as powerful tools for protecting medical images through encryption [13–16]. Despite their widespread use, conventional chaotic systems in image encryption often encounter challenges, including vulnerability to modern cryptanalytic attacks, short periodicity, and limited key space [17–18]. Although these methods demonstrate resilience against many security threats, their effectiveness is sometimes constrained by weak chaotic properties in certain generators, as indicated by low positive Lyapunov exponents. To tackle these limitations, researchers have increasingly adopted fractional chaotic systems and maps, which incorporate memory effects through fractional derivatives.

Fractional-order chaotic systems extend conventional chaotic systems by revealing substantially

more intricate dynamical characteristics, that significantly enhance system complexity and initial conditions sensitivity. This increased complexity originates from the use of fractional-order derivatives, which embed hereditary and memory effects into the dynamics of a system. In contrast to integer-order systems, variations of the fractional order directly influence model behavior, resulting in a heightened sensitivity to initial conditions, broader diversity of chaotic attractors, and parameters, and the possible emergence of coexisting or hidden attractors. The inclusion of fractional orders as part of the secret key improves the unpredictability and randomness of the constructed chaotic sequences and enlarges the key space. These properties lead to longer and more complex key streams and provide stronger resistance to differential, statistical, and brute-force attacks. Therefore, fractional-order chaotic systems offer superior resistance and unpredictability in image encryption compared with conventional integer-order chaotic systems, making them particularly suitable for cryptographic applications [19–23]. However, some advanced algorithms achieve strong security but are computationally expensive, limiting their suitability for real-time medical applications. The high cost of encrypting large, high-resolution medical images can significantly slow processing, delay patient care, and limit their use in time-sensitive scenarios such as telemedicine and emergency healthcare. Despite its advantages, chaotic image encryption faces persistent challenges, particularly in balancing security and efficiency, because higher security typically demands greater computational resources. Thus, there is a need for an innovative image encryption approach that addresses these issues while ensuring that the images remain secure, usable, and quickly accessible for healthcare professionals. Motivated by these considerations, this study introduces an approach for encrypting medical images that uses a 4D fractional-order chaotic system exhibiting symmetric attractors, variability and flexibility of the attractor, and a range of complex dynamical behaviors with significantly enhanced randomness and coverage for the confusion stage and integrates chaotic maps with a symmetry-matrix-based diffusion process, exploiting the matrix's structural properties to efficiently propagate changes across the image. This hybrid design enhances unpredictability and key sensitivity while enabling longer and more complex keystreams and strong diffusion capability, resulting in improved resilience against differential, statistical, and brute-force attacks compared with conventional fractional-order approaches and providing an effective and secure approach tailored for safeguarding sensitive medical images. This paper highlights the following key contributions:

- We employ a fractional-order 4D chaotic system, which has not been previously applied to image encryption, for confusion with enhanced ergodicity and sensitivity to initial conditions. The fractional derivative introduces memory effects and expands the chaotic parameter space, generating highly unpredictable keystreams for effective pixel permutation in medical image encryption.
- A symmetric matrix integrated with a 1D chaotic map is utilized to modify pixels in the diffusion process. Any minor alter to a single pixel in the plain image produces substantial alterations in the ciphered image, thereby enhancing robustness against differential attacks.
- Security assessments and numerous experiments are conducted to verify the efficacy of the suggested approach, and it successfully passes all evaluations and confirming its superiority over several widely used encryption approaches, as well as its robustness and practical applicability.

The structure of this paper is arranged as follows. A review of related works is presented in Section 2. The background and analytical foundation of the fractional-order chaotic system and the 1D chaotic map are presented in Section 3. The proposed algorithm is explained in detail in Section 4. The experimental results and analysis of the security of the proposed algorithm across a range of parameters,

including comparisons with existing algorithms, are discussed in Section 5. Conclusions are presented in Section 6.

2. Related works

Fractional calculus allows integration and differentiation to noninteger orders and has recently attracted remarkable attention because it enables the development of models that can achieve higher accuracy than conventional integer-order calculus [24]. This approach has been applied in various domains, including modeling infectious diseases [25], medical image watermarking [26], and medical image encryption [27–31]. Accordingly, fractional-order chaotic systems represent an outstanding advancement in modern healthcare, where securing medical images has become an essential priority, driving the advancement of various efficient and secure encryption algorithms in recent years. Several notable research works have explored different approaches. Dua et al. [27] developed a chaotic map known as the improved cosine fractional chaotic map (ICFCM), combining it with two existing chaotic maps, the Chebyshev and tangent over cosine cosine (TOCC), alongside DNA operations to develop an encryption algorithm aimed at securing medical images. In [28], Boyraz et al. used two separate one-dimensional discrete-time chaotic systems for encrypting individual dorsal vein images. Wang et al. [29] developed an innovative approach to encrypt medical images that combines chaotic maps with convolutional neural networks (CNNs). Lin et al. [30] presented a memristor-based neural network (MRNN) comprising one nonideal flux-controlled memristor and four neurons, presenting a novel encryption approach to safeguard medical images. Zhang et al. [31] introduced a method to boost encryption efficiency through the selective or partial encryption of medical images, utilizing specific modifications to the variable dimension with a Logistic map. Liu J. Z. et al. [32] presented an approach for safeguarding medical images by utilizing a hyperbolic sine function integrated with a simple chaotic system. In [33], Kamal et al. proposed an algorithm applicable to encrypt grayscale and color medical images, featuring a unique image-splitting approach that processes blocks of image. Chai X. L. et al. [34] integrated a chaotic system with a Latin square to design a technique for encrypting medical images. A. Abbasi et al. [35] recently developed a method involving generalized triangle group parametrization and substitution box construction aimed at strengthening medical image encryption.

By combining Otsu threshold segmentation with coupled chaotic systems, Zhang Y. Z. et al. [36] developed a multilevel approach for securing stereoscopic medical images. Dua and Bhogal [37] introduced an algorithm to encrypt and safeguard medical images that utilizes a new 1D sine-tangent chaotic (STC) map. In [38], Subhrajyoti et al. introduced a logistic tent map-based encryption method, achieving effectiveness and efficiency in encrypting and decrypting medical images. Q. Lai et al. [39] introduced an advanced approach to encrypt medical images by utilizing the 2D logistic-Gaussian hyperchaotic map. Bi et al. [40] designed an encryption method for medical image incorporating an adaptive function, significantly strengthening the system's complexity and security against potential attacks. Using the fractional-order Sprott K chaotic system, Gokyildirim et al. [41] recently developed a method for encrypting biometric iris images. Hua et al. [42] proposed scheme for encrypting medical images combining adaptive pixel diffusion, high-speed scrambling, and random data insertion. Chen et al. [43] designed an optical encryption method by integrating double random phase encoding with Shearlets to improve the medical images' security. In [44], Jackson J. and Perumal R. presented a 1D inverse cosine chaotic-map-based approach for encrypting medical images, combining zigzag permutation, block scrambling, and adaptive diffusion to enhance the system's security.

Zhang et al. [45] investigated methods to encrypt medical images by using dynamic cross-diffusion and Josephus scrambling techniques for protecting patient privacy. In [46], A. Belazi and A. Mabrouk proposed a chaos-driven medical image encryption method using one round of diffusion–confusion with pixel substitution, bitwise exclusive OR (XOR), and pixel permutation. Wang et al. [47] proposed an approach to encrypt medical images that employs a one-dimensional piecewise linear chaotic map to manipulate the most significant bit. map, where prediction errors are corrected through preprocessing before applying diffusion with chaotic keys to construct the encrypted images. Aashiq et al. [48] presented a hybrid encryption algorithm that employs frequency domain encryption alongside chaotic attractors by employing integer wavelet transform and spatial domain encryption via DNA sequences. Lai and Hua [49] presented an encryption method using random DNA coding, a 3D hyperchaotic map, and integer wavelet transformation. Liu et al. [50] developed an approach for encrypting medical images by utilizing a new fourth-order chaotic system.

3. Preliminaries

3.1. Fractional-order chaotic system

The fractional-order chaotic system is defined by [51]:

$$\begin{aligned} D^q x(t) &= -x + xz + ayz, \\ D^q \mathrm{y(t)} &= by - xz - 3w, \\ D^q z(t) &= -cz + xy + dz^2, \\ D^q w(t) &= ey, \end{aligned} \tag{1}$$

where D^q stands for the Caputo fractional derivative $(0 < q \leq 1)$. The variables x, y, z and $w \in \mathbb{R}$ denote the system states, and the parameters are set to $a = 2.3$, $b = 2$, $c = 6$, $d = -0.25$, and $e = 3$. Under these conditions, a symmetric attractor is generated by the system. With a fractional order of $q = 0.98$, Figure 1 illustrates the trajectory obtained using the initial state $[1,0,0,1]$. For simplicity and clarity, the behavior of dynamic analysis of System (1), summarized from the original reference [51], is presented along with the relevant figures.

One important metric for quantifying the level of chaotic behavior in dynamical systems is the Lyapunov exponent (LE). Similarly, bifurcation analysis provides insight into the qualitative behavior of nonlinear systems as control parameters change. Lyapunov exponents together with bifurcation diagrams provide insight into whether a fractional-order system exhibits periodicity or chaos. Table 1 summarizes the maximum LE for each of the four system components under varying values of the parameter b and the order q.

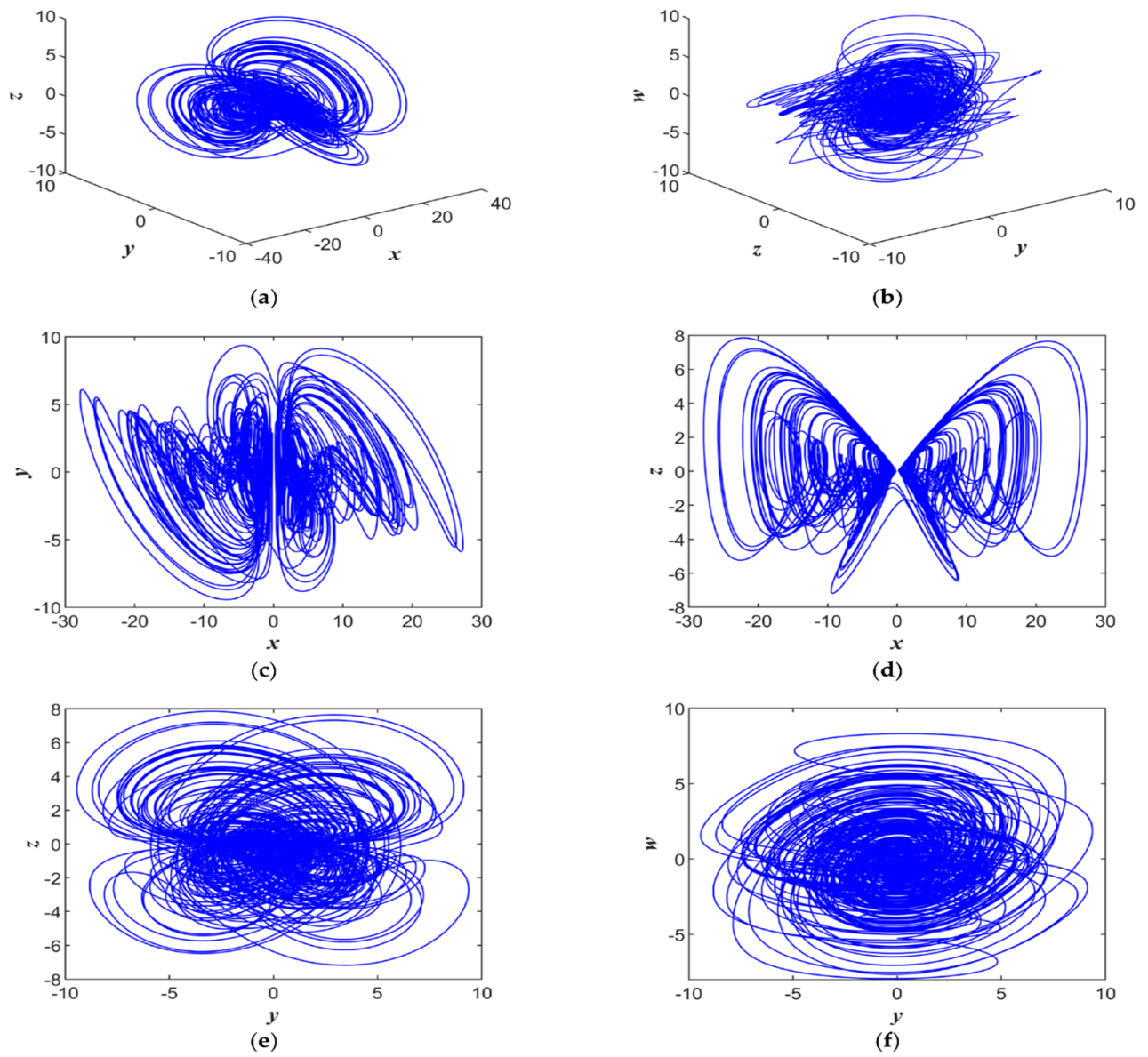


Figure 1. The system's chaotic attractor. (a) x–y–z, (b) y–z–w, (c) x–y, (d) x–z, (e) y–z, and (f) y–w [51].

