Journal of Engineering and Technology for Industrial Applications

ITEGAM-JETIA

Manaus, v.11 n.52, p. 205-219. March./April., 2025.
DOI: https://doi.org/10.5935/jetia. v11i52.1628

ISSN ONLINE: 2447-0228

RESEARCH ARTICLE OPEN ACCESS

A FAST ENHANCED MEDICAL IMAGE ENCRYPTION SCHEME BASED ON 2D-CHAOTIC MAP AND IMPROVED ZIGZAG CONFUSION

Ammar Bouchemel[1] and Elhadi Mehallel[2], Abdelaziz Rebahi[3]

[1,2] LABCAV advanced control laboratory, Faculty of Science and Technology, Université 8 mai 1945, BP 401, Guelma 24000, Algeria.
[3] Laboratory of Telecommunication and Smart Systems (LTSS), Faculty of Science and Technology University of Djelfa, PO Box 3117, Djelfa 17000 Algeria.

[1]https://orcid.org/0000-0002-2861-4819, [2]https://orcid.org/0000-0001-7488-162X, [3]http://orcid.org/0000-0001-8684-4754

Email: bouchemel.ammar@univ-guelma.dz, e.mehallel@univ-djelfa.dz, abdelaziz.rabehi@univ-djelfa.dz

ARTICLE INFO

Article History
Received: February 09, 2025
Revised: March 20, 2025
Accepted: March 15, 2025
Published: April 30, 2025

Keywords:
Chaotic maps,
Medical image encryption,
Magic diffusion,
2D-LSCM ,
Data security.

ABSTRACT

The rapid growth of telecommunication systems has increased the need for the secure transmission of data images in the telemedicine context, ensuring confidentiality and reliability. Chaotic image cryptography, known for its ergodicity and sensitivity to initial conditions, is a robust solution against attacks on medical data in unsecured networks. This paper introduces a chaotic image encryption scheme utilizing the 2D-logistic sine-coupling map (2D-LSCM) to enhance the reliability and security level of medical encrypted images. 2D-LSCM has been used to generate chaotic matrices for achieving confusion and diffusion processes. In the confusion step, a variety of permutation operations are utilized, such as improved 2D zigzag transform, magic confusion, pixel confusion, and image rotation. We use also a pixel diffusion based on modulo arithmetic. Several simulations were carried out to prove the reliability and robustness of the proposed algorithm in protecting medical images. Additionally, we evaluate the system's performance and security, comparing it to other well-known chaos-based encryption schemes. The results obtained in the simulation demonstrated the high security of the cryptosystem, therefore our system can effectively secure multiple medical image formats and resist different security attacks.

I. INTRODUCTION

In the digital age, medical images, including X-rays, MRIs, CT scans, and ultrasounds, are crucial in diagnosis, treatment planning, and patient monitoring [1]. These images contain sensitive patient information, and their confidentiality is of paramount importance. The rise in cyber threats and unauthorized access to medical data has necessitated the development of robust encryption techniques to protect these images [2-4]. Traditional encryption techniques, such as-Advanced Encryption-Standard (AES) [5] and Data encryption-standard (DES) [6] are not suitable for encrypting image data and unable to ensure data privacy and security [7] due to the images' dimensions, high redundancy and pixel correlation [8],[9]. There have been many approaches for encrypting image data over the last two decades, but chaos-based encryption has proven to be the most successful [10-15].

Chaotic systems are ideal candidates for encryption due to their deterministic randomness**,** meaning they can generate unpredictable sequences that are highly sensitive to initial conditions. Small changes in the initial state of the system result in dramatically different outcomes. This property of chaos [16] is used to scramble the image data in such a way that unauthorized decryption becomes infeasible without the correct parameters and initial conditions. Currently, chaotic systems are widely used for encrypting medical images because of their simplicity, efficiency, and ability to create high-security encryption [17],[18]. Existing chaotic maps are generally classified into two types: one-dimensional (1D) [19],[20] and high-dimensional (HD) [21],[22] maps.

1D chaotic maps have fewer parameters and variables, resulting in a smaller secret key space and lower security [23]. The most commonly used 1D chaotic maps in image encryption is the

logistic, sine, and tent map [24-25]. In contrast, high-dimensional chaotic maps feature more variables and parameters, offer a more complex structure, better chaotic performance, and higher complexity in the transformation process, which makes it more secure compared to 1D chaotic maps.

However, given their performance and implementation costs, 2D chaotic maps are regarded as excellent options for image encryption. In order to generate a chaotic matrix using initial values and parameters as secret keys, several 2D chaotic maps have been recently introduced for image encryption. For example, the 2D sine logistic modulation map (2D-SLMM) [26], 2D logistic-adjusted-sine map (2D-LASM) [27], the two-dimensional Sine infinite collapse modulation map (2D-SIMM) [28], 2D logistic-sine-coupling map (2D-LSCM) [29], Logistic Iterative Chaotic Map modulation map (2D-SLIM), and the 2D logistic-modulated-sine-coupling-logistic map (2D-LSMCL) [30].

However, these chaotic maps share a common limitation: their chaotic trajectories are narrow, unevenly distributed, and lack good ergodicity, making them vulnerable to unauthorized attacks and image information theft. While chaotic image encryption schemes provide greater security than conventional methods, their security depends heavily on the chaotic behavior of the maps used and the algorithm's structure. Researchers have shown that if the chaotic performance is inadequate or the algorithm's structure is not robust, these schemes become vulnerable to security issues and attacks.

Many chaos-based image encryption algorithms have drawbacks related to the chaotic systems used and their encryption structures. To overcome these limitations, this paper introduces a novel chaotic image encryption scheme for medical images, designed to enhance chaotic performance and increase the randomness of encrypted data, providing protection against various statistical attacks and cryptanalysis. This is achieved by utilizing the 2D-Logistic Sine-Coupling Map (2D-LSCM) in the algorithm to generate chaotic sequences, which are the used in confusion and diffusion operations. The 2D-LSCM map is a two-dimensional chaos map that offers a wider chaotic range, improved ergodicity, and greater unpredictability compared to several existing 2D maps [29]. The main contributions of this paper are outlined below.

- A novel fast chaotic image encryption algorithm that uses the 2D-LSCM map to enhance chaotic performance and provide greater security for the encrypted medical image.
- The proposed 2D-LSCM medical image encryption algorithm based on improved 2D zigzag confusion and two-level of magic confusion and pixel diffusion.
- Security analysis tests such as key sensitivity analysis, differential analysis, Shannon's entropy, local Shannon's entropy and contrast tests are conducted to validate the proposed scheme's resistance to various attacks.
- The Experimental results of these tests are compared with other prominent chaotic encryption schemes to highlight the improvements achieved by the proposed scheme.

The remainder of the paper is structured as follows: In Section 2, we present a review of existing research on medical image encryption algorithms based on chaotic systems. The 2D-LSCM and its chaotic performance evolution are presented in Section 3. Section 4 develops a new medical image encryption scheme based on 2D-LSCM. The simulation results and security performance of our scheme and its comparisons with several other image encryption algorithms are presented in Section 5. Section 6 provides the conclusion of this paper.

II. RELATED WORKS

Medical image encryption is a critical area of research, given the sensitive nature of medical data and the increasing reliance on digital imaging in healthcare. Chaotic maps are widely used for encryption due to their inherent properties of sensitivity to initial conditions, randomness, and low computational overhead. Currently, various technologies have been implemented in the field of medical image encryption. Below is an overview of the current state of the art with references from recent works.

In [31] developed a novel chaos-based medical image encryption scheme using a sine-cosine chaotic map. Their method involves generating a pseudorandom key and constructing a cipher image through a three-phase process. Its proposed chaotic map exhibited a wider chaotic range and more complex behavior compared to existing maps, enhancing encryption robustness.

In [32] introduced a medical image encryption scheme-based on Josephus traversing and a hyperchaotic Lorenz system. The algorithm employs a hyperchaotic sequence in both scrambling and diffusion stages, utilizing Josephus and Arnold maps for confusion. Experimental results indicated effective hiding of plaintext image information and resistance to common attack types. Another medical image encryption algorithm that utilizes a variable dimensional chaotic map was proposed by in 2023 [33]. Their method features full and semi-full encryption modes, utilizing a confusion-diffusion structure with image integrity verification to balance security and time efficiency.

For [34] proposed a medical image encryption scheme-based on an improved cosine fractional chaotic map combined with DNA operations. The scheme involves generating intermediate keys and chaotic sequences, followed by DNA encoding and diffusion. Security performances such as NPCR, UACI, and information entropy indicated the scheme's robustness.

In the same context, [35] presented an encryption method that integrates wavelet transform with multiple chaotic maps. Utilizing Lorenz and logistic maps for chaotic key generation, the scheme demonstrated high security, low time complexity, and resistance against crop attacks. According to [36] developed a medical image encryption algorithm based on a new five-dimensional multi-band multi-wing chaotic system and QR decomposition. The method utilizes QR decomposition and chaotic sequences for encryption, demonstrating a large key space, strong key sensitivity, and effective resistance to statistical analysis attacks.

According to. [37] developed a fast image encryption system-based on chaotic cryptography. Their approach utilized a hybrid chaotic magic transform (HCMT) to generate the encrypted image from a secret key. By employing the HCMT, which combines the Lanczos algorithm with the chaotic magic transform (CMT), they achieved a correlation coefficient of 0.0012. This result surpassed the performance of the CMT method by [26], which had a correlation coefficient of 0.042. In [38] present a novel chaotic encryption scheme for medical images that combines Arnold’s Cat Map with 2D-LSCM, offering improved security level and time complexity over other existing methods.

