Natural and Applied Sciences International Journal (NASIJ)
eISSN: 2788-4619 (online)
https://ideapublishers.org/index.php/nasij
Vol. 7, No. 1 (January-December), 2026, pp. 122-139
https://doi.org/10.47264/idea.nasij/7.1.7
Original Research Article

Cryptanalysis of a lightweight image encryption scheme based on random shuffling and XOR operation

Lal Said*

Department of Avionics Engineering, Institute of Space Technology, Islamabad, Pakistan.

* Corresponding Author Email: engrlalsaid@yahoo.com

Abstract:

The rapid exchange of visual data across open networks has made image security a critical concern, particularly in fields such as healthcare, surveillance, and remote sensing where image integrity and confidentiality are essential. While many chaotic-based encryption schemes have been proposed, their security often relies on statistical metrics without rigorous cryptanalysis, leaving them potentially vulnerable. This study presents a detailed cryptanalysis of a recently proposed lightweight medical image encryption scheme that uses Henon, Brownian motion, and Chen chaotic systems for block-based shuffling, diffusion, and XOR-based confusion. We first reconstruct an equivalent structure of the scheme and perform a chosen-plaintext attack to recover its key components, including the permutation matrix, multiplication masks, and XOR keystream. Our analysis reveals structural weaknesses that allow full key recovery without knowledge of the original secret key. Based on these findings, we propose design improvements to address the identified flaws and enhance resistance to known cryptanalytic techniques. The work underscores the importance of incorporating cryptanalysis during the design phase of image encryption algorithms to ensure robust security in real-world applications.

Article History

Received:
19-Jun-2026

Revised:
28-Jul-2026

Re-revised:
25-Aug-2026

Accepted:
01-Sep-2026

Published:
09-Sep-2026

Keywords: Image encryption, Chaos theory, Cryptanalysis, Chosen-plaintext attack, Security evaluation, Lightweight cryptography, Medical image protection.

How to Cite:
Said, L. (2026). Cryptanalysis of a lightweight image encryption scheme based on random shuffling and XOR operation. *Natural and Applied Sciences International Journal (NASIJ), 7*(1), 122-139. https://doi.org/10.47264/idea.nasij/7.1.7

1. Introduction

In today's digital world, images play a powerful role in the way we communicate, understand, and interact with information. From social media to medical diagnostics and satellite surveillance, images are used to capture complex ideas quickly and effectively. In fields like healthcare, security, and remote sensing, images carry critical data that can influence real-time outcomes. Images are widely shared over the internet and stored on cloud platforms; they become vulnerable to unauthorized access. Securing images ensures that only intended users can interpret the content. Cryptography is one of the most reliable sources for the security of digital information. In the last decade, a lot of work has been done in the field of cryptography (Khan et al., 2025). The work presented in Jakson and Perumal (2024), introduces a color image encryption method using a fractional-order chaotic map integrated with pixel shuffling and diffusion, validated through statistical metrics and NIST randomness tests. Despite, the scheme's practical applicability may be constrained by implementation complexity and lacks evaluation under real-time or resource-constrained environments. The encryption scheme presented in Tiwari et al. (2025) proposes the OptiSecure-3D algorithm, which combines stacked autoencoders with optimized 3D chaotic maps and an encryption/decryption module to securely encrypt images. The method is validated through entropy, NPCR, UACI, and robustness tests against noise and cryptanalysis. Encryption method for 3-D images, involving SHA-256-based key generation, logistic map scrambling, LDCML-based confusion and diffusion, and tent map-based final confusion, is presented in Singh et al. (2025). The 3-D image is flattened to 2-D, and then encryption is performed. A color image encryption scheme that utilizes a novel 2D chaotic map (2D-CLCM) with RNA encoding, the pixels are encoded and scrambled by utilizing chaotic maps, the process of diffusion is performed through RNA key matrix (Liu et al., 2026). The encryption scheme presented in Kumar and Sharma (2024) utilizes Arnold's cat map for pixel shuffling, elliptic curve cryptography for confusion, and a genetic algorithm is utilized to optimize key. This multi-layered approach enhances security, showing high entropy, low correlation, and fast processing for efficient image encryption.

The study presented in Umar et al. (2024) proposes image encryption for cloud storage. This scheme using a modified Skew Tent chaotic map enhanced with sine function, followed by two permutation rounds and a diffusion step. The scheme possesses high entropy, low correlation, and strong immunity to various attacks. An encryption scheme that utilizes a DNA tree-based key generation and a novel chaotic state machine map (CSMM), combining logistic maps and finite state machines to control permutation and substitution via DNA encoding are presented in Alwida (2024). The algorithm performs two rounds of DNA-based permutation and substitution with XOR. The scheme has high security and efficiency across diverse image datasets. The work presented in Zhu and Zhu (2024), combines compressed sensing with encryption by using a 4D discrete chaotic map and Chebyshev-based Gaussian matrix for key stream generation, followed by scrambling, cyclic shift, and diffusion based on pixel values. In the embedding stage, cipher text is hidden in the high-frequency components of a wavelet-transformed carrier image to produce a visually secure encrypted image. The work utilizes a modified 2D logistic cascade map (2D LCM) combined with kolam-based scrambling [Color image encryption based on novel kolam scrambling and modified 2D logistic cascade map (2D LCM)]. The system generates key streams using the 2D LCM map and achieves encryption through a single round. The study presented in Ali et al. (2024) proposes a lightweight, improved AES-based encryption algorithm. This scheme utilizes a two-step key generation process, the first step involves chaotic function, and the second step utilizes 3D Lorenzo function. The confusion is achieved through dynamically generated S-boxes. This approach

enhances speed and efficiency. The work presented in Liu et al. (2024) introduces an image compression-encryption scheme. The scheme uses compressive sensing with chaotic matrices derived from a chaotic system.