Table 1. Max. LE under the set of varying values [51].

q	b	LE_1	LE_2	LE_3	LE_4
0.98	1.17	0.037	0.040	−0.117	−6.916
0.98	1.44	0.069	0.036	−0.188	−6.623
0.98	2	0.478	0.054	−0.366	−6.378
0.893	2	0.022	−0.151	−0.450	−10.788
0.934	2	0.193	−0.033	−0.625	−8.241

For initial conditions [1, 0, 0, 1] with constant parameters $a, c, d,$ and e, the fractional-order system (1) was simulated. By varying b from 0 to 3, the system transitioned from periodic to quasi-periodic and finally to chaotic behavior, as shown in Figure 2(a). The phase trajectories for $b = 1.17$

and $b = 1.44$ are shown in Figures 2(c) and 2(d), respectively, and the Lyapunov exponent curve confirms these transitions, revealing a double-sided attractor for $b > 1.5$, which is indicative of enhanced chaotic complexity suitable for pseudorandom sequence generation.

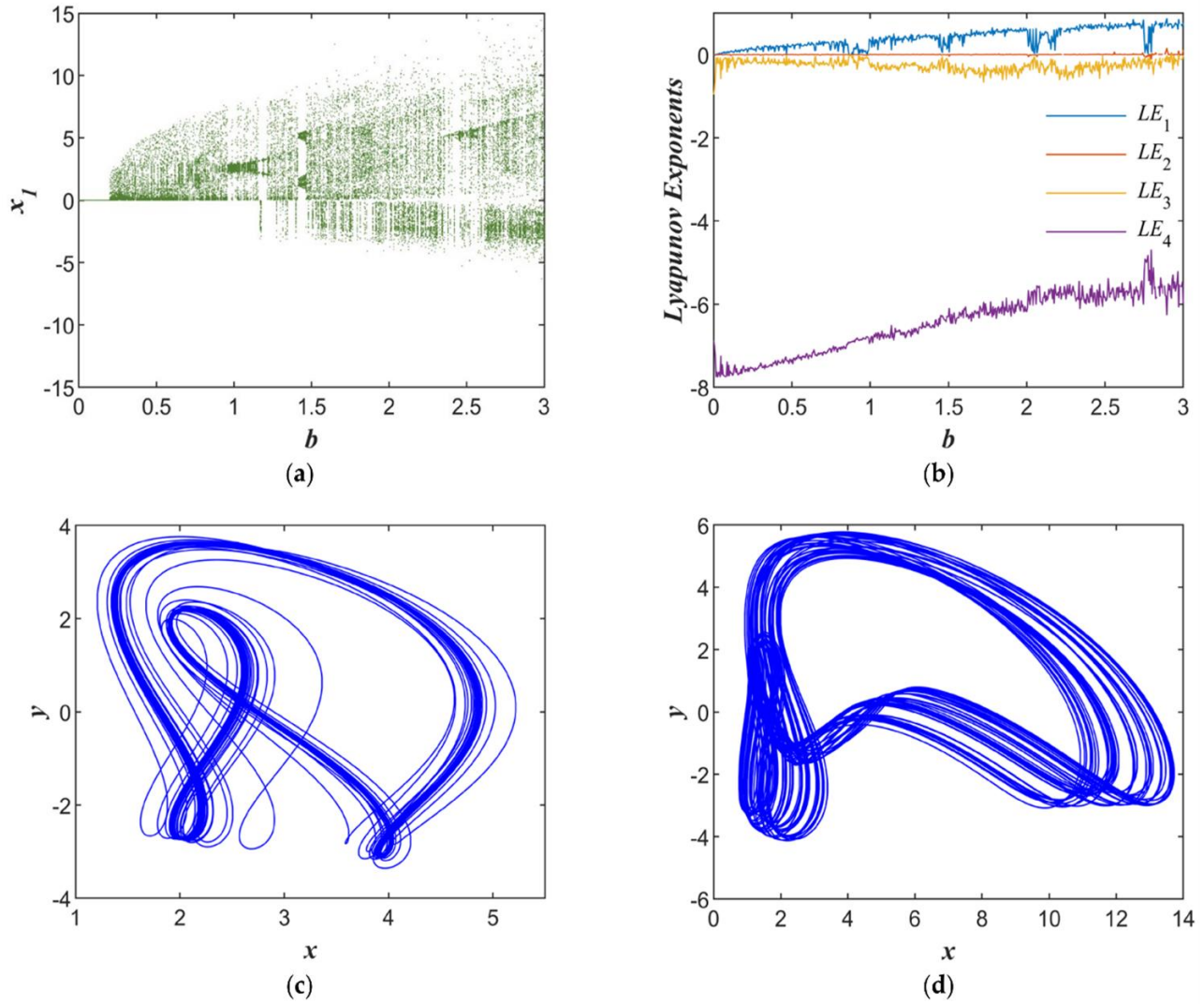


Figure 2. Bifurcation (a) and LE (b) diagrams of the system with $b \in [0,3]$; phase trajectories diagrams for $b = 1.17$ (c) and $b = 1.44$ (d) [51].

Keeping the initial conditions and parameters constant, the bifurcation and LE plots in Figures 3(a) and 3(b) show that System (1) transitions from periodic through quasi-periodic to chaotic behavior as q increases from 0.8 to 1.

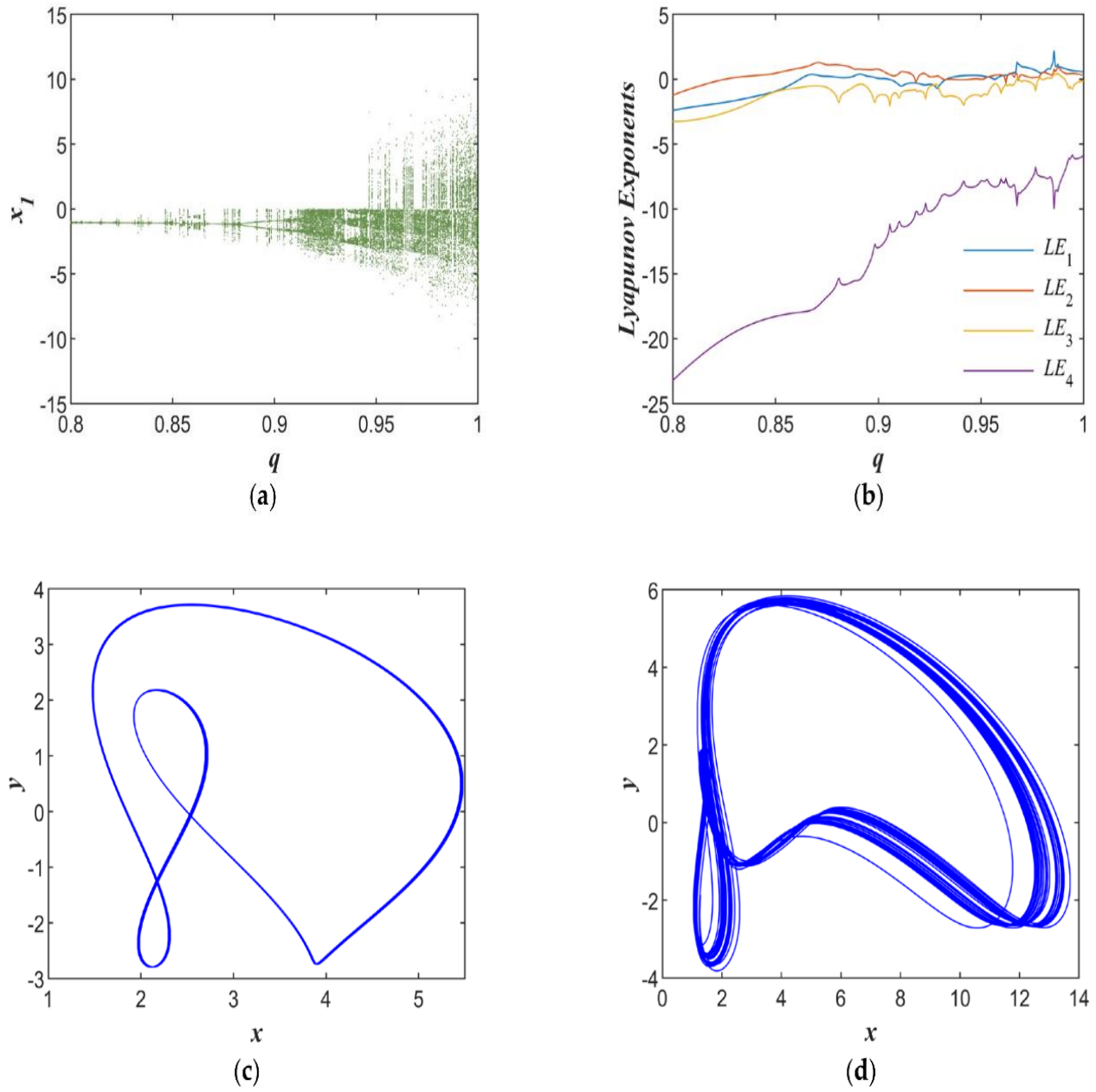


Figure 3. Bifurcation (a) and LE (b) diagrams of the system for $q \in [0.8,1]$; phase trajectories diagrams for $q = 0.893$(c) and $q = 0.934$ (d) [51].

The LE plot confirms this behavior. With $q = 0.893$ and $q = 0.934$, Figures 3(c) and 3(d) present the phase trajectories in the x–y plane, respectively, highlighting the system's complex dynamics as the fractional order q changes.

3.2. 1D chaotic map

The piecewise-logistic-Sine map (PLSM) integrates the dynamic features of both the logistic and sine maps while incorporating a piecewise function to strengthen its chaotic behavior. Additionally, piecewise linear chaotic maps are combined with this structure to form a hybrid system that exhibits

enhanced diffusion and overall security properties. By leveraging the strengths of 1D-chaotic map, the PLSM effectively disperses small variations throughout the image, enabling highly effective secure image encryption. The PLSM defined as follows [52]:

$$x_{n+1} = G(x_n, r, \rho) = \begin{cases} sin\left(\pi\left(4rx_n(1-x_n) + (1-r)\frac{x_n}{\rho}\right)\right), & 0 < x_n < \rho, \\ sin(\pi(4rx_n(1-x_n) + (1-r)\frac{x_n-\rho}{1-\rho})), & \rho \le x_n < 0.5, \\ G(1-x_n, r, \rho), & 0.5 \le x_n < 1. \end{cases} \quad (2)$$

Here, $x_0 \in (0,1)$ denotes the initial condition of the chaotic map, x_n represents the state variable at the iteration n, and r is the system parameter. It can be observed from Eq (2) that the PLSM possesses two key parameters: the segmentation parameter $\rho \in (0,0.5)$ and the control parameter $r \in [0,1]$. Regardless of variations in these parameters, the output of the PLSM consistently remains within the range [0,1]. This behavior makes it ideal for image encryption, as small changes in the initial conditions rapidly propagate through the system, enhancing its security for cryptographic applications. To avoid redundancy, a detailed examination of its dynamical behavior is presented in [52].

4. Proposed algorithm

We describe the proposed framework for encrypting medical images, incorporating two complementary processes in this section. First, a fractional-order (4D) chaotic system is utilized to perform confusion by permuting pixel positions across the image. Second, a symmetric diffusion matrix, is combined with the generated sequence from a 1D chaotic map, PLSM, to modify pixel intensities and ensure strong diffusion. The proposed encryption process is illustrated in Figure 4. Together, these stages provide high security while guaranteeing exact reversibility, an essential requirement for preserving the integrity of medical images.