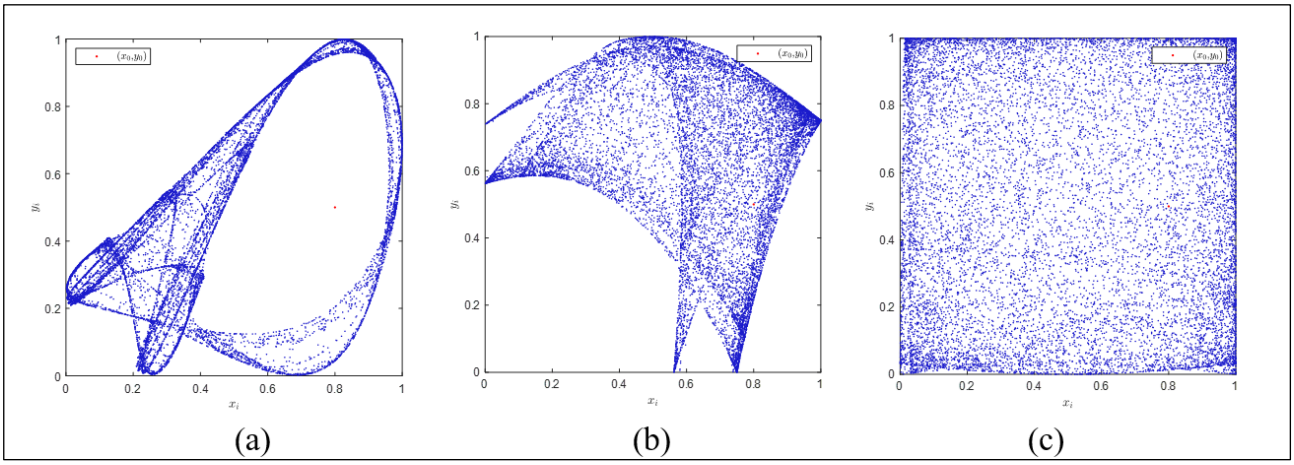


Figure 1:Trajectories of three 2D chaotic maps: (a) the 2D Logistic map with $\boldsymbol{r = 1.19}$; (b) the 2D-LSCM with $\boldsymbol{\alpha}$ = 1; (c) the 2D-LSCM with $\boldsymbol{\theta}$ = 0.99.
Source: Authors, (2025).

III. CHAOTIC MAPS

III.1 LOGISTIC MAP

The Logistic map is a simple yet well-known chaotic system [39], described by the iterative equation (1)

$$x_{i+1} = r(1 - x_i) \tag{1}$$

where x_i is the state variable at the i-th iteration, while $x_i \in [0,1]$, and $r \in [1,4]$ is a parameter that controls the dynamic system.

III.2 LOGISTIC MAP

The Sine map is another 1D chaotic map defined as [40]:

$$x_{i+1} = \alpha sin(\pi x_i) \tag{2}$$

where $x_i \in [0,1]$ is the state variable at the i-th iteration, and $\alpha \in [0,1]$ is a parameter that controls the dynamic map.

III.3 SINE MAP

The two-dimensional logistic-sine-coupling map (2D-LSCM) represents a significant advancement in chaotic systems, especially in the context of image encryption [29]. This discrete chaotic map is created by combining features from both the Logistic map and the Sine map, which enhances its chaotic proprieties and randomness.

The traditional one-dimensional Logistic and Sine maps have certain limitations, including simplistic dynamics and low chaotic ranges, which can negatively impact some chaos-based applications [26]. However, by combining the Logistic and Sine maps, a new chaotic map with significantly more complex behavior and large chaotic range, known as the 2D-LSCM, can be created. This map is defined as [29].

$$\begin{cases} x_{i+1} = sin\left(\pi\left(4\theta x_i(1 - x_i) + (1 - \theta)sin(\pi y_i)\right)\right) \\ y_{i+1} = sin\left(\pi\left(4\theta y_i(1 - y_i) + (1 - \theta)sin(\pi x_{i+1})\right)\right) \end{cases} \tag{3}$$

Where the control parameter θ is within the range of $[0,1]$. Its definition makes clear that this combination allows to extend the dimension from 1D to 2D. As a result, this approach allows for the effective integration of the complexities of the Logistic and Sine maps, resulting in highly intricate chaotic behavior.

Figure 1 illustrates the trajectories of the 2D-logistic map (2D-LM) [41], 2D-sine logistic modulation map (2D-SLMM) [26], and the 2D-LSCM. To generate the trajectories of this three 2D maps, the initial conditions were set as $(0.8, 0.5)$ and the control parameters are chosen as the settings that enable the corresponding chaotic maps to achieve their optimal chaotic performance. In particular, the control parameters for the 2D Logistic map, 2D-SLMM, and 2D-LSCM are set to 1.19, 1, and 0.99, respectively. As shown in the figure, the phase space covered by the 2D-LSCM trajectory is significantly larger compared to the Logistic map and 2D-LSCM. This demonstrates that the randomness exhibited by the 2D-LSCM map is high, making them suitable for secure cryptographic applications.

IV. 2D-LSCM-BASED MEDICAL IMAGE ENCRYPTION ALGORITHM

In this section, we design the 2D-LSCM-based medical image encryption algorithm using 2D-LSCM, and its structure is illustrated in Figure 2. First, the plaintext image P is the original image and the cipher image C is the encrypted image. The secret key is used to generate initial values and control parameters for 2D-LSCM map. In the proposed scheme, we used a 2D-LSCM map to generate the chaotic matrices for confusion and diffusion operations. The confusion and diffusion operations are used to randomly shuffle pixel positions, and change pixel values of the plaintext image, respectively.

Zigzag confusion and magic confusion are used to achieve the confusion property by randomly shuffling all pixel positions. The image rotation operation involves rotating the image clockwise by 90° for a high-efficiency scrambling. The pixel diffusion operation is used to achieve the diffusion property by randomly changing all pixel values. To obtain random-like encryption results while avoiding the cases that 2D-LSCM may lose its chaotic behaviors in some parameter settings the proposed image encryption algorithm uses two steps of magic confusion and pixel diffusion operations. The decryption process simply reverses the encryption operations of image encryption algorithm, as shown in Figure 2. The proposed algorithm for medical image encryption is detailed as follows:

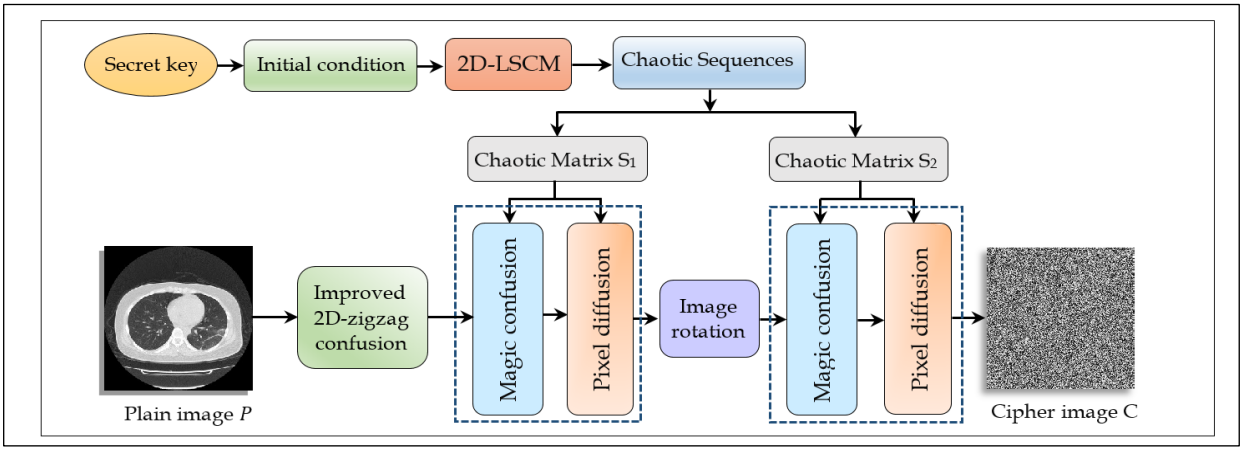


Figure 2: Block diagram of the proposed image encryption Method.
Source: Authors, (2025).

Algorithm 1: The proposed medical image encryption scheme
Input: The secret key $K = (x_0, y_0, \theta, H, G_1, G_2)$ and the original image P with dimensions $M \times N$.

1-Transform the binary sequences x_0, y_0, α, H into decimal numbers, and G_1, G_2 into integers ;
2-Obtain two groups of initial conditions $(x_0^1, y_0^1, \theta_1)$and (x_0^2, y_0^2, θ_2);
3-Generate two chaotic matrices S_1 and S_2 with the same size of P using 2D-LSCM with two groups of initial conditions in Step 2;
4-Apply zigzag confusion to the plaintext image P;
5-Apply magic confusion using the chaotic matrix S_1;
6-Apply pixel diffusion using the chaotic matrix S_1;
7-Image rotation;
8-Apply magic confusion using the chaotic matrix S_2;
9-Apply pixel diffusion using the chaotic matrix S_2;
Output: The encrypted image C

IV.1 INITIAL CONDITION GENERATION

The secret key K a binary sequence with a length of 256 bits which is used to generate the chaotic matrix. Its structure is shown in Figure 3. It contains information of initial values and control parameters of 2D-LSCM and can be divided into 6 parts: x_0, y_0, θ, H, G_1 and G_2 are initial values and θ is control parameter. H, G_1 and G_2 are designed to change the initial values and parameters to enlarge the security key space. x_0 , $y_0, \alpha,$ and H are decimal numbers which are generated by a 52-bit string $\{b_0, b_1, \ldots\ldots, b_{52}\}$ using the IEEE 754 format [41],[42], as shown in Equation 4.

$$x = \frac{1}{2^{52}} \sum_{i=1}^{52} b_i \, 2^{52-i} \tag{4}$$

G_1 and G_2 are two integer coefficients generated by a 24-bit string $\{b_0, b_1, \ldots\ldots, b_{24}\}$.

x_0	y_0	θ	H	G_1	G_2
52bits	52 bits	52bits	52 bits	24bits	24 bits

Figure 3: The security key structure.
Source: Authors, (2025).

The equation 5 defines the initial values and control parameters of 2D-LSCM chaotic map for generating two chaotic matrices, which can be effectively employed in our algorithms to perform confusion and diffusion operations.

$$\begin{cases} x_0^{(i)} = (x_0 + G_i H) \bmod 1 \\ y_0^{(i)} = (y_0 + G_i H) \bmod 1 \\ \theta_i = (\theta + G_i H) \bmod 0.1 \end{cases} \tag{5}$$

Where the phase number i is equal to 1 or 2. In Equation 5, the two generated initial values will fall into the range of $[0, 1]$, and the control parameter θ will be limited within $[0, 1]$. As a result, we can use the initial value (x_0^i, y_0^i, and θ_i) to generate a sufficiently long chaotic matrices, whose length equals the size of the original image P using the Equation 3.