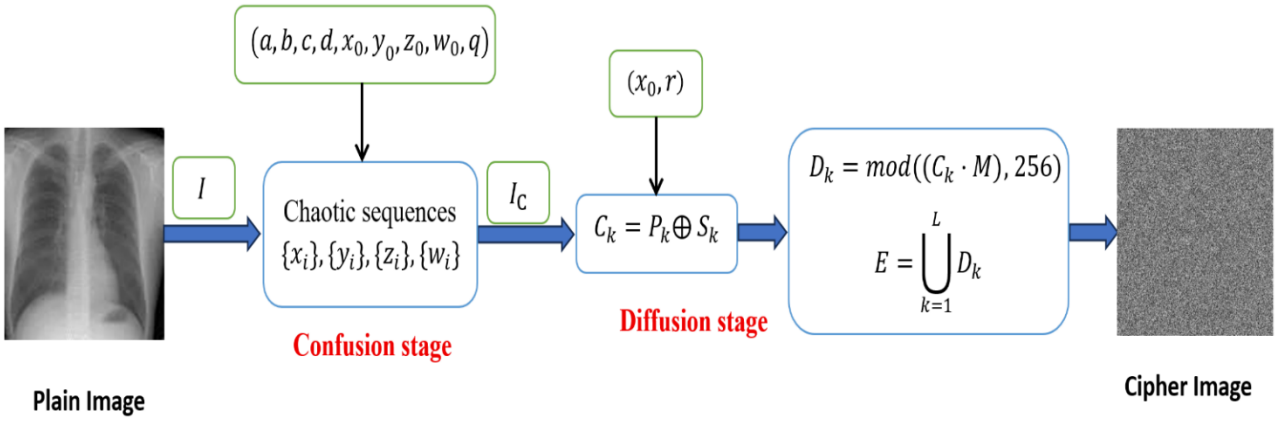


Figure 4. General diagram of the encryption process.

4.1. Encryption process

4.1.1. Confusion stage

In this subsection, the confusion stage of the encryption process is described, with the detailed procedural steps provided as follows:

Step 1: Consider the input plaintext medical image I of size $M \times N$.

Step 2: Flatten the image I of size $M \times N$ into a one-dimensional vector V.

Step 3: Initialize the chaotic system by selecting the system parameters (a, b, c, d), the fractional order $q \in (0,1)$, and the initial conditions (x_0, y_0, z_0, w_0); these values are combined to design the secret key, and the system is then initialized according to Eq (1) based on the given image as follows:

$$x_1 = \frac{\sum_{i=1}^{MN} V(i)+(M\times N)}{2^{23}+M\times N}. \tag{3}$$

For computing the other initials, we use

$$x_i = mod(x_{i-1}10^8, 1), \quad \text{where } i = 2, 3, 4. \tag{4}$$

where mod (•) represents the modulus after division, x_1, x_2, x_3, x_4, represent the 4D fractional-order system's initial condition, and the image vector's length is denoted by MN.

Step 4: Iterating the fractional 4D chaotic model results in the generation of four chaotic sequences, $\{x_i\}, \{y_i\}, \{z_i\}, \{w_i\}$. A sequence H of length MN is then obtained by running the system in Eq (1) for $N_0 + MN$ iterations. The initial N_0 values are discarded, and the sequences $\{x_i\}$ are selected.

Step 5: Use chaotic sequence $\{x_i\}$ to generate a permutation vector of length $M \times N$:

- Sort the chaotic sequence H (e.g., $\{x_i\}$) in ascending order to obtain P.
- Record the original indices of the sorted sequence. These indices form the permutation pattern.

Step 6: Permute the pixel positions of the vector according to the chaotic permutation vector, resulting in a newly shuffled sequence $I_{confused}$ as follows:

$$I_{confused} = V(P_i), \qquad i = 1,2, \dots, MN. \tag{5}$$

Step 7: Reshape the 1D the permuted vector $I_{confused}$ to obtain the confused image I_C with dimensions $M \times N$.

4.1.2. Diffusion stage

The diffusion stage of the proposed scheme relies on a symmetric matrix with invertibility that is combined with a one-dimensional chaotic map.

Step 1: Image partitioning into sub-blocks

Given a confused image I_C of size $M \times N$, it is partitioned into nonoverlapping 4×4 sub-blocks, where L = (M × N) /16. Each sub-block is represented as

$$P_k \in Z_{256}^{4\times 4}, k = 1,2, \dots, L. \tag{6}$$

Step 2: Chaotic sequence construction

A 1D chaotic map in Eq (2) is employed to generate a chaotic sequence. From the initial conditions (x_0, r), the sequence is produced and scaled into 8-bit integers to produce values in {0,…,255}

as

$$S_i = \lfloor x_i \times 10^{14} \rfloor \, mod \, 256, \quad i = 1,2, \ldots, MN. \tag{7}$$

Step 3: Symmetric matrix

A 4×4 symmetric matrix defined as follows:

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{bmatrix}. \tag{8}$$

Step 4: Diffusion operation

- During the diffusion phase, a symmetric matrix M is applied, and the scrambled image is partitioned into 4×4 sub-blocks represented by P_k.

For each scrambled block P_k, an XOR operation is performed to construct the corresponding block C_k as

$$C_k = P_k \oplus S_k. \tag{9}$$

By multiplying M by C_k, the modified pixel block D_k, is calculated as:

$$D_k = (C_k \cdot M) mod 256. \tag{10}$$

Eq (10) can be represented as:

$$\begin{bmatrix} D_{i,j} & D_{i,j+1} & D_{i,j+2} & D_{i,j+3} \\ D_{i+1,j} & D_{i+1,j+1} & D_{i+1,j+2} & D_{i+1,j+3} \\ D_{i+2,j} & D_{i+2,j+1} & D_{i+2,j+2} & D_{i+2,j+3} \\ D_{i+3,j} & D_{i+3,j+1} & D_{i+3,j+2} & D_{i+3,j+3} \end{bmatrix} = \begin{bmatrix} C_{i,j} & C_{i,j+1} & C_{i,j+2} & C_{i,j+3} \\ C_{i+1,j} & C_{i+1,j+1} & C_{i+1,j+2} & C_{i+1,j+3} \\ C_{i+2,j} & C_{i+2,j+1} & C_{i+2,j+2} & C_{i+2,j+3} \\ C_{i+3,j} & C_{i+3,j+1} & C_{i+3,j+2} & C_{i+3,j+3} \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{bmatrix} \bmod 256, \tag{11}$$

$$i = 1 : 4 : M; \; j = 1 : 4 : N$$

- The final cipher image E is obtained by combining all cipher blocks D_k:

$$E = \bigcup_{k=1}^{L} D_k \tag{12}$$

4.2. Decryption process

Decryption in the proposed method exactly reverses the encryption by reversing the encryption steps, making the algorithm fully reversible. The diffusion stage is reconstructed using the modular inverse of the symmetric matrix, and the same set of secret keys is applied to achieve exact recovery of the original image.

5. Experimental results and security analysis

To assess the performance of the suggested approach, this section provides comprehensive experiments and a thorough security analysis. The Adams-Bashforth-Moulton method is widely adopted for fractional-order differential equations; it was used to generate the solutions of the model in Eq (1). A step size of $h = 0.001$ was used to ensure accurate and stability representation of the chaotic dynamics. The simulation was conducted over the fractional order $q = 0.98$ and for the initial conditions $[1,0,0,1]$. The experiments were carried out in MATLAB R2015a on a laptop featuring an Intel(R) Core(TM) i7-2.9 GHz processor and 8GB RAM and using the Windows 11 operating system. Samples of medical images from various modalities, including X-ray, CT, and MRI, each with a size of 512 × 512 pixels, were used in the experiments and are shown in Figure 5. In addition, the results obtained are compared with existing algorithms previously reported [26, 28, 32, 37, 39] to highlight the relative performance of the proposed algorithm.

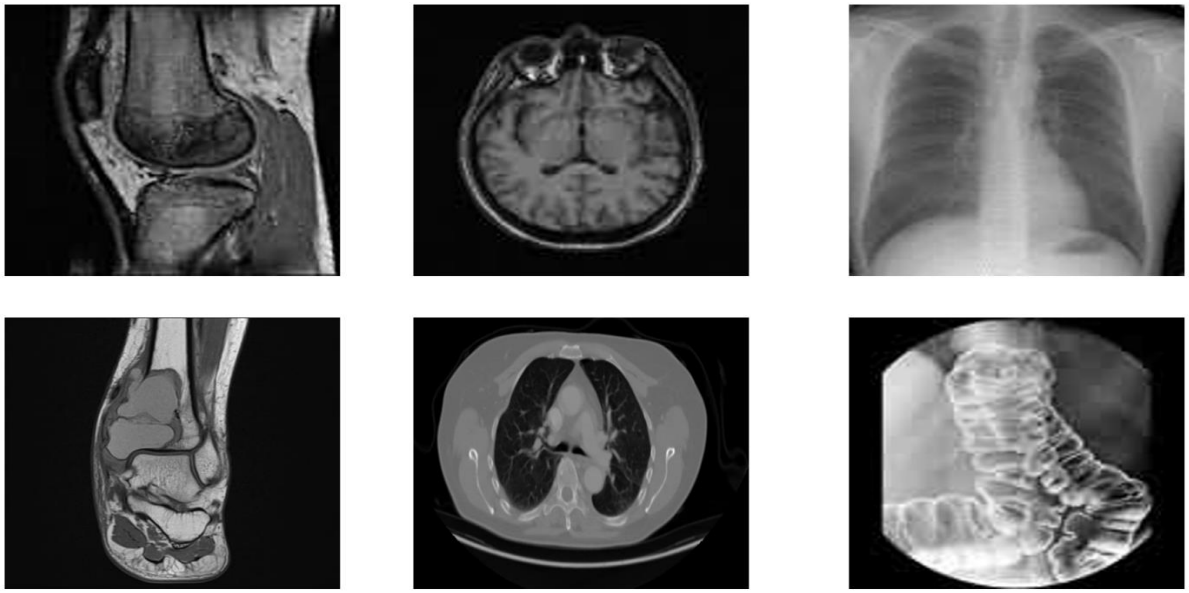


Figure 5. Medical images.

5.1. Visual analysis

The primary consideration for evaluating an image encryption method is its effect on human visual perception, ensuring that the encrypted image conceals information effectively. Visual evaluation assesses the differences and resemblance between the plain medical image and its encrypted and decrypted versions. To examine the visual performance and perceptual integrity of the suggested encryption and decryption algorithm, experiments were carried out on 512×512 standard medical images, as presented in Figure 5.

Figure 6 shows the medical images through the complete encryption and decryption process. It is evident that the original image contains clear diagnostic details, whereas the encrypted version is completely noise-like in nature, exhibiting no recognizable features or resemblance to the plain image, effectively concealing sensitive information. After applying the correct keys, decryption reproduces

the plain images exactly, fully restoring all anatomical structures necessary for accurate diagnosis, achieving strong visual security, and confirming that the proposed encryption algorithm successfully protects sensitive medical content from visual inspection.

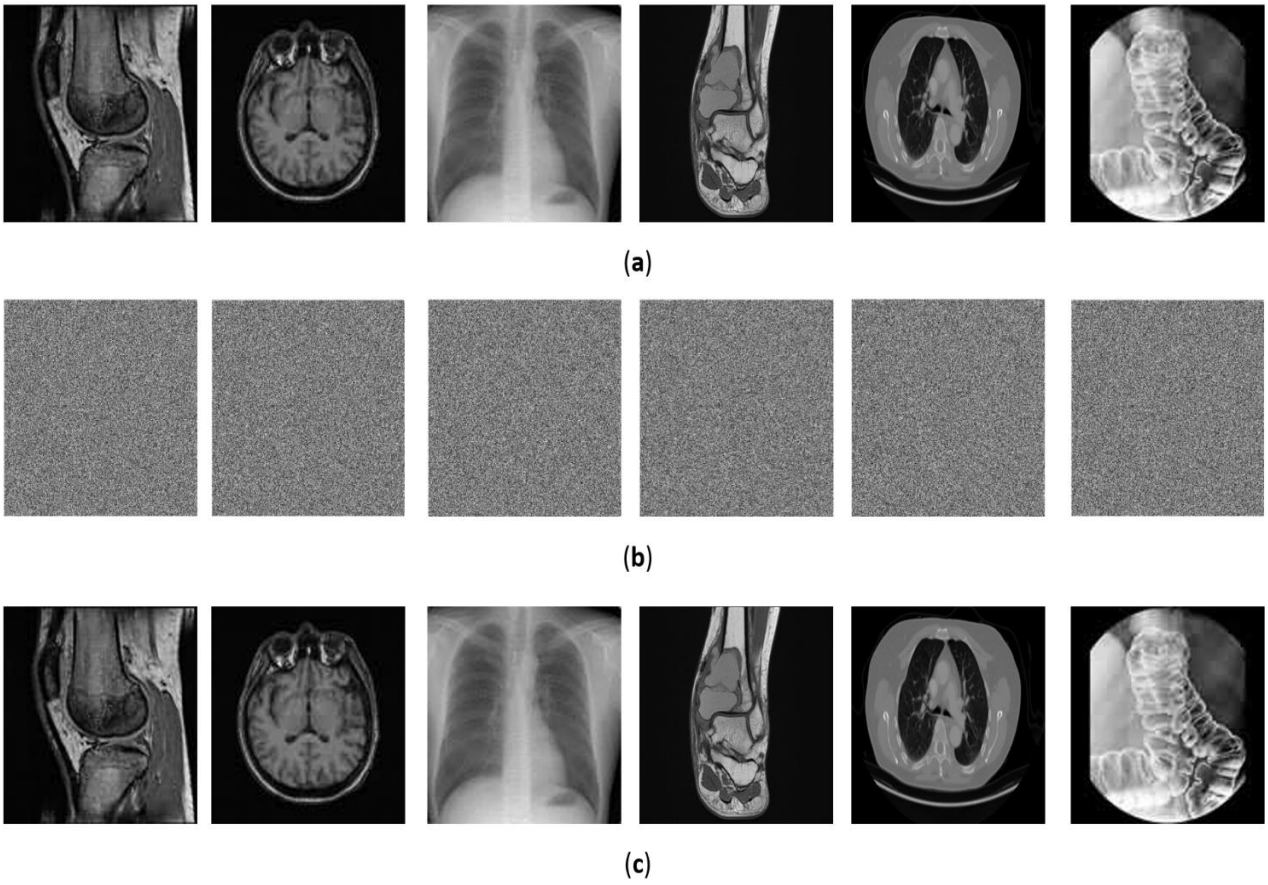


Figure 6. Visual results of (a) plain, (b) encrypted, and (c) decrypted images, respectively.

5.2. Statistical analysis

To thoroughly examine the security characteristics of the suggested algorithm, this subsection analyzes key statistical indicators, including information entropy, histogram distributions, and correlation coefficients, which collectively reflect its resilience to statistical attacks.

5.2.1. Information entropy analysis

Information entropy is a statistical metric widely used to examine uncertainty and randomness, reflecting the amount of information or complexity contained within the data. Within the domain of image encryption, entropy reflects an algorithm's ability to securely and effectively obscure information. A high entropy value signifies strong randomness, safeguarding the image against prediction or reconstruction. Conversely, a lower entropy value suggests that certain pixel values dominate, reducing randomness and compromising security. Mathematically, the information entropy H can be computed as follows:

$$H = -\sum_{i=0}^{L-1} P(i) \log_2 P(i), \tag{13}$$

where $P(i)$ specifies the probability of occurrence of i, and L refers to the total possible gray levels.

For effective medical image encryption, plain medical images have relatively lower entropy values, reflecting predictable pixel distributions. After encryption, the cipher images exhibit much higher entropy, nearing the ideal value of 8. This indicates uniformly distributed pixels and strong randomness, ensuring that sensitive medical information is securely protected. Tables 2 and 3 summarize the information entropy values of 256 × 256 and 512 × 512 medical images, comparing the plain images with their corresponding encrypted versions. It is evident from Tables 2 and 3 that the entropy values of the ciphered images all exceed 7.99, nearly reaching the theoretical maximum of 8, demonstrating that the suggested algorithm generates highly random ciphertext images, resulting in strong encryption and improved image security. Furthermore, this high level of unpredictability enhances resistance to statistical attacks, providing more robust protection for sensitive medical data.

Table 2. Entropy values of 256 × 256 medical images.

Image	Plain Image	Encrypted Image
I1	6.9022	7.9975
I2	5.4294	7.9972
I3	7.2368	7.9971
I4	5.3969	7.9971
I5	5.6643	7.9976
I6	6.9022	7.9975

Table 3. Entropy values of 512×512 medical images.

Image	Plain Image	Encrypted Image
I1	5.8696	7.9993
I2	5.4297	7.9993
I3	7.2384	7.9993
I4	5.4626	7.9994
I5	5.6749	7.9993
I6	6.9011	7.9993

Table 4 demonstrates the entropy values of the proposed method in comparison with several approaches [33, 35, 39, 44, 46, 52], showing that the proposed algorithm achieves values comparable to or higher than those of the existing algorithms across different types of 256 × 256 medical images, with a best average entropy of 7.9994, indicating enhanced randomness and stronger security.

Table 4. Comparing the entropy of encrypted medical images.

Algorithm	I1	I2	I3	I4	I5	I6	Average
Proposed	7.9975	7.9972	7.9971	7.9971	7.9976	7.9975	7.9973
[33]	7.9970	7.9972	7.9974	7.9973	7.9970	7.9967	7.9971
[35]	7.9826	7.9831	7.9858	7.9832	7.9839	7.9838	7.9837
[39]	7.9974	7.9973	7.9971	7.9972	7.9974	7.9970	7.9972
[44]	7.9958	7.9947	7.9966	7.9961	7.9953	7.9928	7.9952
[46]	7.9891	7.9896	7.9891	7.9894	7.9891	7.9890	7.9892
[52]	7.9964	7.9845	7.9976	7.9955	7.9673	7.9802	7.9869

5.2.2. Histogram analysis

The histogram determines how pixel intensities are distributed within an image, offering a key metric to assess the efficacy of an encryption algorithm. The histograms of the encrypted images should be nearly uniform or flat. This signifies that every possible pixel value appears with an equal probability of occurrence, making it statistically indistinguishable from random noise. The histograms of the plain images exhibit concentrated peaks corresponding to common gray levels, revealing structural details. After encryption, the histograms exhibit a distribution that is near-uniform, with pixel values spread across the full gray-level range. Because medical images require high confidentiality, an effective encryption algorithm should produce a flat histogram without noticeable peaks. This uniform distribution demonstrates that the proposed method successfully conceals image content, eliminates statistical patterns, and prevents information leakage, thereby enhancing the security of sensitive medical data. Figure 7 illustrates the plaintext and encrypted images alongside their histograms. The ciphertext histograms exhibit a uniform distribution, whereas the plaintext histograms display concentrated gray-level patterns. This result demonstrates that the encrypted images contain no discernible statistical features, making information extraction impossible and demonstrating the proposed algorithm's strong capability to conceal the content of medical images.

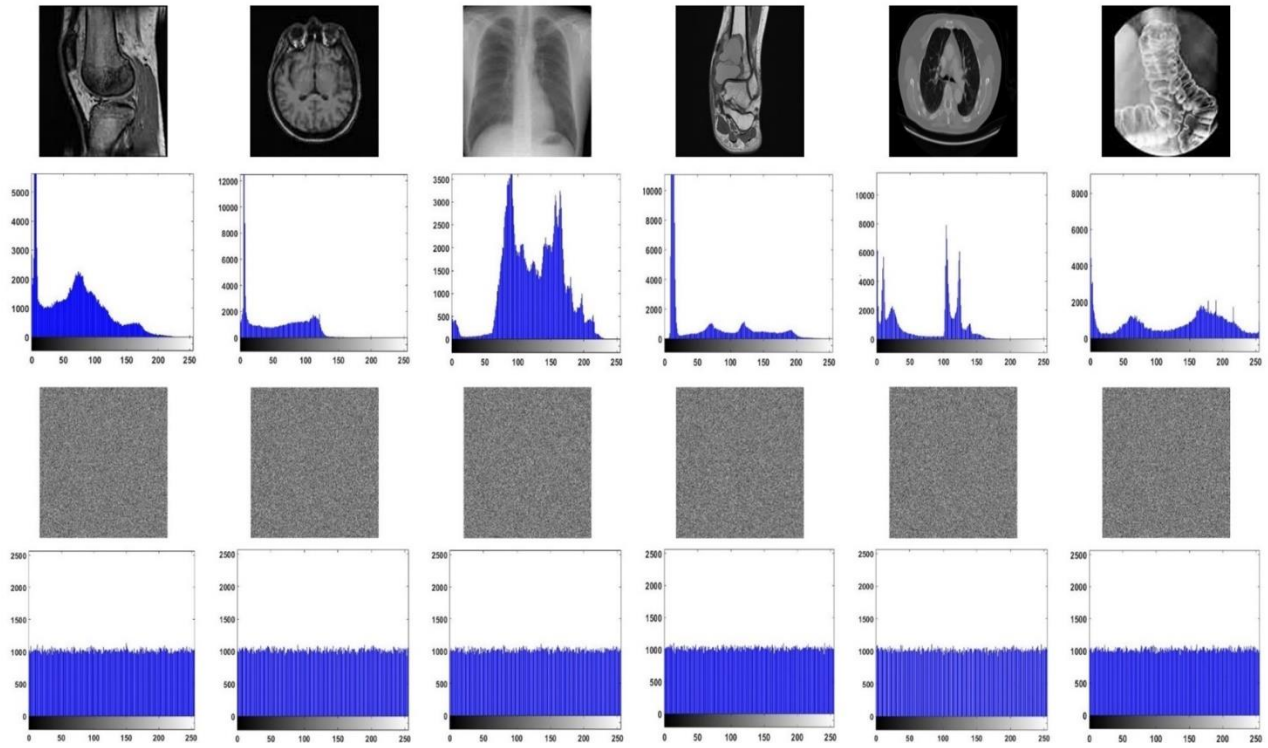


Figure 7. The original and ciphered image histograms.

5.2.3. Correlation analysis

Correlation analysis is a crucial metric for examining the effectiveness of the encryption scheme. The inherent correlation in plaintext images presents a statistical weakness that correlation-based attacks can exploit to undermine encryption security. The objective is to remove any statistical redundancy present in the plain image so that the ciphered image appears completely random and secure in the cryptosystem. This section assesses the correlations between adjacent pixels in grayscale medical images in horizontal (H), vertical (V), and diagonal (D) directions, comparing the results before and after encryption. The correlation coefficient $r_{x,y}$ is calculated as follows:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \big(x_i - E(x)\big)^2,$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} \big(x_i - E(x)\big)\big(y_i - E(y)\big), \tag{14}$$

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

where N denotes the total number of adjacent pixels, and x and y represent the intensity values of two neighboring pixels in the image. The mathematical expectation and variance of x are denoted by $E(x)$ and $D(x)$, respectively, and $Cov(x, y)$ indicates the covariance between x and y.

For a plaintext image, the correlation coefficient is close to 1, reflecting a strong linear dependency between adjacent pixels. In contrast, for an encrypted image, the value should approach 0, demonstrating that the encryption has efficiently removed statistical relationships. Therefore, evaluating the correlation coefficient in H, V, and D directions provides a reliable measure of the encryption scheme's ability to eliminate pixel-to-pixel dependencies. To quantitatively evaluate the correlation analysis, a set of $N = 10{,}000$ adjacent pixel pairs were randomly chosen from each medical image. The resulting correlation coefficients in the directions (H, V, D), computed using the suggested algorithm, are reported in Table 5.

Table 5 clearly demonstrates that the plain images have coefficients near 1, confirming a strong linear dependency, whereas the encrypted images have coefficients near 0, demonstrating that the suggested algorithm successfully destroys statistical relationships among neighboring pixels, confirming its robustness against statistical attacks and its ability to secure sensitive medical data. Thus, it is not possible to predict a pixel's value by the values of its neighboring pixels.

Table 5. A summary of the correlation coefficients for sample 512 × 512 medical images.

Image	Plain image			Encrypted image		
	H	V	D	H	V	D
I1	0.9931	0.9968	0.9914	0.0014	-0.00060	-0.000175
I2	0.9956	0.9966	0.9924	-0.0022	-0.002387	0.000380
I3	0.9992	0.9995	0.9987	0.0018	-0.002613	-0.001450
I4	0.9861	0.9896	0.9773	0.0008	0.000302	0.001049
I5	0.9945	0.9962	0.9909	-0.0015	-0.003751	-0.000912
I6	0.9978	0.9975	0.9951	-0.001822	-0.001192	-0.000620

To visually assess the correlation coefficients, Figure 8 shows the correlation coefficients of three selected original medical images and their encrypted versions, illustrating the relationships between adjacent pixels in the directions (H, V, D). As shown in Figure 8, the correlation plots of the plain images form a spindle shape, with pixels strongly aligned along the diagonal, demonstrating strong correlation among adjacent pixels. Those of the encrypted images, however, appear randomly distributed, reflecting uniform pixel values and the absence of correlation between neighboring pixels. This shows that the encryption successfully eliminates any predictable patterns, ensuring that the ciphertext reveals no information about the structure of the plain images.