In such a way, we make encryption key K to generate two initial states and control the two pseudo-random matrices produced from the 2D-LSCM for pixel confusion, magic confusion, and pixel diffusion in each phase. Therefore, the 2D-LSCM demonstrates strong chaotic performance with these settings. In our medical image encryption algorithm, users can either manually choose a 256-bit binary sequence or randomly generate a binary stream to create the security key. In our simulations and comparisons, we generate random 256-bit binary streams as the security keys, which are provided along with the encrypted results for image decryption.

In our medical image encryption algorithm, the users have the flexibility of manually selecting a binary sequence with 256 bits or randomly generating a binary stream to produce the security key. In our simulations and comparisons, we randomly generate binary streams with a length of 256 bits as the security keys that will be returned along with the encrypted results for image decryption.

IV.2 IMPROVED 2D ZIGZAG CONFUSION

The 2D zigzag scan [43] was generally employed to scramble the pixel positions of medical images. This operation can effectively disrupt the high correlation between adjacent pixels. The process began with the first pixel of the medical image matrix, and subsequent pixels were traversed in a 2D zigzag pattern [44]. This traversal transformed the two-dimensional matrix into a one-dimensional sequence, as illustrated in Figure 4.

In this section, we present a new scrambling algorithm inspired by the zigzag transform. The concept of the improved 2D

zigzag confusion is detailed in algorithm 3, with a numerical example provided in Figure. 4. The detailed zigzag confusion procedure is as follows:

For the pixel located in the i-th row and j-th column of the original image, its value is represented by $P(i,j)$. The corresponding index for this pixel is calculated as $(M-j)\times N+i$, denoted as $I(i,j)$. The typical zigzag transformation technique involves starting from one corner of the matrix array $I(i,j)$, moving along the diagonal to its end, scanning all elements parallel to the diagonal to form a one-dimensional vector, and then reconstructing the vector based on predetermined rules.

Algorithm 3: Improved 2D zigzag confusion

Input: the original image P with dimensions $M \times N$.

1-Apply zigzag transform to the plaintext image P, obtain two-dimensional array I and corresponding one-dimensional index array I_V ;

2-Reshape the matrix P into a vector array P_V;

3-for $i = 1$ to $M \times N$ do

4- $P_{1V} = P_V(I_V(i))$;

5-end for

6-Reshape the vector P_{1V} into a matrix array P_2

Output: Zigzag confusion result P_2.

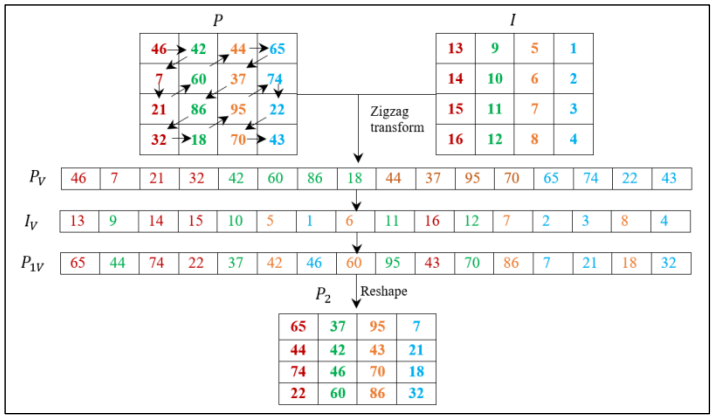


Figure 4: A numerical example of the improved 2D zigzag confusion.
Source: Authors, (2025).

IV.3 MAGIC CONFUSION

Digital images typically exhibit high information redundancy due to the strong correlations between neighboring pixels. To disrupt these correlations, this section proposes employing a magic confusion method based on a chaotic matrix to randomly alter the positions of image pixels.

The shuffling procedure using magic confusion based chaotic magic confusion can be detailed as follows [26]:

- **Step 1**: the original image P and chaotic matrix S with the same size of $M \times N$, which is generated using the 2D-LSCM with the initial state;
- **Step 2**: Sort each column of S in ascending order to obtain the sorted matrix $\acute{S}$ and its corresponding index matrix O. The generation of the index matrix O from a chaotic matrix S is then defined as follows
- $$O(i,j) = k \qquad for \quad \acute{S}(i,j) = S(i,j) \tag{6}$$

where i, j, and k are integers, $1 \le i,k \le M$ and $1 \le j \le N$

- **Step 3**: Set row index $i = 1$;
- **Step 4**: Connect the pixels in P with positions $\{(P_{i,1},1),(P_{i,2},2),(P_{i,3},3),\dots,(P_{i,N},N)\}$ using the locations $\{(O_{i,1},1),(O_{i,2},2),(I_{i,3},3),\dots,(I_{i,N},N)\}$ into a circle;
- **Step 5**: Shift these pixels i positions to the left;
- **Step 6**: Iterate Step 3 to Step 6 up to $i = M$, we can obtain the magic confusion result T.

To clarify the process of magic confusion using 2D-LSCM, an illustrative numerical example with an image size of 4×4 is provided, as illustrated in Figure 5.

The magic confusion procedure have the ability to modify the pixel positions in the original image P based on the chaotic matrices S_1 et S_2 produced by 2D-LSCM. It randomly links pixels from different rows and columns into circular groups and then shifts their positions within these circles.

IV.4 IMAGE ROTATION

As mentioned in the previous section, the scrambling process only rearranges the $L^2 \times L^2$ portion of the image, leaving the remaining pixels with strong correlations between them. To ensure that all the pixels in the image are shuffled during encryption, image rotation is introduced as another operation of scrambling. This is achieved by rotating the image by 90° in the anticlockwise direction. The rotation angle of the image does not significantly affect the final encryption parameter values, so the image can be rotated by any random angle. The primary purpose of rotation is to displace the image pixels from their original positions. In the decryption step, the scrambled image is rotated clockwise to reverse these changes and restore the pixels to their original positions. Therefore, this operation not only shifts the pixel positions but also changes their spatial arrangement, making it more difficult to reverse-engineer the image.

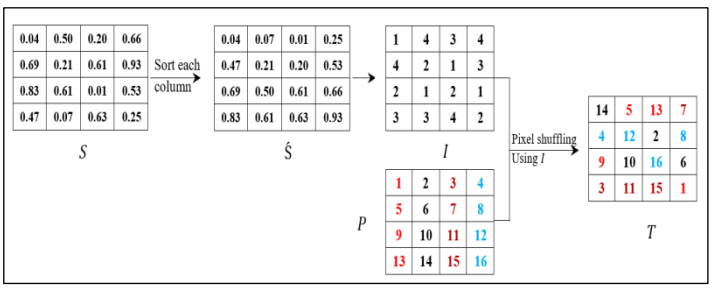


Figure 5: An example of the pixel shuffling processes using magic confusion.
Source: Authors, (2025).

IV.5 PIXEL DIFFUSION

An encryption algorithm with good diffusion properties can effectively resist chosen plaintext attacks. Diffusion property ensures that even a minor difference between two plaintexts, when encrypted with the same key, produces completely different cipher images. This process spreads small changes in the plain image across all pixels in the cipher image. It involves altering the current pixel based on the previous pixel and a randomly generated value. To perform the diffusion operation, Let the scrambling result matrix T and the generated chaotic matrix S both have dimensions of $M \times N$. Then, the pixel diffusion result is defined by the mathematical eq. (7) [45].

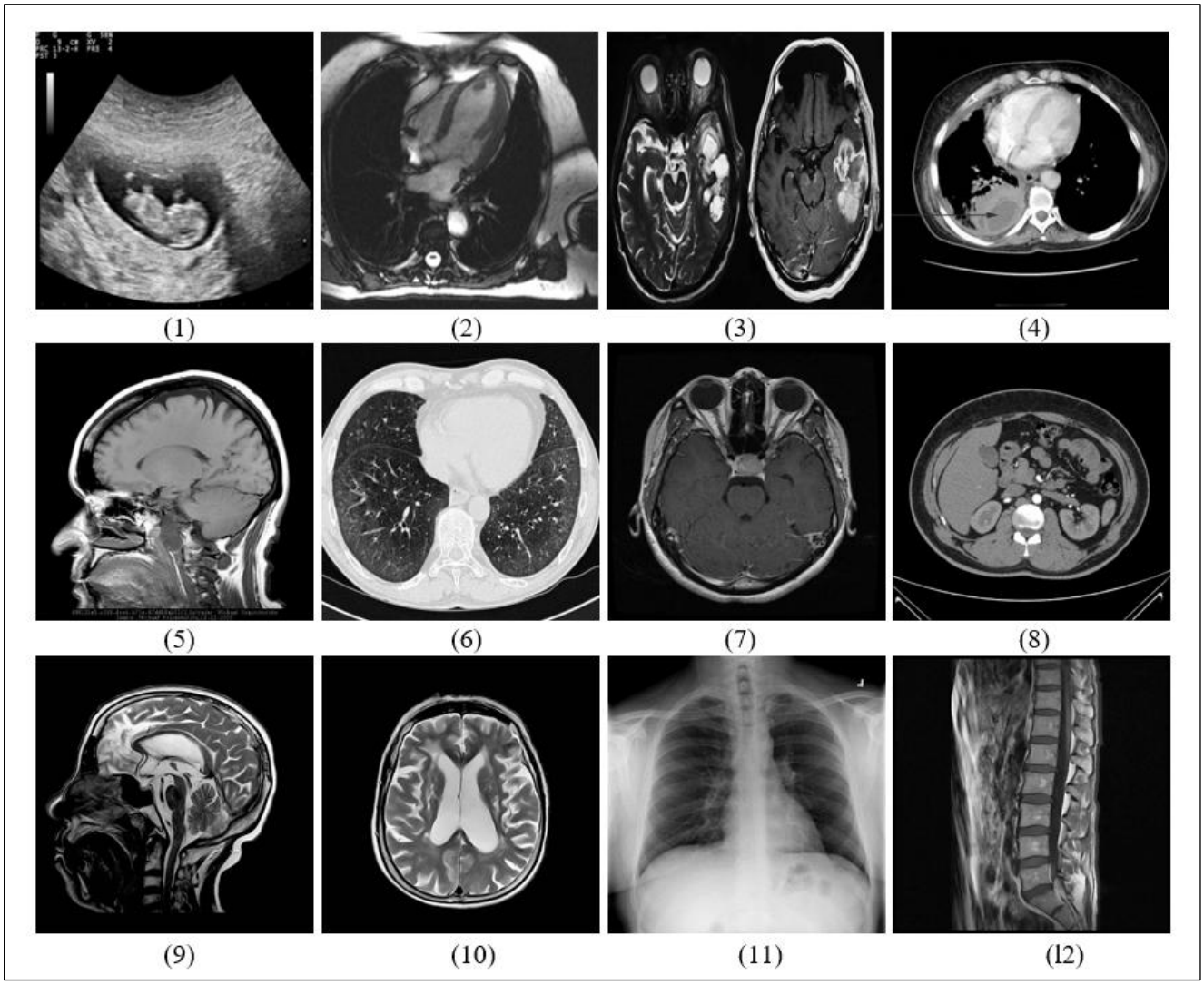


Figure 6: Examples of medical images used to test the proposed algorithm.
Source: Authors, (2025).