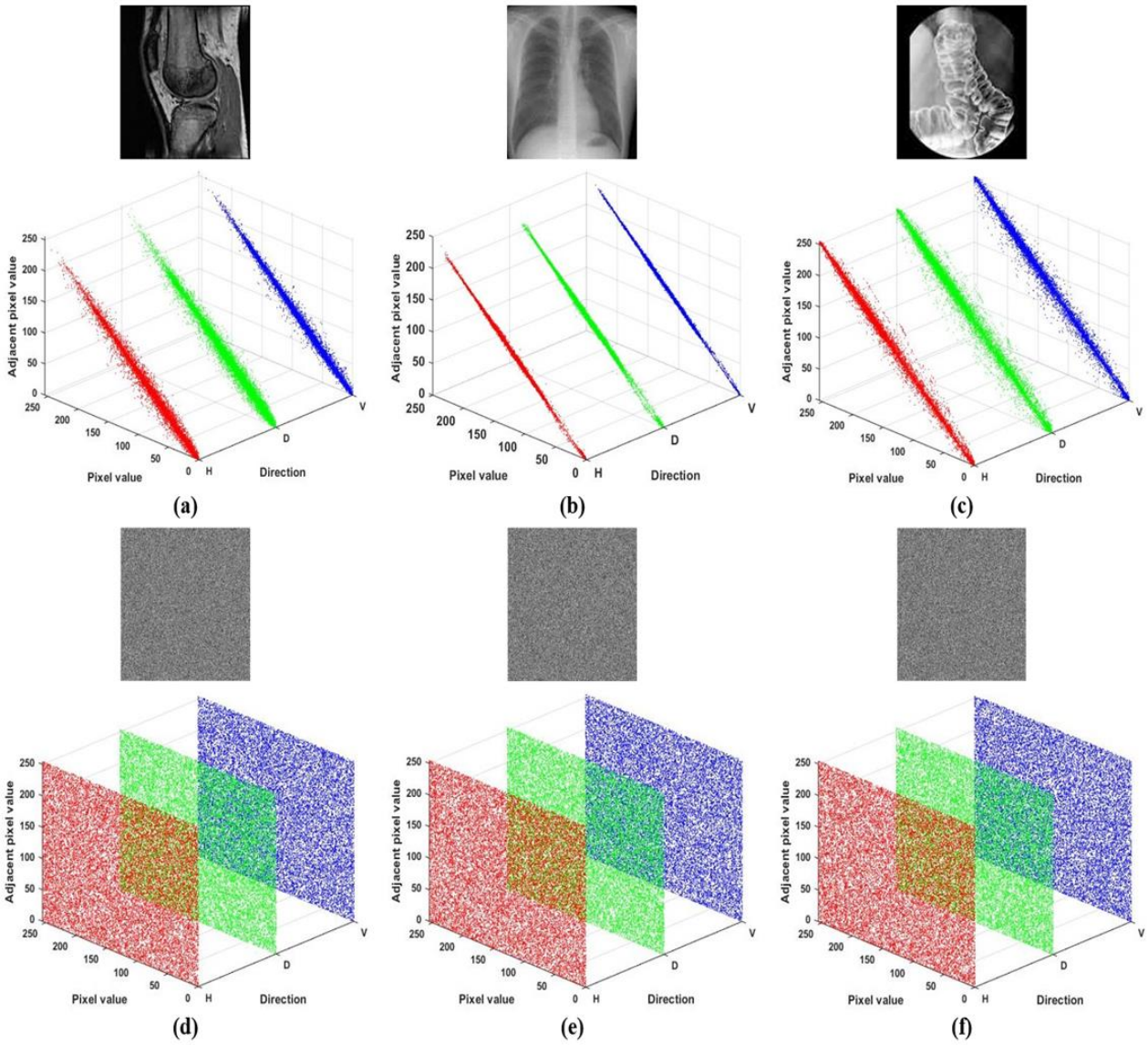


Figure 8. Correlation of adjacent pixels in (H, D, V): (a)–(c) plaintext images, (d)–(f) ciphered images.

Table 6 shows a comparison of the average and standard deviations values of correlation coefficient in all directions computed by suggested algorithm and various algorithms. Although all algorithms succeed in lowering pixel correlations in the encrypted images, the proposed method exhibits a noticeably stronger reduction in certain cases. Overall, the findings highlight that the suggested algorithm consistently minimizes pixel correlations in the three directions, outperforming the compared algorithms and providing enhanced security against statistical attacks.

Table 6. Comparison of correlation coefficients in (H, D, V) for images with the size of 512 × 512.

Algorithm	Direction	Cipher images							
		I1	I2	I3	I4	I5	I6	Average	STDV
Proposed	H	0.0014	-0.0022	0.0018	0.0008	-0.0015	-0.0018	6.0E-05	0.0018
	V	-0.0006	-0.0024	-0.0026	0.0003	-0.0038	-0.0012	-0.0017	0.0015
	D	-0.0002	0.0004	-0.0015	0.0011	-0.0009	-0.0006	-2.83E-04	9.33Ee-04
[33]	H	0.0100	-0.0200	-0.0155	-0.0191	0.0063	0.0063	-0.0053	0.0142
	V	0.0127	0.0198	0.0207	-0.0066	0.0213	0.0031	0.0118	0.0114
	D	0.0112	-0.0055	0.0118	0.0145	-0.0045	0.0149	0.0071	0.0095
[35]	H	0.0138	0.0581	-0.0381	-0.0281	0.0471	-0.0148	0.0063	0.0400
	V	-0.0372	0.0415	0.0259	-0.0167	0.0238	0.0133	0.0084	0.0296
	D	0.0769	0.0823	0.0718	0.0647	0.0837	0.0853	0.0775	0.0080
[39]	H	-0.0098	-0.0145	0.0155	-0.0094	0.0101	-0.0057	-0.0023	0.0121
	V	-0.0113	-0.0034	-0.0067	0.0003	-0.0040	-0.0045	-0.0049	0.0039
	D	-0.0136	0.0100	-0.0100	-0.0124	0.0031	0.0128	-0.0017	0.0118
[44]	H	-0.0070	0.0008	0.0057	-0.0070	0.0117	0.0050	0.0015	0.0075
	V	0.0127	0.0267	0.0150	-0.0045	0.0125	0.0100	0.0121	0.0100
	D	0.0037	-0.0139	-0.0130	0.0223	-0.0064	0.0017	-9.33E-04	0.0135
[46]	H	-0.0320	-0.0064	0.0055	0.0113	0.0071	-0.0069	-0.0036	0.0158
	V	0.0010	0.0071	-0.0015	-0.0093	-0.0017	-0.0135	-0.0030	0.0074
	D	-0.0079	0.0073	0.0048	0.0111	0.0058	-0.0094	0.0020	0.0085
[52]	H	-0.0124	0.0134	-0.0139	0.0181	-0.0098	-0.0062	-0.0018	0.0139
	V	0.0053	0.0101	0.0073	0.0060	0.0118	0.0214	0.0103	0.0060
	D	0.0143	0.0060	-0.0014	-0.0029	-0.0114	0.0283	0.0055	0.0142

5.2.4. NIST SP800-22 test

The NIST test examines the randomness characteristics of cryptographic algorithms and their generated chaotic sequences. The test suite consists of 15 distinct tests, each targeting a specific aspect of randomness. These subtests provide an essential measure of an encryption algorithm's security and suitability for cryptographic applications through the analysis of the statistical characteristics of the encrypted data. A sequence was considered statistically random if its corresponding P-value exceeded a significance level of 0.01. As reported in Table 7, the computed P-values consistently exceed the threshold of 0.01, demonstrating that the proposed scheme successfully satisfies all NIST statistical test criteria. This confirms that the chaotic sequences produced by the F4DHS system exhibit strong

randomness properties suitable for cryptographic applications, thereby improving both overall effectiveness and the security robustness of the suggested encryption algorithm.

Table 7. NIST SP 800-22 results.

No.	Test	P-Value	Result
1	Frequency	0.2185	✓
2	Block Frequency	0.7837	✓
3	Cumulative Sums	0.4761	✓
4	Runs	0.5148	✓
5	Longest Run	0.2447	✓
6	Binary Matrix Rank	0.2649	✓
7	FFT	0.6415	✓
8	Non-Overlapping Template	0.2506	✓
9	Overlapping Template	0.4150	✓
10	Approximate Entropy	0.5219	✓
11	Random Excursions	0.5658	✓
12	Random Excursions Variant	0.5418	✓
13	Linear Complexity	0.4976	✓
14	Serial	0.4236	✓
15	Universal	0.8115	✓

5.3. Keys analysis

5.3.1. Key space analysis

The key space serves as a crucial measure of the system's security and its resistance to brute-force attacks. A sufficiently large key space is required for the encryption algorithm to effectively withstand brute-force attacks. The total key space of proposed algorithm has 12 parameters such as:

1) Four initial values (x_0, y_0, z_0, w_0), five system parameters (a, b, c, d, e), and fractional order, q of the 4D fractional chaotic system.
2) The initial conditions (x_0, r) of the 1D chaotic map.

With an effective floating-point precision of 10^{-15}, the resulting total key space is $(10^{15})^{12} = 10^{180} \approx 2^{598}$, far exceeding the minimal threshold of 2^{100}. Consequently, the system secures sensitive medical images by employing an extensive key space, offering robust protection and high resilience to brute-force attacks. The key space of the suggested algorithm, as compared to various algorithms, is presented in Table 8. As seen in Table 8, the suggested algorithm has a larger key space, demonstrating strong resistance to brute-force attacks.

Table 8. Key space analysis.

Algorithm	Proposed	[33]	[35]	[39]	[44]	[46]	[52]
Key space	2^{598}	2^{116}	--	2^{256}	2^{512}	2^{177}	2^{256}

5.3.2. Key sensitivity analysis

Key sensitivity confirms that even minor alterations in the encryption key result in completely distinct cipher images. The proposed method is evaluated by decrypting with a slightly modified key to assess its robustness. It prevents attackers from extracting meaningful data, even with a key that deviates slightly from the correct one. Key sensitivity is tested by encrypting the image with the original key and decrypting it with a slightly changed key.

Key sensitivity is evaluated by making a small change to one of the initial values, x_0, y_0, w_0, z_0 of F4DHS by 10^{-15} at a time. For example, the initial value x_0 is modified as $x_0 + 10^{-15}$ whereas the other initial values y_0, w_0, z_0 are kept constant; we repeat this for all initial values. Figure 9 illustrates the encryption of medical image "I1" with both the correct key and a slightly altered key, respectively. As illustrated in Figure 9, slight alterations to the encryption key result in significant changes in the output images, demonstrating the superior key sensitivity and security of the suggested algorithm. To evaluate key sensitivity, decryption is performed with both the correct and a slightly altered key. Figure 10 demonstrates that the original plaintext cannot be retrieved with a modified key, confirming the suggested encryption algorithm's strong key sensitivity and robust security, as even a small variation in the secret key prevents successful decryption.

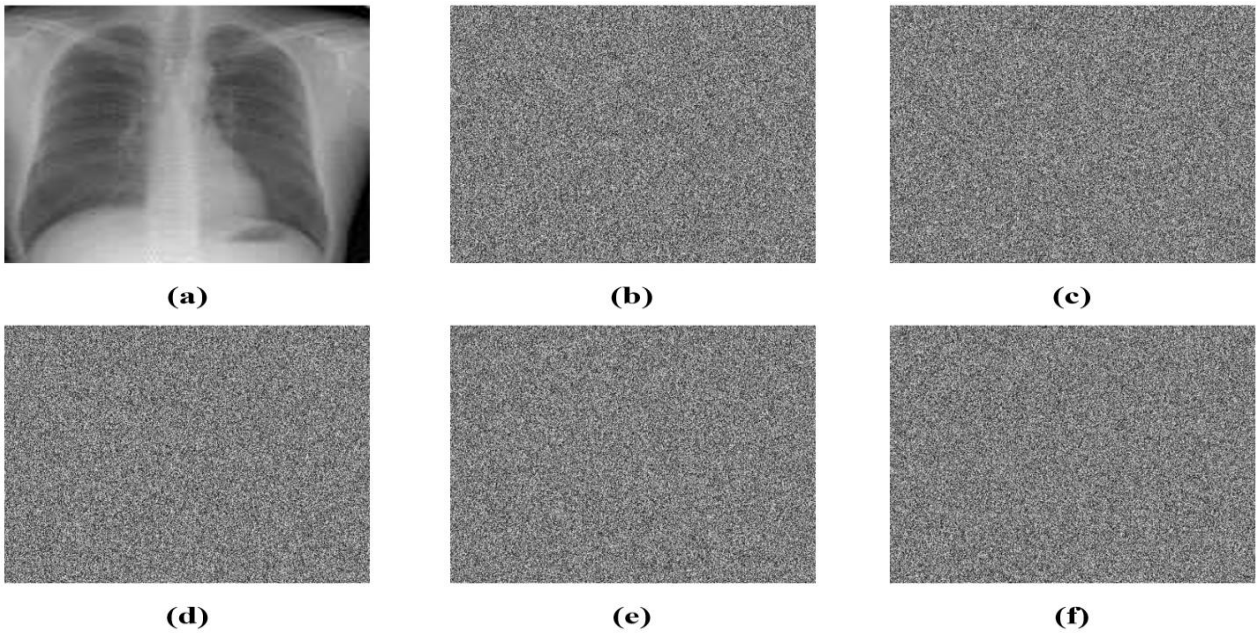


Figure 9. Key sensitivity test: (a) Original image; (b) Encrypted (a) with the correct key; (c–f) Encrypted (a) with a tiny variation (1×10^{-15}) in x_0, y_0, w_0, and z_0, respectively.

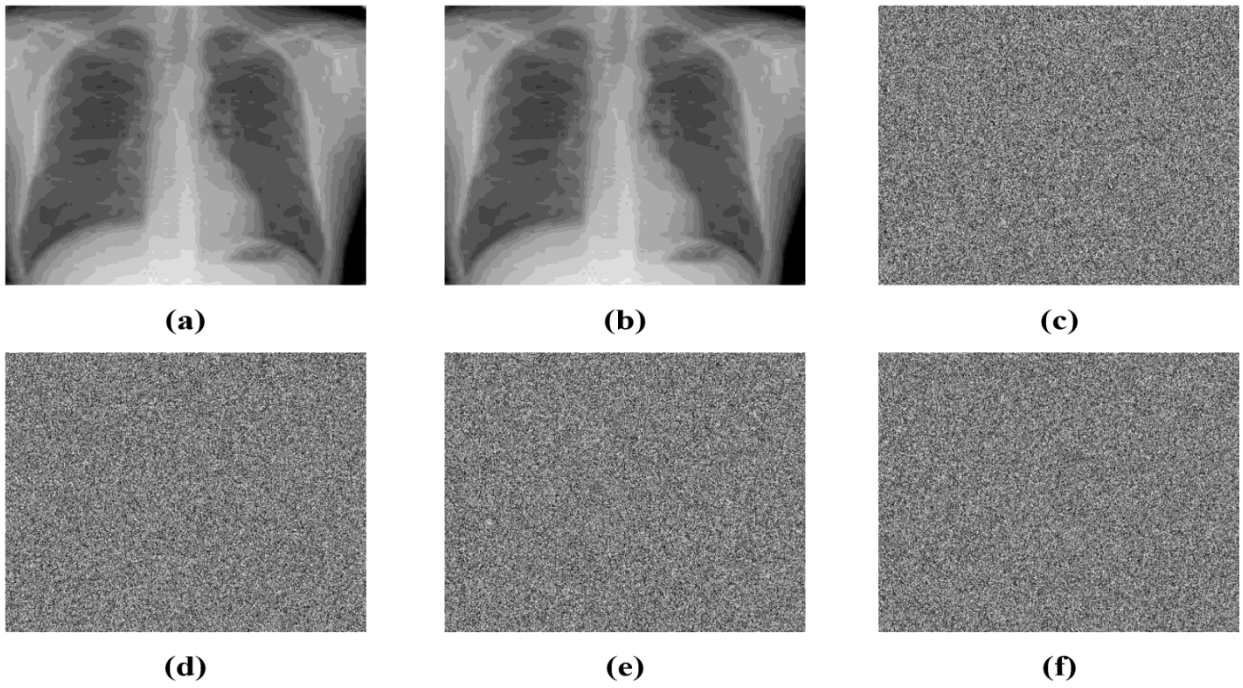


Figure 10. Key sensitivity test: (a) Original image; (b) Decrypted image with the correct key; (c–f) Decrypted images with minor variations (1×10^{-15}) in x_0, y_0, w_0, and z_0, respectively.

5.4. Differential attack analysis

A differential attack examines how minor changes in a plaintext image affect its ciphertext. Typically, two nearly identical images differing by only a single bit are encrypted, and the obtained encrypted images are compared. An effective encryption algorithm produces substantial and unpredictable differences in the ciphertext even for minimal plaintext modifications, highlighting its strong robustness to differential attacks, which are commonly quantified using the NPCR and UACI metrics. High NPCR and UACI values demonstrate the algorithm's strong robustness to differential attacks computed as follows:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%,$$

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

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{15}$$

where $C_1$and C_2 denote the ciphertexts resulting from encrypting two plaintext images, $P_1$and P_2, that differ by only a single pixel, using the same encryption key.

The theoretical values for an 8-bit image are 99.6094% for NPCR and 33.4635% for UACI. These values represent the expected outcomes for completely distinct ciphertexts. The closer the computed

values of NPCR and UACI are to these theoretical values, the more robust the algorithm is against differential attacks

This experiment is conducted in 50 rounds to examine the resistance of the suggested algorithm to differential attacks by introducing a random single-pixel modification in each plain image in each round. The results, presented in Table 9, were obtained by averaging these tests to ensure robustness. Because the observed NPCR and UACI values nearly match the theoretical benchmarks, it is clear that even minor alterations in the plaintext cause major and unpredictable differences in the cipher images. These results indicate that the suggested algorithm's superior resilience to differential attacks.

Table 9. Average values of UACI and NPCR.

Images	UACI (%)	NPCR (%)
I1	33.4667	99.6023
I2	33.4508	99.6170
I3	33.4595	99.6111
I4	33.4648	99.6114
I5	33.4668	99.6108
I6	33.4611	99.6084

5.5. Known-plaintext and chosen-plaintext attacks analysis

Among typical attacks, chosen-plaintext (CPAs) and known-plaintext attacks (KPAs) are considered the most powerful ones. In CPAs, adversaries often exploit specially constructed images such as entirely black or entirely white images to extract information about the secret key. These images are particularly attractive to attackers because of their uniform pixel values, which are 0 for black and 255 for white. Generally, an encryption algorithm that demonstrates resistance to CPAs is also likely to withstand other common types of attacks. For assessing the resilience of the suggested encryption scheme to CPAs and KPAs, tests are first carried out on two 512 × 512 images with uniform pixel values (all-black and all-white). Figure 11 shows the original images, their encrypted counterparts, and the histograms of the resulting cipher images, and an additional test result is presented in Table 10. As depicted in Figure 11, as the encryption of both particular plain images results in cipher images that exhibit noise-like, the histograms become more uniform and convey no information regarding the plain images, which indicates nondeterministic encryption. As a result, no meaningful information can be obtained from it. These results demonstrate that the suggested algorithm has the ability to resist KPAs and CPAs.

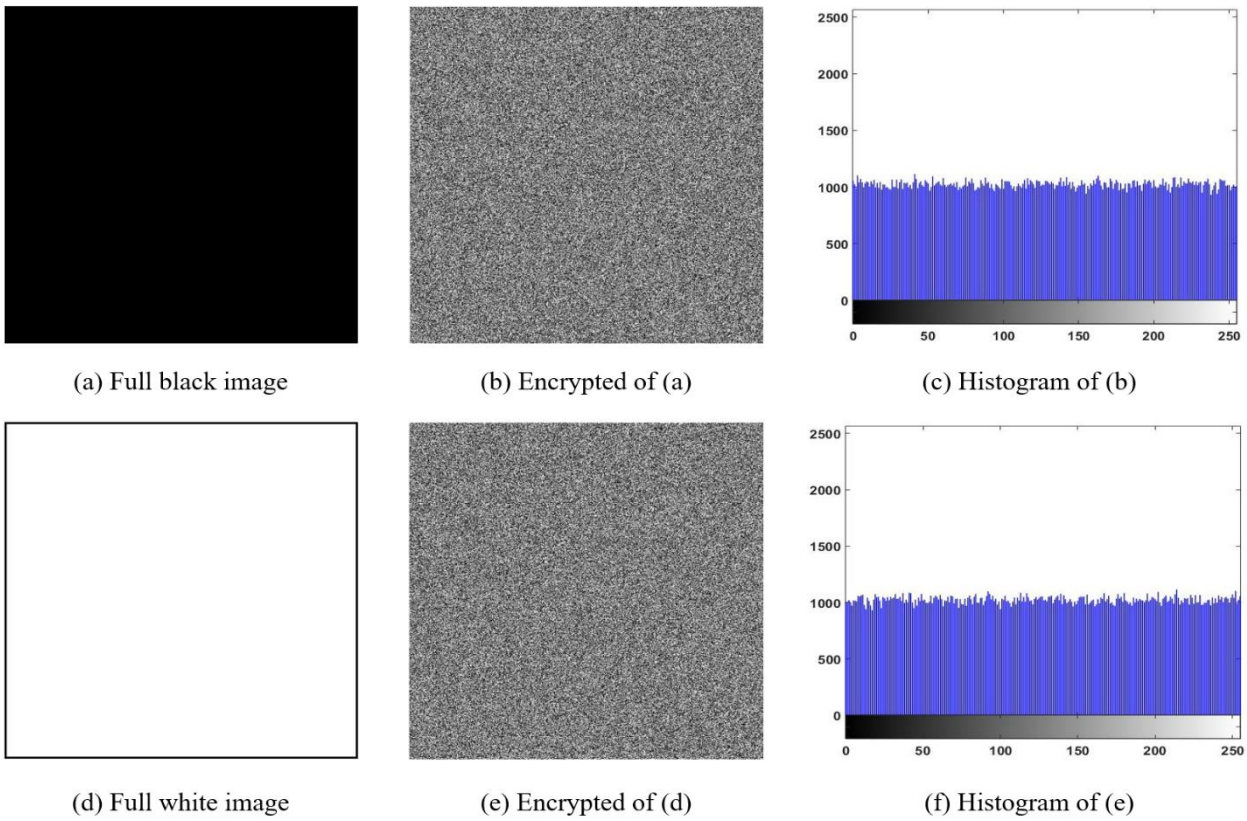
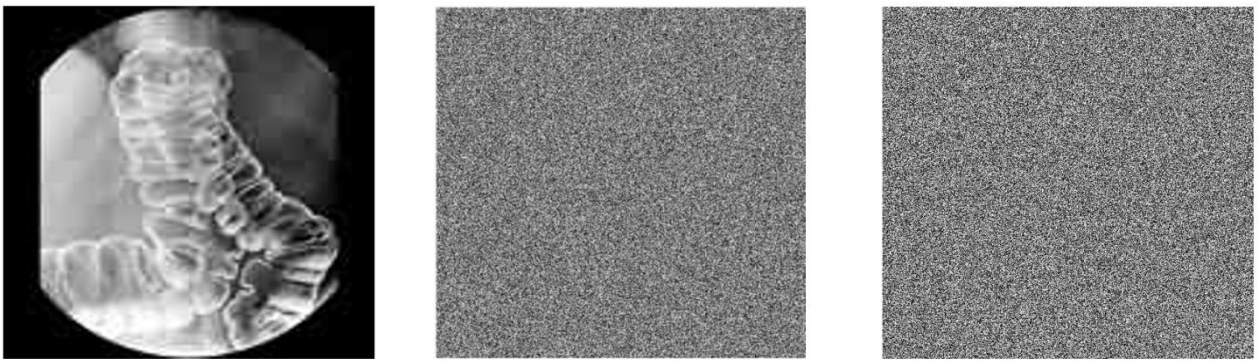


Figure 11. Analysis of chosen-plaintext and known-plaintext attacks analysis.

Table 10. Common test results of full-black and full-white images.

Image	Entropy	Correlation coefficient		
		H	V	D
Full-black	0	-	-	-
Full-black encrypted	7.9993	0.004742	0.004635	0.000328
Full-white	0	-	-	-
Full-white encrypted	7.9993	0.001359	-0.000797	0.008684

Second, the cryptosystem was tested against a CPA using the 512 × 512 plain image "I6". The attack failed to break the encryption, and the PSNR value between the decrypted and plain images was computed as 7.0367 dB. The PSNR results indicate very low similarity between the plain image and the ciphered image obtained via the CPA. As shown in Figure 12, the recovered image is entirely different from the original image, demonstrating that the proposed algorithm effectively resists CPAs. Consequently, an attacker is unable to extract any valuable data. Thus, the suggested algorithm is capable of resistance against these attacks.



(a) Plain image (b) Encrypted of (a) (d) Decrypted of (b) by the CPA

Figure 12. Resistance to CPA.

5.6. Robustness analysis

Encrypted images transmitted over public networks or stored in cloud environments are susceptible to noise interference and information loss, which can reduce decryption accuracy and compromise data integrity. Noise interference is a common distortion in image transmission and storage processes, whereas a cropping attack simulates the partial loss of image regions, which often occurs during data tampering, transmission errors, or storage issues.

Consequently, the proposed image encryption algorithm must demonstrate strong robustness, ensuring that critical information of the plain image is preserved and accurately recovered during decryption under such adverse conditions.

The proposed encryption algorithm's robustness was examined through experiments involving two common attacks scenarios: salt-and-pepper noise and cropping. These tests aim to evaluate the algorithm's ability to maintain confidentiality and accurately recover the original image despite image degradation or partial data loss. Encrypted images were intentionally subjected to simulated salt-and-pepper noise and cropping attacks to mimic real-world disruptions.

The PSNR metric is employed to assess the robustness of the proposed algorithm in preserving image quality under the influence of random noise and data loss. It quantitatively measures the similarity between the plain image and its corresponding decrypted image, and it is mathematically expressed as follows:

$$PSNR = 10 \times log_{10}\left(\frac{255^2}{MSE}\right), \tag{16}$$

$$MSE = \frac{1}{M \times N}\left(\sum_{i=1}^{M}\sum_{j=1}^{N}[P(i,j) - I(i,j)]^2\right), \tag{17}$$

where the $P(i,j)$ and $I(i,j)$ denote the pixel intensities of the plain and the decrypted image, respectively.