$$C_{i,j} = \begin{cases} (T_{i,j} + T_{M,N} + S_{i,j}) \mod \mathrm{F}, & \text{if } i = 1, j = 1 \\ (T_{i,j} + T_{M,j-1} + S_{i,j}) \mod \mathrm{F}, & \text{if } i = 1, j = 1 \sim N \\ (T_{i,j} + T_{i-1,j} + S_{i,j}) \mod \mathrm{F}, & \text{if } i = 1 \sim M \end{cases} \quad (7)$$

where F denotes the number of intensity levels, e.g. $F = 256$ if a pixel is represented by 8 bits. S is a chaotic matrix generated by 2D-LSCM with the initial state $(x_0^i\, y_0^i, \theta_i)$ ($i = 1$ in the first phase and $i = 2$ in the second phase). It has the same size and its elements are represented as the same data format as the pixels in T. In the decryption process, the inverse operation of Eq. (7) is defined as

$$T_{i,j} = \begin{cases} (C_{i,j} - T_{M,N} - S_{i,j}) \mod \mathrm{F}, & \text{if } i = 1, j = 1 \\ (C_{i,j} - C_{M,j-1} - S_{i,j}) \mod \mathrm{F}, & \text{if } i = 1, j = 1 \sim N \\ (C_{i,j} - C_{i-1,j} - S_{i,j}) \mod \mathrm{F}, & \text{if } i = 1 \sim M \end{cases} \quad (8)$$

V. SIMULATION RESULTS AND SECURITY ANALYSIS

This section simulates the proposed medical image encryption algorithm based on 2D-LSCM map and evaluates its performance under the MATLAB implementation. A variety of medical images, including MRI, X-ray, CT, and ultrasound images, successfully encrypted using our algorithm. The majority of test medical images used in our experiments are chosen from the Open Access Open-I images dataset (https://openi.nlm.nih.gov). For simplicity, we use twelve images, displayed in Figure 6, as examples for our experiments and security analysis. In Figure 6, the images in (1)-(4) have dimensions of 256 × 256, the images in (5)-(8) have dimensions of 512 × 512, but the size of the last four images is 1024 × 1024.

V.1 COMPUTATION TIME ANALYSIS

In this section, we assess the encryption and decryption times of the developed image encryption algorithm and compare its execution times with those of four recent schemes. All the algorithms, including the developed one, are implemented in the MATLAB environment (R2021b), and the experiments are conducted on a computer with an Intel i5-7300U CPU @ 2.60GHz, 8 GB of RAM, and the Windows 10 operating system. Table 1 presents a comparison of the encryption and decryption times of various image encryption algorithms for different image sizes. The simulation results indicate that our proposed algorithm outperforms the others in terms of total computation time. Furthermore, our encryption algorithm not only offers better security but also executes faster than the other advanced image encryption schemes.

Table 1: Comparison of encryption and decryption times for different encryption algorithms.

Test image	Size of the image	Computation Time (second)				
		Ref. [26]	Ref. [23]	Ref. [29]	Ref. [38]	Our
Image 3	256 × 256	2.12	4.21	1.75	1.38	1.66
Image 5	512 × 512	3.97	13.73	2.71	2.30	2.23
Image 9	1024×1024	8.24	102.64	4.76	5.91	4.35

Source: Authors, (2025).

V.2 SECURITY KEY ANALYSIS

Evaluating performance metrics is essential for assessing the effectiveness and security of medical image encryption techniques. Various key indicators are typically used to evaluate these algorithms, such as the key space and key sensitivity. However, the users are flexible to choose any other settings by considering the tradeoff between the security level and computation cost.

V.2.1 SECURITY KEY SPACE

One of the typical fundamental elements used to evaluate encryption algorithms is key space, which refers to the total number of possible keys that can be generated for an encryption algorithm. A substantial key space is crucial for protection against brute-force attacks, making it a cornerstone of effective encryption systems. Generally, a key space exceeding 2^{100} is required to ensure sufficient defense against such threats [46]. In theory, a larger key space enhances the algorithm's security. The proposed medical image encryption algorithm uses a security key of 256 bits, resulting in a key space of 2^{256}. This key space is large enough to withstand brute-force attacks, given the computational power of current computers.

V.2.2 KEY SENSITIVITY ANALYSIS

Another important metric that is used to evaluate encryption algorithms is key sensitivity, which measures how responsive the encryption algorithm is to changes in initial conditions or keys. In chaotic systems, even minor variations can lead to dramatically different results, ensuring that each encrypted image remains unique and secure. This characteristic helps to undermine potential attacks that rely on predictability. However, the secret key should exhibit sensitivity during both the encryption and decryption processes. This means that a single-bit difference between two secret keys will lead to completely different cipher-images during encryption and result in totally different decrypted images during the decryption process.

Figures 7 display the key sensitivity analysis for the encryption and decryption processes, respectively. K_2 and K_3 are two secret keys derived from K_1 with one bit difference. As shown in Figure 7, when the plain-image is encrypted using K_2, and K_3, the resulting cipher-images are completely different as shown in Figure 7(b) and 7(c). Figure 7(e) illustrates that the cipher-image can only be fully reconstructed with the correct secret key, and even a small difference in the secret keys produces entirely different decrypted images, as seen in Figure 7(f) and 7(g). Therefore, our medical image encryption algorithm is highly sensitive to changes in its secret key in both the encryption and decryption processes.

V.3 STATISTICAL ANALYSIS

In this section, we evaluate the resistance of our medical image encryption scheme to statistical attacks by examining four aspects: histogram, correlation, information entropy, and local Shannon entropy. This section presents several experiments to demonstrate the reliability of our proposed algorithm.

V.3.1 HISTOGRAM ANALYSIS

Histogram analysis is used to evaluate how effectively the algorithm randomizes pixel values within encrypted images. An ideal histogram should display a uniform distribution across pixel intensity values, indicating successful scrambling of the image data while preventing any leakage of information about the original content. The histograms of the original images and their corresponding encrypted images are shown in Figure 8. The results clearly indicate that the encrypted images exhibit a much more uniform distribution compared to the original images, indicating a high resistance to statistical attacks.

V.3.2 INFORMATION ENTROPY ANALYSIS

The randomness of the pixels in the encrypted image is a crucial factor in ensuring the security of the encryption scheme. This randomness can be effectively measured using Local Shannon Entropy [47], calculated using the formula provided in Eq. (9).

$$H(x) = -\sum_{i=0}^{2^n-1} Pr(x_i)\, log_2 Pr(x_i) \tag{9}$$

Here, $Pr(x_i)$ is the probability of a specific symbol x, and n denotes the number of bits in a pixel.

For an encrypted image to be secure against attacks, its pixel distribution must be completely uniform. When the pixel distribution of an n-bit image is fully uniform, the entropy of the image equals n. In this study, as we are working with 8-bit images, the objective is to achieve entropy values close to 8, ensuring a uniform pixel distribution and maximizing security [47].

Table 2. shows the information entropy values of twelve medical images with different sizes encrypted by several image encryption algorithms. As shown in Table 4, our encryption scheme achieves a mean entropy value of 7.998884, which is closer to 8 compared to other schemes used in comparison, indicating superior performance. These result indicates that the proposed scheme can encrypt images into cipher-images with good randomness.

V.3.3 LOCAL SHANNON ENTROPY

Global Shannon entropy, discussed in the previous subsection as information entropy, has certain limitations such as inaccuracy, inconsistency, and low efficiency [47]. To address these issues, the local Shannon entropy (LSE) has been introduced, which can provide a precise characterization of the randomness in image pixels. For a data image I, we divide the image I into k non-overlapping sub-image blocks $S_1, S_2, \ldots, S_k$, each sub-image block containing T_B pixels. Then, the LSE is defined as:

$$H_{k,T_B}(I) = -\sum_{i=0}^{k} \frac{H(S_i)}{k} \tag{10}$$

Here $H(S_i)$ represents the Shannon entropy of image block S_i.

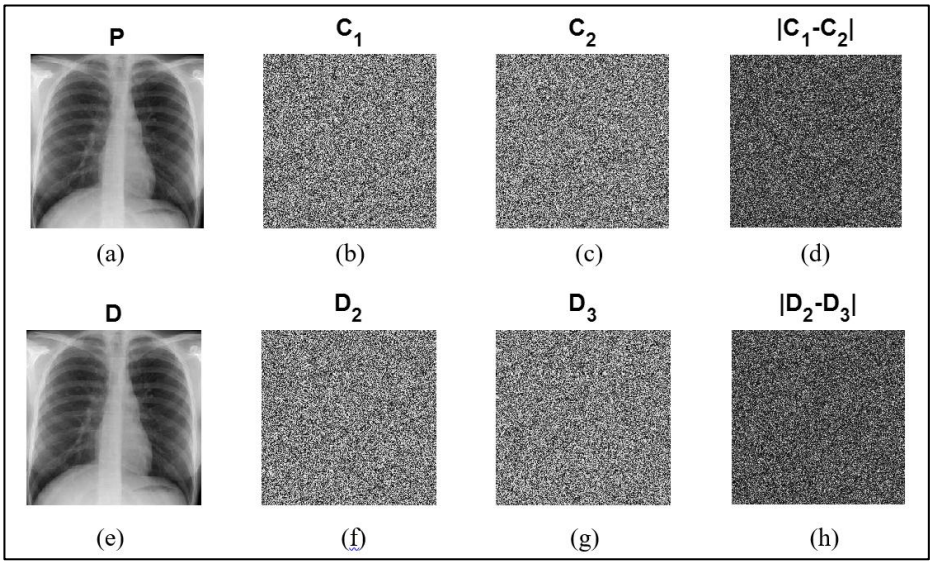


Figure 7: Key sensitivity analysis. (a) Plaintext image $\boldsymbol{P}$; (b) ciphertext image $\boldsymbol{C_1}$, (c) ciphertext image $\boldsymbol{C_2}$; (d) difference of ciphertext images: $|\boldsymbol{C_1} - \boldsymbol{C_2}|$; (e) decrypted image $\boldsymbol{D_1}$, (f) decrypted image $\boldsymbol{D_2}$, (g) decrypted image $\boldsymbol{D_3}$ and (h) difference of decrypted images: $|\boldsymbol{D_2} - \boldsymbol{D_3}|$.
Source: Authors, (2025).

In our experiment, we certain medical images from the OPEN-I image dataset for simulation to validate the robustness of our scheme. To enable comparisons with other encryption algorithms and following the recommendation in [47], we set the parameters $k = 30$, and $T_B = 1936$ with a significance level of $\alpha = 0.05$ [48-50]. Under these settings, the ideal LSE value is 7.902469317, and LSE test is considered successful if the score for a ciphered image falls between 7.901901305 and 7.903037329 [47].

Table 3 presents the LSE results, showing that the pass rate of our algorithm is 12/12, which is notably higher compared to 8/12 [26], 7/12 [23], and 8/12 [29], and 10/12 [38]. Additionally, the average LSE value for ciphered images generated by our algorithm is 7.902467, with a standard deviation of 0.000349. These results indicate that the average LSE value from our proposed scheme is very close to the theoretical value of 7.902469317, with the smallest standard deviation among the compared methods. Therefore, our scheme demonstrates superior security. This means that the encrypted images by our scheme have better random distributions. This suggests increased unpredictability in pixel values, enhancing security against statistical attacks.

V.3.4 PIXEL CORRELATION ANALYSIS

Correlation reflects the linear relationship between two random variables and is used to measure the relationship between adjacent pixels in image processing. In plain-images, the pixels tend to have a high correlation with their neighboring pixels in all direction. Therefore, it is important to ensure that the correlation between adjacent pixels is low enough to prevent recognition in horizontal, vertical, or diagonal directions. Therefore, the image encryption algorithm aims at breaking these pixel correlations in the original images and transforming them into noise-like encrypted images with little or no correlations. Generally, having a correlation coefficient close to 0 is one of the important performance indicators of an excellent encryption scheme. The values of the correlation coefficient can be calculated by

$$C_{xy} = \frac{cov(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{11}$$

where

$$cov(x,y) = \frac{1}{N}\sum_{i=0}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big) \tag{12}$$

and

$$D(x) = \frac{1}{N}\sum_{i=0}^{N}\big(x_i - E(x)\big)^2 \quad , \quad E(x) = \frac{1}{N}\sum_{i=0}^{N} x_i \tag{13}$$

where x_i and y_i present the adjacent pixels, $D(.)$ is variance of corresponding pixels, $E[.]$ is the expectation value. If two sequences x and y have high correlations, their correlation value is close to 1. Otherwise, it is close to 0.

In our test, we randomly select 2000 pairs of neighbor pixels from original and encrypted images and we analyses correlation from adjacent pixels along with the horizontal, vertical and diagonal directions. Figure 9 plots the distributions of the pixel sequence pairs, X and Y of the original image and its encrypted version generated by the proposed algorithm. As shown in Figure 9, the horizontal axis represents the concentration of randomly selected pixels, while the vertical axis shows the intensity of their corresponding neighboring pixels. In the original image, the neighboring pixel pairs are distributed or near the diagonal line, indicating that the pixels are similar or nearly identical, reflecting a strong correlation between adjacent pixels. In contrast, the neighboring pixel pairs of the encrypted image are distributed randomly across the entire data range, demonstrating an extremely low correlation in the encrypted image.

Table 5 compares correlations of the original images with its encrypted versions generated by the proposed medical image encryption algorithm. The results of the original image are close to 1 while the ciphertext image's results are close to 0. These further verify that the encrypted image by the medical image encryption algorithm has an extremely low correlation. The results indicate that this can effectively eliminate the correlation between neighboring pixels in an input image.

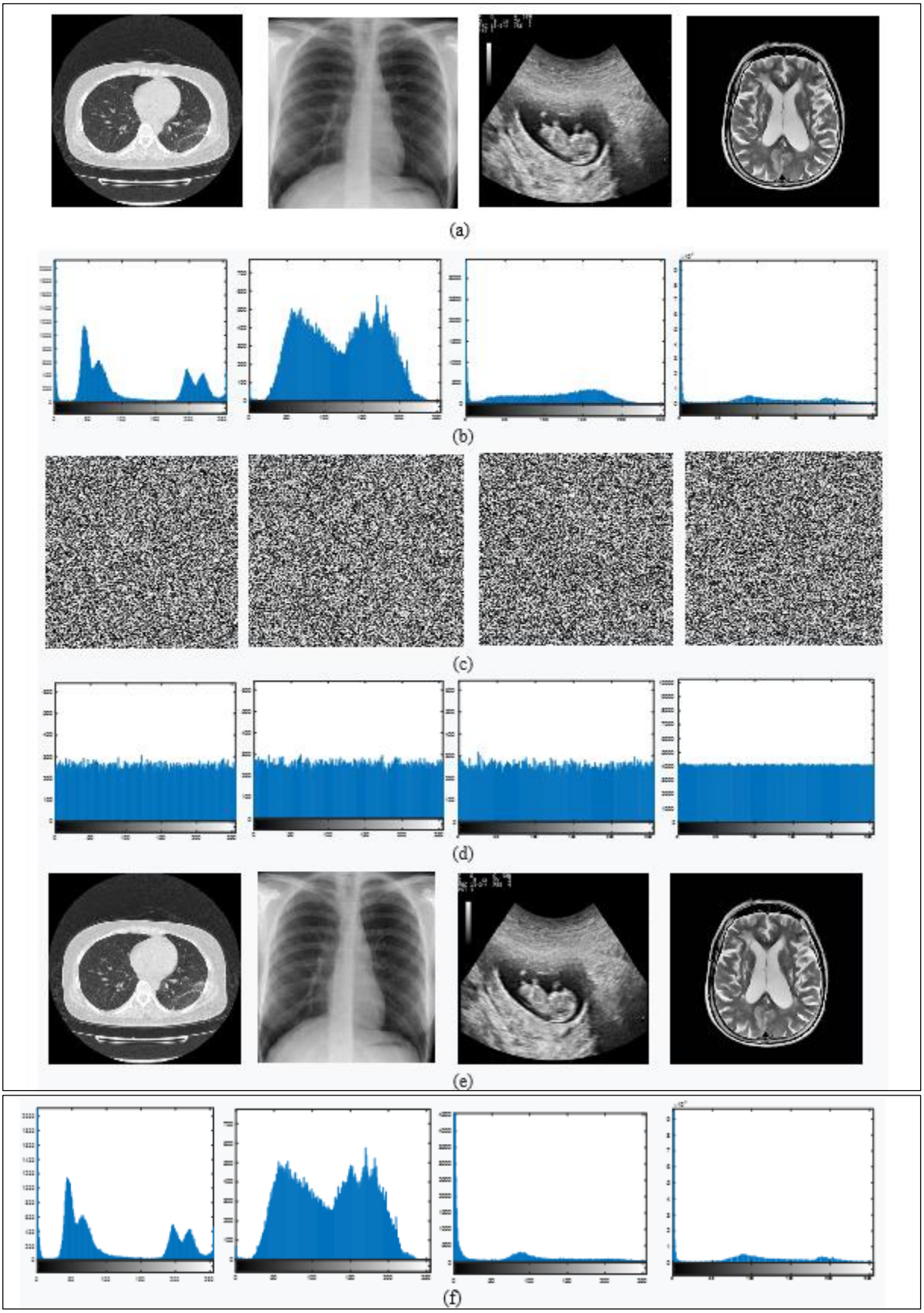
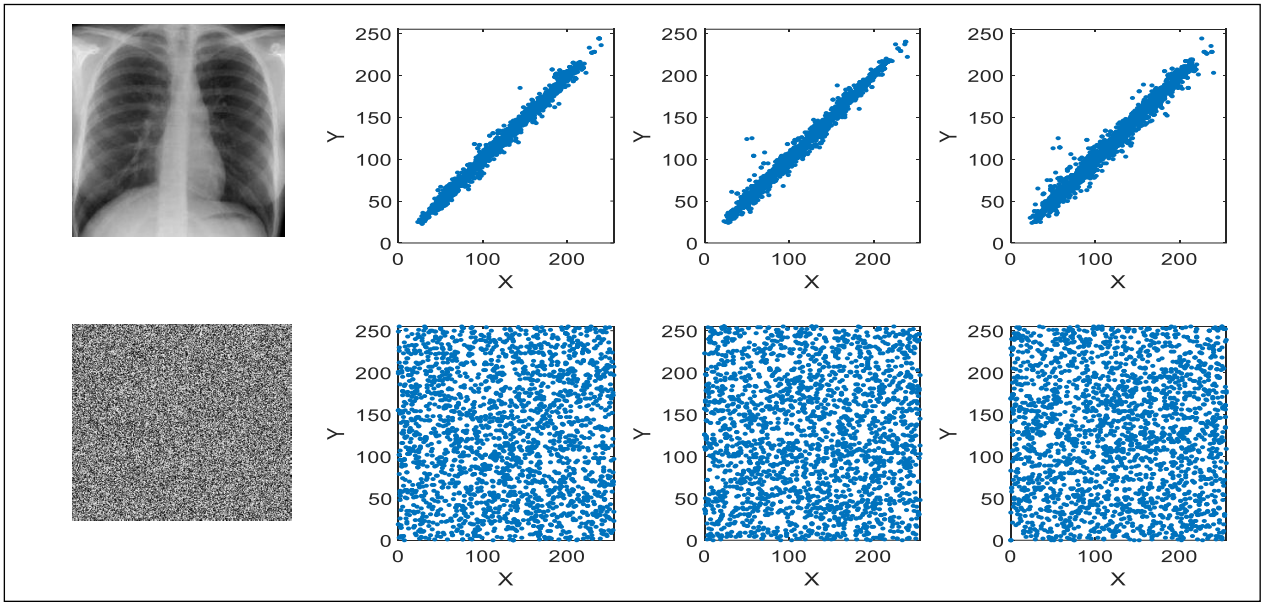


Figure 8: Simulation result of histogram analysis of some images. (a) The original images; (b) the histogram of (a); (c) the encrypted images; (d) the histogram of (c); (e) the decrypted images; (f) the histogram of (e).
Source: Authors, (2025).