Experiment (1): To evaluate the algorithm's performance under noise attack, salt-and-pepper noise with densities of 0.01, 0.02, 0.05, 0.1, and 0.2 were added to the encrypted image. After decrypting the noisy encrypted images using the correct key, the resulting decrypted images were analyzed visually and quantitatively. Figure 13 presents the results of the noise attack experiments, with the

corresponding PSNR values listed in Table 11. The experimental results indicate that, despite the addition of salt-and-pepper noise, the decrypted images maintained high similarity to the original images, as reflected by PSNR values, confirming that the proposed algorithm exhibits strong resilience to such noise interference.

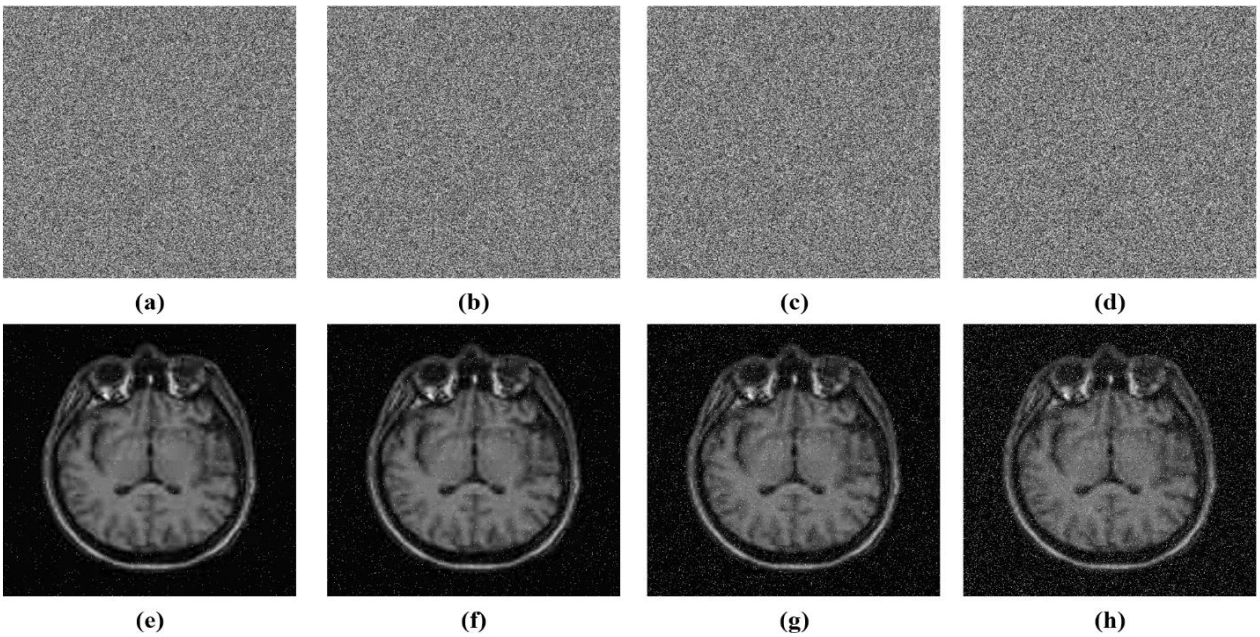


Figure 13. Analysis of salt-and-pepper noise attacks of encrypted images with (a) 0.01, (b) 0.02, (c) 0.05, (d) 0.1, (e), (f), (g), and (h) representing their corresponding decrypted images.

Table 11. PSNR of noise attacks.

	Noise densities			
	0.01	0.02	0.05	0.1
PSNR	26.362	23.372	19.37	16.42

Experiment (2): To test the algorithm's performance under cropping attacks, 10%, 20%, 30%, and 40% of the encrypted image regions were intentionally cropped from different parts of the image. Using the correct key, the cropped encrypted images were decrypted. The results of cropping attacks test are presented in Figure 14, with the corresponding values of PSNR listed in Table 12. The results demonstrate that even under significant cropping (up to 40%), the proposed algorithm preserves a substantial amount of information, allowing the recovery of the plain image structure with high fidelity. Based on the above experiments, the robust analysis indicates that the proposed algorithm effectively preserves image quality under both noise and cropping attacks. This strong resilience makes the algorithm well-suited for secure image transmission in environments prone to noise or data loss.

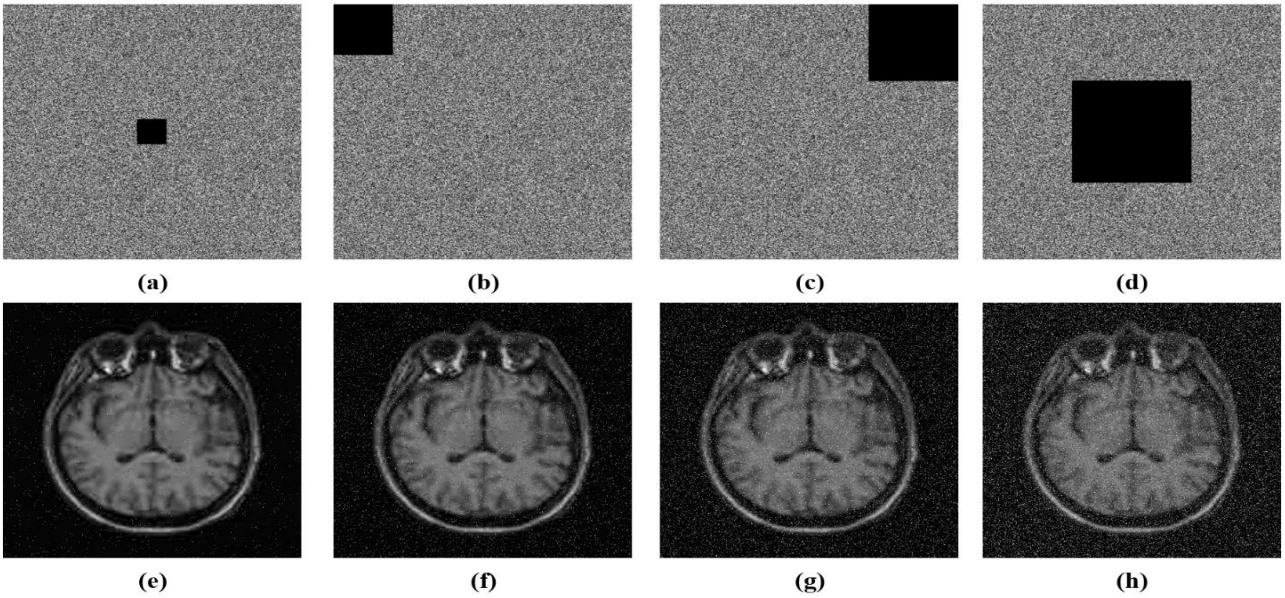


Figure 14. Analysis of cropping attacks: (a–d) encrypted images with 10%, 20%, 30%, and 40% data loss; (e–h) corresponding decrypted images.

Table 12. PSNR of cropping attacks.

	Cropping attack			
	10	20	30	40
PSNR	26.237	20.344	16.822	14.301

Table 13 presents a comparison of the resistance of the suggested algorithm and existing algorithms [33, 35, 39, 44, 46, 52] against noise and cropping attacks by computing the average values of PSNR between the decrypted and plain images. These results indicate that the suggested algorithm achieves higher average PSNR values and demonstrates superior resistance to both cropping and noise attacks compared with the other algorithms.

Table 13. Comaprison of PSNR for noise and cropping attacks.

Image	Density of noise			Cropping attack		
	0.005	0.050	0.100	1/16	1/8	1/4
Proposed	30.4150	20.5200	17.0470	27.8010	24.4270	19.3510
[33]	22.2065	15.4205	12.2691	19.1284	17.5292	13.3681
[35]	21.7520	14.6509	11.8017	18.3674	17.3860	14.2018
[39]	25.6438	16.3401	13.5185	20.8525	17.6628	14.7815
[44]	26.9083	17.3607	14.4562	21.3658	18.8235	15.2258
[46]	29.8960	19.7283	16.6418	24.0680	21.4850	18.7910
[52]	23.7251	16.0358	12.9163	20.0863	17.6143	14.3067

5.7. Complexity and time efficiency analysis

The computational complexity of the suggested image encryption algorithm can be divided into chaotic sequence generation, confusion, and diffusion. Assume that the size of the plaintext image is $M \times N$, $O(4MN)$ is the time complexity for constructing a sequence of length $L = M \times N$, the confusion stage requires time complexity approximately $O(MN)$, and the diffusion stage requires $O(MN)$ for 1D PLSM chaotic sequence generation and the symmetry matrix for all nonoverlapping subblocks of image requires $O(MN/16)$. Therefore, the overall time complexity is $O(4MN) + O(MN) + O(MN) + O(MN/16) \approx O(MN)$, which offers high efficiency and is suitable for encryption. To assess efficiency, the encryption and decryption times were measured by executing the proposed algorithm 30 times on plain images of different sizes. The average execution time is reported in Table 14.

Table 14. Encryption and decryption time.

Image size	Encryption time	Decryption time
256 × 256	0.003528	0.003311
512 × 512	0.011912	0.011176
1024 × 1024	0.045361	0.041761

The results show the efficiency and scalability of the suggested algorithm across varying image sizes, reflecting that the proposed algorithm strikes a balance between computational speed and security. Table 15 provides a comparison of the execution time of the suggested algorithm with existing algorithms, indicating that the execution time of the suggested algorithm is acceptable and that it is more suitable for real-time application scenarios.

Table 15. Time comparison.

Algorithm	Image size		
	256 × 256	512 × 512	1024 × 1024
Proposed	0.0069	0.0232	0.0868
[33]	9.6978	12.5688	23.4659
[44]	0.0052	0.0220	0.1101
[52]	0.9601	4.0758	--

6. Conclusions

In this paper, a new medical image encryption framework was introduced, integrating a fractional-order four-dimensional chaotic system for pixel confusion and a symmetry matrix integrated with a one-dimensional chaotic map for diffusion. The proposed design effectively leverages high-dimensional chaotic dynamics to achieve enhanced randomness, sensitivity to initial conditions, and resilience to common cryptanalytic attacks. Experimental evaluations confirmed the algorithm's strong security metrics, including high entropy, optimal NPCR and UACI values, and negligible correlation between adjacent pixels, all of which demonstrate its robustness and suitability for protecting sensitive medical images in telemedicine environments. Despite its excellent performance, further

improvements can be explored. Future work may focus on optimizing computational efficiency to enable real-time encryption of high-resolution medical datasets and integrating hardware acceleration through GPU or FPGA implementations.

Author contributions

Conceptualization, M.M.D.; methodology, A.S.A and M.M.D.; software, A.S.A and M.M.D.; validation, M.M.D.; formal analysis, A.S.A; investigation, M.M.D.; resources, A.S.A and M.M.D.; data curation, A.S.A and M.M.D.; writing—original draft preparation, A.S.A and M.M.D.; writing—review and editing, A.S.A and M.M.D.; visualization, M.M.D.; project administration, A.S.A.; funding acquisition, A.S.A. All authors have read and agreed to the published version of the manuscript.

Funding

This research was funded by Prince Sattam bin Abdulaziz University, Project No. (PSAU/2025/01/32676).

Acknowledgments

The authors extend their appreciation to Prince Sattam bin Abdulaziz University for funding this research work through the project number (PSAU/2025/01/32676).