(a) (b) (c) (d)

Figure 9: Distributions of adjacent pixel sequence pairs of (a) the plain-image and its cipher-image along with the (b) horizontal, (c) vertical, and (d) diagonal directions, respectively.
Source: Authors, (2025).

Table 2: Comparison of information entropy values for various encrypted images.

Test image	**Size of the image**	**Original image**	**Encrypted image**				
			Ref. [26]	Ref. [23]	Ref. [29]	Ref. [38]	Our algorithm
Image 1	256 × 256	6.018538	7.997298	7.997468	7.997207	7.997504	7.997500
Image 2		6.670125	7.997163	7.997241	7.997547	7.997385	7.997445
Image 3		6.864571	7.997214	7.997274	7.997055	7.997355	7.997390
Image 4		4.867913	7.997508	7.997061	7.997466	7.997128	7.997567
Image 5	512 × 512	5.529474	7.999429	7.999382	7.999297	7.999220	7.999316
Image 6		7.249175	7.999301	7.999299	7.999320	7.999284	7.999372
Image 7		6.033099	7.999357	7.999328	7.999305	7.999392	7.999304
Image 8		4.467764	7.999296	7.999407	7.999296	7.999300	7.999325
Image 9	1024 × 1024	4.613337	7.999819	7.999796	7.999843	7.999821	7.999849
Image 10		4.046626	7.999826	7.999820	7.999806	7.999846	7.999854
Image 11		7.677182	7.999846	7.999824	7.999815	7.999841	7.999849
Image 12		6.342696	7.999819	7.999815	7.999858	7.999817	7.999845
Mean		5.86504167	7.998823	7.9988091	7.9988179	7.9988244	7.9988846
Std		1.17006255	0.0011497	0.0011639	0.001136	0.001121	0.001064

Source: Authors, (2025).

Table 3: The LSE scores of cipher-images encrypted by different image encryption schemes.

Test image	**Size of the image**	**LSE values of encrypted images**				
		Ref. [26]	Ref. [23]	Ref. [29]	Ref. [39]	Our algorithm
Image 1	256 × 256	7.902104	7.903087	7.902114	7.902997	7.902732
Image 2		7.902343	7.900276	7.901377	7.902443	7.902637
Image 3		7.901306	7.900218	7.902113	7.902936	7.902304
Image 4		7.904267	7.900625	7.902801	7.901417	7.901921
Image 5	512 × 512	7.902099	7.902357	7.905825	7.899788	7.902898
Image 6		7.902596	7.901037	7.901908	7.902434	7.902831
Image 7		7.902716	7.902308	7.905475	7.901833	7.902070
Image 8		7.899989	7.901197	7.902024	7.902961	7.902322
Image 9	1024 × 1024	7.903846	7.901467	7.900868	7.902690	7.902111
Image 10		7.902185	7.902204	7.901187	7.902942	7.902432
Image 11		7.901439	7.903602	7.902529	7.903084	7.902351
Image 12		7.902638	7.902749	7.903081	7.902112	7.902998
Mean		7.902294	7.901760	7.902608	7.902303	7.902467
Std		0.0011199	0.0011192	0.001558	0.000948	0.0003495
Pass/All		8/12	7/12	8/12	10/12	12/12

Source: Authors, (2025).

Table 4: Correlation coefficients for various encrypted images.

Test image	Size of the image	Original image			Encrypted image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Image 1	256 × 256	0.979429	0.978050	0.961882	-0.022281	0.015536	0.035114
Image 2		0.980633	0.974735	0.957295	0.000035	0.007166	-0.037567
Image 3		0.885755	0.953481	0.853835	-0.003321	0.004171	-0.003195
Image 4		0.971358	0.966191	0.934692	-0.000554	0.000274	0.005378
Image 5	512 × 512	0.986619	0.985892	0.973654	-0.009633	0.001169	-0.001427
Image 6		0.987208	0.986487	0.974914	-0.009005	0.009597	0.007787
Image 7		0.987514	0.984080	0.970312	0.004144	0.021803	-0.001043
Image 8		0.968627	0.948725	0.940331	0.005555	0.004621	0.007703
Image 9	1024 × 1024	0.992121	0.993768	0.983130	-0.024726	0.028376	-0.009513
Image 10		0.992848	0.996047	0.989666	0.040142	-0.012564	0.013787
Image 11		0.998847	0.999121	0.998515	-0.001969	0.004487	-0.001418
Image 12		0.995155	0.998722	0.994371	-0.006361	0.009663	0.004471
Mean		0.97717617	0.98044158	0.9610498	-0.002331	0.0078583	0.0016731

Source: Authors, (2025).

Table 5: Comparison of correlation values of encrypted images for various algorithms.

Test image	Size of the image	Direction	Encrypted image				
			Ref. [26]	Ref. [23]	Ref. [29]	Ref. [38]	Our algorithm
Image 3	256 × 256	Horizontal	-0.005232	-0.021848	0.025001	-0.038534	0.000035
		Vertical	0.003435	-0.002923	-0.028009	0.005827	0.007494
		Diagonal	-0.030729	0.014174	-0.001203	0.003749	-0.003195
Image 5	512 × 512	Horizontal	-0.000637	0.028980	0.006032	-0.004001	-0.009661
		Vertical	0.011822	-0.015811	0.004157	-0.013116	-0.045108
		Diagonal	-0.016458	0.013305	0.012856	0.033941	-0.008454
Image 9	1024 × 1024	Horizontal	0.020733	0.027330	0.021507	-0.003379	0.000213
		Vertical	0.009093	0.006693	-0.024616	0.009539	-0.000159
		Diagonal	-0.031264	0.017534	-0.009884	0.036621	-0.009210
Mean			-0.00436	0.0074927	0.000649	0.0034052	0.000276

Source: Authors, (2025).

V.4 RESISTANCE TO DIFFERENTIAL ATTACK

The differential attacks analyze how variations in plaintexts influence the corresponding ciphertexts. For an image encryption algorithm, its resistance to such attacks can be evaluated quantitatively using the Number of Pixel Change Rate (NPCR) and the Unified Average Change Intensity (UACI) metrics. NPCR quantifies the number of differing pixels between two images, while UACI measures the intensity of pixel value differences between the two images. Let C_1 and C_2 represent two cipher-images encrypted from plain-images that differ by only one bit. The NPCR and UACI are defined as follows:

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=0}^{M} \sum_{j=0}^{N} D(i,j) \times 100(\%) \tag{14}$$

and

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{C_1(i,j) - C_2(i,j)}{2^l - 1} \times 100(\%) \tag{15}$$

Here, M and N denote the width and height of the image, respectively, while l represents the number of binary bits per pixel. D represents the difference between C_1 and C_2 , defined as

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \tag{17}$$

The theoretical values of NPCR and UACI is recorded as 99.6094% and 33.4635%, respectively [51].

The NPCR and UACI test results of various medical images for different encryption algorithms are shown in Table 6. It can see from the Table 6 that our scheme achieves high performance by having NPCR values no less than 99.5810 % and UACI values no less than 33.461%. Moreover, we can see that our medical image encryption scheme achieves excellent NPCR and UACI results with a mean score of 99.6085% for NPCR and 33.5665% for UACI, which are close to ideal values. Thus, we can conclude that the proposed scheme is well resistant to differential attacks.

V.5 ROBUSTNESS TO RESIST DATA LOSS AND NOISE ATTACKS

When a digital image is transmitted through networks or stored in the physical media, it is easily contaminated by noise or may have the data loss. An image encryption algorithm should have the robustness to resist noise and the data loss. In the proposed algorithm, the encryption and decryption processes are asymmetric. In the encryption process, one pixel change in the plaintext image will spread over all pixels in the ciphertext image. However, in the decryption procedure, the change of one pixel in the ciphertext image can affect only a few pixels in the recovered result. Thus, the proposed medical image algorithm can decrypt the ciphertext image with noise or data loss.

In the first experiment, we simulate a scenario where medical images are illegally intercepted during transmission and subjected to varying degrees of data loss. Specifically, we examine four cases where 1/16, 1/8, 1/4, and 1/2 of the encrypted medical image 5 are obscured. Figure 10(a) illustrates the encrypted medical images and its corresponding decrypted images, while Figures 10(b)-(d) the encrypted images with 1/16 loss, 1/8 loss, 1/4 loss, and the corresponding restored images using the correct keys.

It is evident that even with minor data loss, useful information about the original image cannot be reconstructed from the decrypted output. This indicates that even if the correct key is compromised and an intruder intercepts most of the encrypted data, the details of the original image remain unrecoverable.

In the second experiment, it is assumed a scenario where images are subjected to varying kinds of noises during transmission. Salt-and-pepper noise with a value of density equal 0.01, Gaussian, and speckle noises with a value of variance equal 0.01 are added to the encrypted medical image no 5. The noisy encrypted images are then decrypted, and the resulting outputs are displayed in Figures 11. It is observed that for encrypted images affected by noise, the decrypted output remains unrecognizable, even when the correct decryption key is used.

Table 6: The NPCR and UACI results of various images for different encryption algorithms.