Conflict of interest

The authors declare that they have no conflicts of interest.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

References

1. M. Magdy, K. M. Hosny, N. I. Ghali, S. Ghoniemy, Security of medical images for telemedicine: a systematic review, *Multimed. Tools Appl.*, **81** (2022), 25101–25145. https://doi.org/10.1007/s11042-022-11956-7
2. P. T. Akkasaligar, S. Biradar, Selective medical image encryption using DNA cryptography, *Inf. Secur. J. Glob. Perspect.*, **29** (2020), 91–101. https://doi.org/10.1080/19393555.2020.1718248
3. Y. Ding, F. Tan, Z. Qin, M. Cao, K. K. R. Choo, Z. Qin, DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption, *IEEE T. Neur. Net. Lear.*, **33** (2022), 4915–4929. https://doi.org/10.1109/TNNLS.2021.3062754
4. Y. Wu, L. Zhang, S. Berretti, S. Wan, Medical image encryption by content-aware dna computing for secure healthcare, *IEEE T. Ind. Inform.*, **19** (2023), 2089–2098. https://doi.org/10.1109/TII.2022.3194590

5. O. Kocak, U. Erkan, A. Toktas, S. Gao, Pso-based image encryption scheme using modular integrated logistic exponential map, *Expert Syst. Appl.*, **237** (2024), 121452. https://doi.org/10.1016/j.eswa.2023.121452
6. M. Gafsi, N. Abbassi, M. A. Hajjaji, J. Malek, A. Mtibaa, Improved chaos-based cryptosystem for medical image encryption and decryption, *Sci. Program.*, **2020** (2020), 6612390. https://doi.org/10.1155/2020/6612390
7. W. El-Shafai, F. Khallaf, E. S. M. El-Rabaie, F. E. A. El-Samie, Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications, *J. Ambient Intell. Human. Comput.*, **12** (2021), 9007–9035. https://doi.org/10.1007/s12652-020-02597-5
8. F. Masood, M. Driss, W. Boulila, J. Ahmad, S. U. Rehman, S. U. Jan, et al., A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations, *Wireless Pers. Commun.*, **127** (2022), 1405–1432. https://doi.org/10.1007/s11277-021-08584-z
9. S. Gao, Z. Zhang, H. H. C. Iu, S. Ding, J. Mou, U. Erkan, et al., A parallel color image encryption algorithm based on a 2D logistic-rulkov neuron map, *IEEE Internet Things*, **12** (2025), 18115–18124. https://doi.org/10.1109/JIOT.2025.3540097
10. S. Gao, Z. Zhang, Q. Li, S. Ding, H. H. C. Iu, Y. Cao, et al., Encrypt a story: A video segment encryption method based on the discrete sinusoidal memristive rulkov neuron, *IEEE T. Depend. Secure*, **22** (2025), 8011–8024. https://doi.org/10.1109/TDSC.2025.3603570
11. S. Gao, R. Wu, H. H. Iu, U. Erkan, Y. H. Cao, Q. Li, et al., Chaos-based video encryption techniques: A review, *Comput. Sci. Rev.*, **58** (2025), 100816. https://doi.org/10.1016/j.cosrev.2025.100816
12. U. Erkan, F. Toktas, A. Toktas, Q. Lai, S. Zhou, Y. Lin, et al., Multi-layer and multi-directional image encryption algorithm based on hyperchaotic 3D Xin-She Yang map, *Expert Syst. Appl.*, **304** (2026), 130808. https://doi.org/10.1016/j.eswa.2025.130808
13. M. Li, S. Pan, W. Meng, W. Guoyong, Z. Ji, L. Wang, Medical image encryption algorithm based on hyper-chaotic system and DNA coding, *Cogn. Comput. Syst.*, **4** (2022), 378–390. https://doi.org/10.1049/ccs2.12070
14. Z. Man, C. Gao, Y. Dai, X. Meng, Dynamic rotation medical image encryption scheme based on improved Lorenz chaos, *Nonlinear Dyn.*, **112** (2024), 13571–13597. https://doi.org/10.1007/s11071-024-09732-3
15. K. M. Hosny, S. T. Kamal, M. M. Darwish, A novel color image encryption based on fractional shifted Gegenbauer moments and 2D logistic-sine map, *Vis. Comput.*, **39** (2023), 1027–1044. https://doi.org/10.1007/s00371-021-02382-1
16. A. Belazi, M. Talha, S. Kharbech, W. Xiang, Novel medical image encryption scheme based on chaos and DNA encoding, *IEEE Access*, **7** (2019), 36667–36681. https://doi.org/10.1109/ACCESS.2019.2906292
17. S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, C. Wang, et al., Asynchronous updating Boolean network encryption algorithm, *IEEE T. Circ. Syst. Vid.*, **33** (2023), 4388–4400. https://doi.org/10.1109/TCSVT.2023.3237136
18. S. Gao, H. H. C. Iu, U. Erkan, C. Simsek, A. Toktas, Y. Cao, et al., A 3D memristive cubic map with dual discrete memristors: Design, implementation, and application in image encryption, *IEEE T. Circ. Syst. Vid.*, **35** (2025), 7706–7718. https://doi.org/10.1109/TCSVT.2025.3545868

19. K. M. Hosny, S. T. Kamal, M. M. Darwish, Novel encryption for color images using fractional order hyperchaotic system, *J. Ambient. Intell. Human. Comput.*, **13** (2022), 973–988. https://doi.org/10.1007/s12652-021-03675-y
20. T. Li, W. Fan, J. Wu, D. Zhang, Image encryption based on a fractional-order hyperchaotic system and fast row column-level joint permutation and diffusion, *Nonlinear Dyn.*, **112** (2024), 10555–10581. https://doi.org/10.1007/s11071-024-09597-6
21. H. Nabil, H. Tayeb, Exploring chaos and bifurcation in a fractional-order gyrostat system with application to color image encryption, *Comp. Appl. Math.*, **45** (2026), 89. https://doi.org/10.1007/s40314-025-03562-8
22. F. Q. Meng, G. Wu, A color image encryption and decryption scheme based on extended DNA coding and fractional-order 5D hyper-chaotic system, *Expert Syst. Appl.*, **254** (2024), 124413. https://doi.org/10.1016/j.eswa.2024.124413
23. J. Jackson, R. Perumal, A robust image encryption technique based on an improved fractional order chaotic map, *Nonlinear Dyn*., **113** (2025), 7277–7296. https://doi.org/10.1007/s11071-024-10480-7
24. M. A. Barakat, Comprehensive weighted Newton inequalities for broad function classes via generalized proportional fractional operators, *Axioms*, **14** (2025), 234. https://doi.org/10.3390/axioms14040234
25. M. M. Alarady, M. A. Barakat, M. M. Darwish, Fractional modeling and dynamic analysis of COVID-19 transmission with computational simulations, *Mathematics*, **13** (2025), 3619. https://doi.org/10.3390/math13223619
26. A. Abdelaziz, M. M. Darwish, M. A. Barakat, Fractional-order polar harmonic Fourier moments and 1D chaotic mapping for robust zero-watermarking of medical images, *AIMS Math.*, **10** (2025), 30354–30383. https://doi.org/10.3934/math.20251333
27. S. Dua, A. Kumar, M. Dua, D. Dhingra, ICFCM-MIE: improved cosine fractional chaotic map based medical image encryption, *Multimed Tools Appl.*, **83** (2024), 52035–52060. https://doi.org/10.1007/s11042-023-17438-8
28. O. F. Boyraz, E. Guleryuz, A. Akgul, M. Z. Yildiz, H. E. Kiran, J. Ahmad, A novel security and authentication method for infrared medical image with discrete time chaotic systems, *Optik*, **267** (2022), 169717. https://doi.org/10.1016/j. ijleo.2022.169717
29. X. Wang, S. Yin, M. Shafiq, A. A. Laghari, S. Karim, O. Cheikhrouhou, et al., A new V-net convolutional neural network based on four-dimensional hyperchaotic system for medical image encryption, *Secur. Commun. Netw.*, **2022** (2022), 1–14. https://doi.org/10.1155/2022/4260804
30. H. Lin, C. Wang, L. Cui, Y. Sun, X. Zhang, W. Yao, Hyperchaotic memristive ring neural network and application in medical image encryption, *Nonlinear Dyn.*, **110** (2022), 841–855. https://doi.org/10.1007/s11071-022-07630-0
31. B. Zhang, B. Rahmatullah, S. L. Wang, H. M. Almutairi, Y. Xiao, X. Liu, et al., A variable dimensional chaotic map-based medical image encryption algorithm with multi-mode, *Med. Biol. Eng. Comput.*, **61** (2023), 2971–3002. https://doi.org/10.1007/s11517-023-02874-3
32. J. Liu, Y. Ma, S. Li, J. Lian, X. Zhang, A new simple chaotic system and its application in medical image encryption, *Multimed. Tools Appl.*, **77** (2018), 22787–22808. https://doi.org/10.1007/s11042-017-5534-8

33. S.T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, M. M. Fouda, A new image encryption algorithm for grey and color medical images, *IEEE Access*, **9** (2021), 37855–37865. https://doi.org/10.1109/ACCESS.2021.3063237
34. X. Chai, J. Zhang, Z. Gan, Y. Zhang, Medical image encryption algorithm based on Latin square and memristive chaotic system, *Multimed. Tools Appl.*, **78** (2019), 35419–35453. https://doi.org/10.1007/s11042-019-08168-x
35. A. Z. Abbasi, A. Rafiq, L. Kolsi, Parametrization of generalized triangle groups and construction of substitution-box for medical image encryption, *J. King Saud Univ. Com.*, **36** (2024), 102159. https://doi.org/10.1016/j.jksuci.2024.102159
36. Y. Zhang, H. Xie, J. Sun, H. Zhang, An efficient multi-level encryption scheme for stereoscopic medical images based on coupled chaotic system and Otsu threshold segmentation, *Comput. Biol. Med.*, **146** (2022), 105542. https://doi.org/10.1016/j.compbiomed.2022.105542
37. M. Dua, R. Bhogal, Medical image encryption using novel sine-tangent chaotic map, *e-Prime Adv. Electr. Eng. Electron. Energy*, **9** (2024), 100642. https://doi.org/10.1016/j.prime.2024.100642
38. S. Deb, B. Bhuyan, Chaos-based medical image encryption scheme using special nonlinear filtering function based LFSR, *Multimed. Tools Appl.*, **80** (2021), 19803–19826. https://doi.org/10.1007/s11042-020-10308-7
39. Q. Lai, G. Hu, U. Erkan, A. Toktas, High-efficiency medical image encryption method based on 2D Logistic-Gaussian hyperchaotic map, *Appl. Math. Comput.*, **442** (2023), 127738. https://doi.org/10.1016/j.amc.2022.127738
40. J. Bi, S. Yin, H. Li, L. Teng, C. Zhao, Research on medical image encryption method based on improved Krill herb algorithm and chaotic systems, *Int. J. Netw. Secur.*, **22** (2020), 484–489. https://doi.org/10.6633/IJNS.202005
41. A. Gokyildirim, S. Çiçek, H. Calgan, A. Akgul, Fractional-order Sprott K chaotic system and its application to biometric iris image encryption, *Comput. Biol. Med.*, **179** (2024), 108864. https://doi.org/10.1016/j.compbiomed.2024.108864
42. Z. Hua, S. Yi, Y. Zhou, Medical image encryption using high-speed scrambling and pixel adaptive diffusion, *Signal Process.*, **144** (2018), 134–144. https://doi.org/10.1016/j.sigpro.2017.10.004
43. M. Chen, G. Ma, C. Tang, Z. Lei, Generalized optical encryption framework based on shearlets for medical image, *Opt. Lasers Eng.*, **128** (2020), 106026. https://doi.org/10.1016/j.optlaseng.2020.106026
44. J. Jackson, R. Perumal, A robust medical image encryption technique using inverse cosine chaotic map, *Expert Syst. Appl.*, **298** (2026), 129574. https://doi.org/10.1016/j.eswa.2025.129574
45. Z. Zhang, J. Tang, F. Zhang, T. Huang, M. Lu, Medical image encryption based on Josephus scrambling and dynamic cross-diffusion for patient privacy security, *IEEE T. Circ. Syst. Vid.*, **34** (2024), 9250–9263. https://doi.org/10.1109/TCSVT.2024.3394951
46. A. Belazi, A. Mabrouk, A refined sine-derived chaotic map for securing medical image encryption in telemedicine, *Comput. Biol. Med.*, **196** (2025), 110667. https://doi.org/10.1016/j.compbiomed.2025.110667
47. G. Ke, H. Wang, S. Zhou, H. Zhang, Encryption of medical image with most significant bit and high capacity in piecewise linear chaos graphics, *Measurement*, **135** (2019), 385–391. https://doi.org/10.1016/j.measurement.2018.11.074

48. S. A. Banu, R. Amirtharajan, A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach, *Med. Biol. Eng. Comput.*, **58** (2020), 1445–1458, https://doi.org/10.1007/s11517-020-02178-w
49. Q. Lai, H. Hua, Secure medical image encryption scheme for healthcare IoT using novel hyperchaotic map and DNA cubes, *Expert Syst. Appl.*, **264** (2025), 125854. https://doi.org/10.1016/j.eswa. 2024.125854
50. J. Liu, S. Tang, J. Lian, Y. Ma, X. Zhang, A novel fourth order chaotic system and its algorithm for medical image encryption, *Multidim. Syst. Sign. Process.*, **30** (2019), 1637–1657. https://doi.org/10.1007/s11045-018-0622-0
51. Y. Cui, Z. Zheng, Novel fractional-order chaotic system applied to mobile robot path planning and chaotic path synchronization, *Symmetry*, **17** (2025), 350. https://doi.org/10.3390/sym17030350
52. S. Shao, J. Li, P. Shao, G. Xu, Chaotic image encryption using piecewise-logistic-sine map, *IEEE Access*, **11** (2023), 27477–27488. https://doi.org/10.1109/ACCESS.2023. 3257349

AIMS Press