Test image	Ref. [26]		Ref. [23]		Ref. [29]		Ref. [38]		Proposed algorithm	
	NPCR	UACI	NPCR	UACI	NPCR	NPCR	NPCR	UACI	NPCR	UACI
Image 1	99.6749	33.6001	99.5971	33.5059	99.6093	99.6093	99.5907	33.2772	99.6093	33.4908
Image 2	99.6139	33.5385	99.6475	33.4780	99.6078	99.6078	99.6134	33.5133	99.6078	33.4949
Image 3	99.6215	33.6963	99.6109	33.5487	99.6368	99.6368	99.6310	33.8715	99.6109	33.4151
Image 4	99.5788	33.5234	99.6475	33.3194	99.6139	99.6139	99.5884	33.6033	99.6032	33.4612
Image 5	99.5006	32.4290	99.6101	33.4249	99.6147	99.6147	99.6190	33.4522	99.6147	33.4802
Image 6	99.6181	33.5518	99.6150	33.4572	99.6177	99.6177	99.6252	33.4834	99.6177	33.4744
Image 7	99.6089	33.4472	99.6208	33.4043	99.6143	99.6143	99.5950	33.5015	99.6017	33.4655
Image 8	99.3354	31.6879	99.5895	33.4856	99.6231	99.6231	99.6081	33.5255	99.6059	33.5032
Image 9	99.6091	33.5007	99.6216	33.4638	99.6109	99.6109	99.5800	33.4434	99.6093	33.4654
Image 10	99.6100	33.4661	99.6106	33.4939	99.6061	99.6061	99.6108	33.4589	99.6057	33.4757
Image 11	99.5988	33.4693	99.6031	33.4310	99.6090	99.6090	99.6045	33.4361	99.6090	33.4676
Image 12	99.6081	33.4562	99.6169	33.4510	99.6210	99.6210	99.5180	33.3290	99.5810	33.4838
Mean	99.5815	33.2805	99.6158	33.4553	99.6150	33.5086	99.5986	33.4912	99.6063	33.4731
Std	0.08694	0.59641	0.01746	0.05790	0.01293	0.06059	0.02967	0.14740	0.00914	0.02240

Source: Authors, (2025).

Table 7: Comparison of PSNR values for various schemes under different noise conditions

Schemes	Variance	PSNR [dB]		
		Gaussian noise	Salt and pepper noise	Speckle noise
Ref. [26]	0.001	29.5764	54.1853	30.7218
Ref. [29]		29.2577	29.0399	28.6587
Our scheme		31.4438	54.1853	29.0134
Ref. [26]	0.005	29.2858	40.3832	31.8049
Ref. [29]		29.0933	29.2161	29.0665
Our scheme		31.6086	48.1647	30.9632

Source: Authors, (2025).

Table 7 presents a comparison of PSNR values for different image encryption schemes under different noise conditions when the grayscale medical image 4 of size 512 x 512 is used as a test image. Despite the image after encryption being affected by various kinds of noise with a variance value equal to 0.001, the decrypted images manage to retain much of the original image information. Experimental results validate the efficacy of the encryption algorithm, demonstrating its resilience against various kinds of attacks while providing robust encryption. This indicates that our proposed scheme is effective against noise attacks. Therefore, our method not only demonstrates strong resistance to data loss and noise attacks but also exhibits robust performance overall.

VI. CONCLUSIONS

Telemedicine facilitates remote monitoring, diagnosis, and first-aid administration, offering cost-effective healthcare solutions, but the transmission of high-resolution medical images through public networks raises concerns about data security. Traditional encryption methods like DES and AES are insufficient for digital image encryption, leading to the development of chaos-based encryption schemes as a promising alternative to secure image transmission and storage. This paper utilizes the 2D-LSCM chaotic map, derived from Sine and Logistic maps, to generate security keys for encryption and decryption. The 2D-LSCM is chosen for its wider chaotic range, better ergodicity, hyperchaotic properties, and superior chaotic performance compared to existing maps. To demonstrate the performance of 2D-LSCM in medical data security applications, a new fast medical image encryption algorithm is designed. This algorithm is essentially based on improved 2D zigzag confusion, magic confusion, and pixel diffusion. The confusion operations can rapidly shuffle adjacent pixels in an image in both the row and column directions, and the latter can achieve the diffusion property by spreading a few original image changes over the entire encrypted image. Simulation results confirm that our scheme efficiently encrypts various medical images into unrecognizable encrypted images with high security and low run time, outperforming some advanced encryption algorithms. Given its high efficiency and security level, future research will explore its application in other media data such as video encryption.

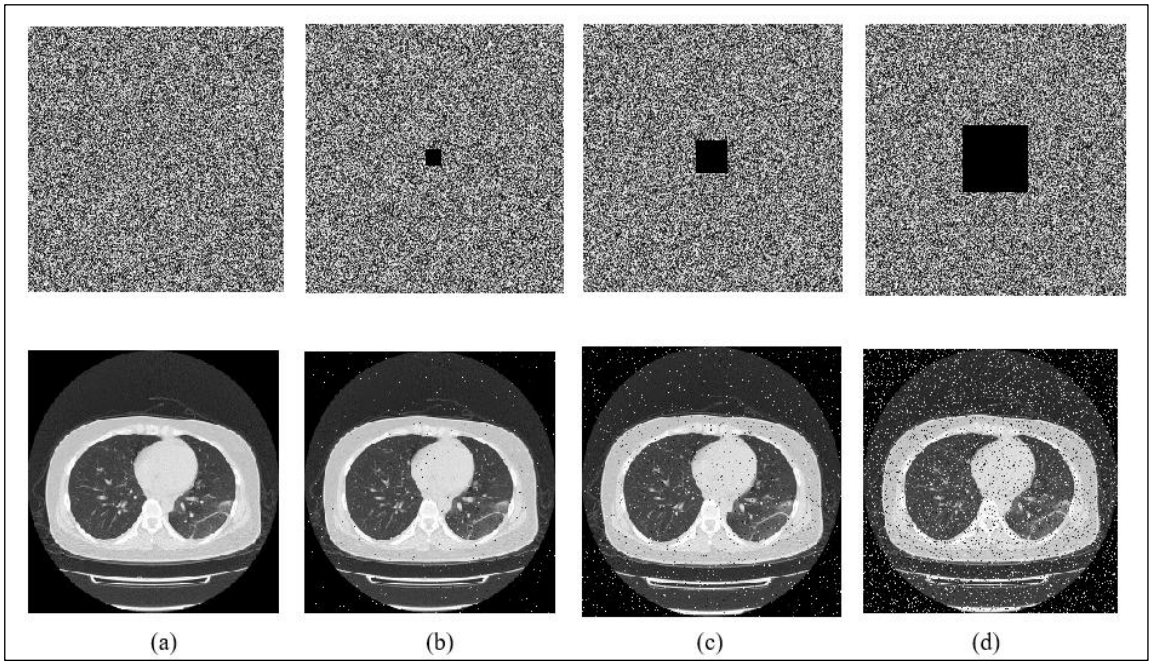


Figure 10: Robustness results to loss data attack. (a) The encrypted original image and its decrypted image; (b)-(d) the encrypted images with 1/16 loss, 1/8 loss, 1/4 loss, and the corresponding restored images.
Source: Authors, (2025).

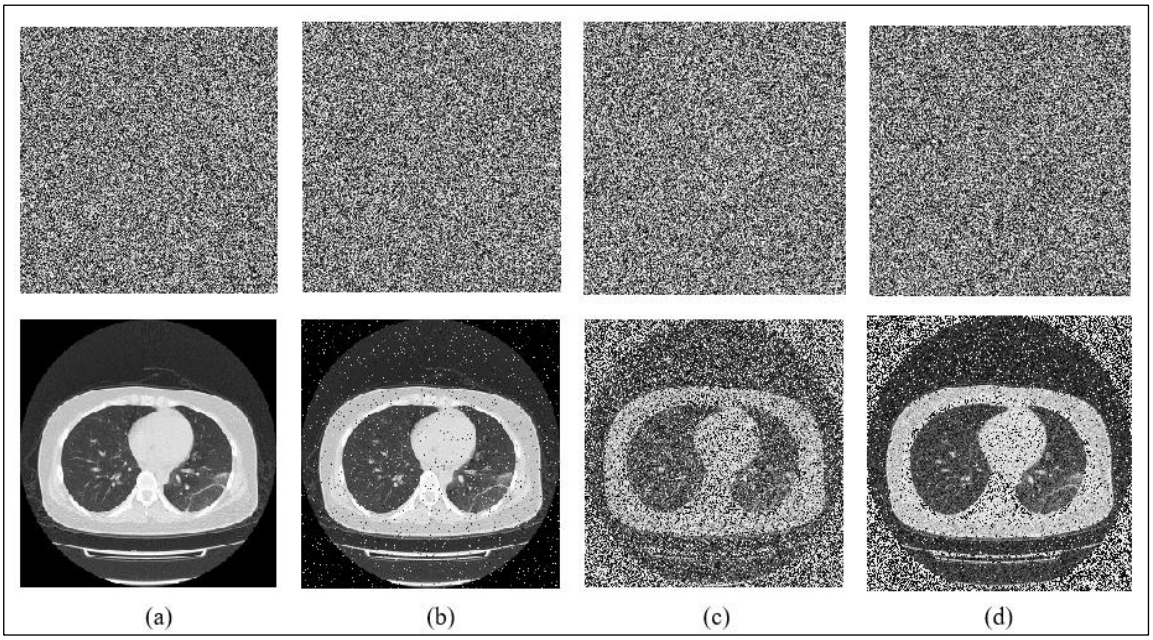


Figure 11: Robustness results to noise attack. (a) The encrypted original image and its decrypted image; (b)-(d) the encrypted images with 1% salt and pepper, 1% Gaussian noise, 1% speckle noise, and the corresponding restored images.
Source: Authors, (2025).

VII. AUTHOR'S CONTRIBUTION

Conceptualization: Author One, Author Two and Author Three.
Methodology: Author One and Author Two.
Investigation: Author One and Author Two.
Discussion of results: Author One, Author Two and Author Three.
Writing – Original Draft: Author One.
Writing – Review and Editing: Author One and Author Two.
Resources: Author Two.
Supervision: Author Two and Author Three.
Approval of the final text: Author One, Author Two and Author Three.

VIII. REFERENCES

[1]. Kiran, Parameshachari B D, Panduranga H T, Naveenkumar S K. "Partial encryption of medical images by dual DNA addition using DNA encoding", Recent Innovations in Signal processing and Embedded Systems, pp.310–314, 2017.

[2]. J., Ali, M.K., Jamil, R. Ali, et al. "Extended fractional transformation-based S-box and applications in medical image encryption", Multimed Tools Appl, pp.1-17, (2025). https://doi.org/10.1007/s11042-024-20575-3.

[3]. A. Roy, D. R. Mahanta, and L. B. Mahanta, "A Semi-Synchronous Federated Learning Framework with Chaos-Based Encryption for Enhanced Security in Medical Image Sharing", Results in Engineering, 103886, 2025

[4]. X. Wang, and Y. Wang, “Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd-even interleaved points”, Expert Systems with Applications, vol.213, Article 118924, 2023.

[5]. F. Pub, Data encryption standard (des), FIPS PUB (1999) 43–46.

[6]. V. Rijmen, J. Daemen, Advanced encryption standard, in: Proceedings of Federal Information Pro

[7]. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28(4):656–715

[8]. A., Jolfaei, and A. Mirghadri, “An image encryption approach using chaos and stream cipher”, Journal of Theoretical and Applied Information Technology, vol.19, no.2, pp.117-125, 2010.

[9]. X. Wang, L. Teng, X. Qin, “A novel colour image encryption algorithm based on chaos”, Signal Processing, vol.92, no.4, pp.1101-1108, 2012.

[10]. Coppersmith Don. “The Data Encryption Standard (DES) and its strength against attacks”, IBM Journal of Research and Development, 1994.

[11]. S. Das, “Medical Image Encryption Using 3D Unified Chaotic System and Dynamic DNA Coding”, 2022.

[12]. M. Zia, B. McCartney, J. Scotney, Martinez, M. AbuTair, J. Memon and A. Sajjad. “Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains”, Aug 2022.

[13]. S. Sun. “A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling”, (accessed Dec 24, 2024). [Online]. Available: https://ieeexplore.ieee.org/document/8320365/

[14]. S. Inam, S. Kanwal, R. Firdous and F. Hajjej. “Blockchain based medical image encryption using Arnold's cat map in a cloud environment”, Mar 2024. [Online]. Available: https://www.nature.com/articles/s41598-024-56364-z

[15]. C. İnce, K. İnce and D. Hanbay. “Novel image pixel scrambling technique for efficient color image encryption in resource-constrained IoT devices". Sep 2024. [Online].

[16]. hang, B.; Liu, L. “Chaos-Based Image Encryption: Review, Application, and Challenges”, Mathematics 2023, vol.11, pp.2585, 2023.

[17]. H. Li, S. Yu, W. Feng, Y. Chen, J. Zhang, Z. Qin, Z. Zhu and M. Wozniak. “Exploiting Dynamic Vector-Level Operations and a 2D-Enhanced Logistic Modular Map for Efficient Chaotic Image Encryption”, Jul 2023.

[18]. R., Tamayo-Pérez, U. J., ... & E. Inzunza-González, “Real-time medical image encryption for H-IoT applications using improved sequences from chaotic maps”, Integration, vol.90, pp.131-145, 2023.

[19]. Z. Hua, Y. Zhou, and H. Huang, “Cosine-transform-based chaotic system for image encryption,” Information Sciences, vol. 480, pp. 403–419, 2019.

[20]. J. Tang, F. Zhang, and H. Ni, “A novel fast image encryption scheme based on a new one-dimensional compound sine chaotic system”, The Visual Computer, vol.39, no.10, pp.4955-4983, 2023.

[21]. B. Zhang, B. Rahmatullah, S. L. Wang, and Z.Liu, “A plain-image correlative semi-selective medical image encryption algorithm using enhanced 2D-logistic map”, Multimedia Tools and Applications, vol.82, no.10, pp.15735–15762, 2023.

[22]. Z. Hua, Z. Wu, Y. Zhang, H. Bao and Y. Zhou, “Two-Dimensional Cyclic Chaotic System for Noise-Reduced OFDM-DCSK Communication,” in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 72, no. 1, pp. 323-336, Jan. 2025.

[23]. L. Xu, et al., “A novel bit-level image encryption algorithm based on chaotic maps”, Optics and Lasers in Engineering vol.78, pp.17–25, 2016.

[24]. Fang, P., Liu, H., Wu, C., Liu, M.: “A survey of image encryption algorithms based on chaotic system”, Vis. Comput. (2022). https:// doi.org/10.1007/s00371-022-02459-5

[25]. M. Alawida, A. Samsudin, J.S. Teh, R.S. Alkhawaldeh, “A new hybrid digital chaotic system with applications in image encryption”, Signal Process. vol.160, pp.45–58 (2019). https://doi.org/10.1016/j. sigpro.2019.02.016.

[26]. Z. Hua, Y. Zhou, C.M. Pun, C.L.P. Chen, “2D Sine Logistic modulation map for image encryption”, Inf. Sci. Vol.297, pp.80–94, 2015.

[27]. Z. Hua, Y. Zhou, “Image encryption using 2D Logistic-adjusted-Sine map, Inf. Sci. vol.339, pp.237–253, 2016.

[28]. W. Liu, K. Sun, and C. Zhu, “A fast image encryption algorithm based on chaotic map,” Optics and Lasers in Engineering”, vol. 84, pp. 26–36, 2016.

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

[30]. H. Zhu, Y. Zhao, Y. Song, “2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption”, IEEE Access, vol.7, pp.14081–14098, 2019.

[31]. A. Kumar, and M. Dua, “A novel chaos map based medical image encryption scheme”, The Imaging Science Journal, vol.69, no.(5–8), pp:219–238, 2021.

[32]. N. Yang, S. Zhang, M. Bai, et al. “Medical Image Encryption Based on Josephus Traversing and Hyperchaotic Lorenz System”, J. Shanghai Jiaotong Univ. (Sci.) vol.29, pp.91–108, 2024. https://doi.org/10.1007/s12204-022-2555-x.

[33]. B. Zhang, B. Rahmatullah, S.L. Wang, et al. “A variable dimensional chaotic map-based medical image encryption algorithm with multi-mode”, Med Biol Eng Comput vol.61, pp. 2971–3002, 2023. https://doi.org/10.1007/s11517-023-02874-3

[34]. K. Demla, and A. Anand, “MieWC: Medical image encryption using wavelet transform and multiple chaotic maps”, Security and Privacy, vol.7, no.3, e369, 2024

[35]. S. Dua, A. Kumar, M. Dua, et al. ICFCM-MIE: “Improved Cosine Fractional Chaotic Map based Medical Image Encryption”, Multimed Tools Appl. Vol.83, pp. 52035–52060, 2024. https://doi.org/10.1007/s11042-023-17438-8

[36]. Z. Zhuang, Z. Zhuang, and T. Wang, “Medical image encryption algorithm based on a new five-dimensional multi-band multi-wing chaotic system and QR decomposition”, Sci Rep vol.14, pp. 402, 2024.

[37]. S. Koppu, V. M. Viswanatham, “A fast enhanced secure image chaotic cryptosystem based on hybrid chaotic magic transform”, Modell Simul Eng. Vol.1, pp. 7470204, 2017. https://doi.org/10.1155/2017/7470204.

[38]. K. Jain, A. Aji, and P. Krishnan, “Medical image encryption scheme using multiple chaotic maps”, Pattern Recognition Letters, vol.152, pp. 356-364, 2021.

[39]. R.M. May, “Simple mathematical models with very complicated dynamics”, Nature, vol. 261, no. 5560, pp. 261–5560, 1976.

[40]. Y. Zhou, L. Bao, C.L.P. Chen, “A new 1D chaotic system for image encryption”, Signal Process. vol.97, pp. 172–182, 2014.

[41]. Y. Wu, G. Yang, H. Jin, J.P. Noonan, “Image encryption using the two-dimensional logistic chaotic map”, J. Electron. Imaging, vol.21, no.1, pp. 013014-013014-15, 2012.

[42]. Wikipedia, “Double-precision Floating-point Format”, Wikipedia, the Free Encyclopedia, 2013 (online; accessed 10.12.13).

[43]. X. Wang, J. Zhang, G. Cao, “An image encryption algorithm based on Zigzag transform and LL compound chaotic system”, Opt. Laser Technol. Vol.119, pp. 105581, 2019. https://doi.org/10.1016/j.optlastec. 2019.105581

[44]. K. Prabhavathi, M. B. Anandaraju, and V. Ravi, “Region based medical image encryption using advanced zigzag transform and 2D logistic sine map (2DLSM)”, International Journal of Cognitive Computing in Engineering, vol.4, pp:349-362, 2023.

[45]. Z., Hua, S., Yi, and Y. Zhou, “Medical image encryption using high-speed scrambling and pixel adaptive diffusion”, Signal Processing, vol.144, pp.134-144, 2018.

[46]. G. Alvarez, S. Li, “Some basic cryptographic requirements for chaos-based cryp-tosystems”, Int. J. Bifurcation Chaos, vol.16, no.08, pp.2129–2151, 2006.

[47]. Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J.P. Noonan, P. Natarajan, “Local Shannon entropy measure with statistical tests for image randomness”, Inf. Sci. vol.222, pp.323–342, 2013. https://doi.org/ 10.1016/j.ins.2012.07.049

[48]. Y. Xian, X. Wang, “Fractal sorting matrix and its application on chaotic image encryption”, Inf. Sci. vol.547, pp. 1154–1169, 2021.

[49]. R.M. Haralick, et al., “Textural features for image classification”, IEEE Transactions on systems, man, and cybernetics, vol.6, pp.610–621, 1973.

[50]. T. Li, et al., “Image encryption algorithm based on logistic and two-dimensional lorenz”, IEEE Access, vol.8, pp.13792–13805, 2020.

[51]. Cao, C., Sun, K., Liu, W.: “A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map”, Signal Process, vol.143, pp.122–133 (2018). https://doi.org/10.1016/j.sigpro.2017.08.020.