For any secure image encryption method, it is essential that the resulting cipher text appears statistically random. Moreover, to have immunity against brute-force attack, the algorithm must have a larger key space. However, only the statistical and differential analysis of an encryption scheme, are not necessary and enough that the encryption scheme is secure. Cryptanalysis appears to be a major driving force in the advancement of encryption technology. As a result, a significant portion of research now focuses not only on developing chaotic encryption schemes but also on rigorously analyzing their vulnerabilities. This study presented in Zhou and Yu (2024) that chaotic image encryption schemes that depend on plaintext features must be designed with extreme care to avoid introducing patterns that make them vulnerable to differential and S-box-based attacks. The three methods proposed here expose the flaws in diffusion, substitution, and randomness, which are all fundamental to modern cryptography. The work of Wen and Lin (2024) presents a two-step attack: first, differential cryptanalysis is used to extract an equivalent permutation key; second, a chosen-plaintext attack with just four specific image pairs removes the DNA substitution layer. This results in full recovery of the original image with minimal computational effort. The findings demonstrate that QCMDC-IEA is fundamentally insecure and offer recommendations to enhance the robustness of similar chaos- and DNA-based encryption systems. Subsequently, many other cryptographic attacks are offered for different types of vulnerabilities (Chen et al., 2020).

1.1 Research Motivation and Contribution

Many chaos-based image encryption schemes report strong statistical performance, their resistance to cryptanalysis is often untested. High entropy, low correlation, and good NPCR/UACI values do not guarantee security if structural weaknesses remain. This gap is critical in domains like medical imaging, where data confidentiality is essential. To address this, we analyze a recently proposed lightweight chaos-based image encryption scheme. We reconstruct its internal structure, design a chosen-plaintext attack to recover its key components, and reveal vulnerabilities that allow full key recovery without knowing the original key. Based on these findings, we propose improvements such as incorporating key-dependent substitutions, per-round key expansion, and stronger coupling between confusion and diffusion layers to enhance resistance against cryptanalytic attacks. The researchers in the field of cryptography will consider the cryptanalysis concerns raised in the literature and will design more secure encryption scheme. Therefore, this paper analyzes a lightweight encryption scheme that is based on the random shuffling and XOR operation (Masood et al., 2021). The research contribution of this study is as follows:

- The under-discussion scheme is thoroughly analyzed, and an equivalent scheme is developed.
- A chosen plain text attack is performed on the under-discussion scheme to extract the key matrices i-e permutation matrix, multiplication and XOR matrix.
- Suggestions for improvements are given.

1.2 Organization of the Paper

The rest of the paper is organized as: the section 2 of the paper discusses some basic concepts,

the under-discussion scheme (Masood et al., 2021) is discussed in section 3 of the paper. The cryptanalysis is performed in section 4 of the paper. Section 5 performs computational complexity. The developed scheme having addressed the limitations are discussed in section 6 of the article. And finally, conclusion is drawn.

2. Basic concepts

This section is devoted to the definitions and introduction to the basic terms utilized in this study.

2.1 Cryptanalysis

The study of encryption schemes with the objective of breaking or extracting plaintext, key or structure without any prior knowledge is called cryptanalysis. Let:

- P = Plaintext space
- C = Ciphertext space
- K = Key space
- $E_k: P \rightarrow C$= Encryption function under key $k \in K$
- $D_k: C \rightarrow P$ = Decryption function under key $k \in K$

A cryptanalyst aims to find either:

The secret key k such that:

$$D_k\left(E\ k(p)\right) = p \qquad \forall p \in P \tag{1}$$

i.e., break the cipher by recovering the correct key. Or an equivalent key $k' \in K$such that:

$$D_{k'}\left(E\ k(p)\right) = p \qquad \forall p \in P \tag{2}$$

i.e., find a different key that works the same way. Or A function $f: C \rightarrow P$ such that:

$$f(c) = p, where\ c = E_k(p) \tag{3}$$

i.e., decrypt without recovering the key. A structural weakness allows partial recovery of plaintext or keys.

2.2 Cryptanalysis technique

Cryptanalysis refers to the study and practice of breaking cryptographic systems to reveal hidden information without access to the secret key. It plays a crucial role in evaluating the strength and security of encryption algorithms. There are several cryptanalysis techniques discussed in the subsequent section of the article.

Brute-force Attack: To recover the secret encryption key $k \in K$ by exhaustively searching all possible keys in the key space K, and checking which one correctly decrypts the cipher text c to the known plaintext $\boldsymbol{p}$. The brute-force attack involves:

$$Find\ k' \in K\ such\ that\ D_{k'}(c) = p \quad (4)$$

A known plaintext cipher text pair (p, c) is input and Loop over all possible keys $k' \in K$. For each k',check if $D_{k'}(c) = p$, then k' is the correct key.

Cipher text-Only Attack (COA): In a cipher text-only attack, the attacker has access only to one or more cipher texts $C = \{c_1, c_2 \ldots, c_n\}$, and attempts to deduce the original plaintexts $P = \{p_1, p_2, \ldots, p_n\}$ or the encryption key k, or both but without any knowledge of the plaintext. Given only cipher text $c = E_k(p)$ the attacker's goal is to approximate or recover either:

$$\hat{p} \approx \text{p} \quad \text{or} \quad \hat{k} \approx \text{k} \quad (5)$$

In images, plain text is highly redundant, if encryption does not fully randomize then COA can crack the system. Table 1 shows the matrices to detect COA weaknesses in image cipher.

Table 1: Metrics to Detect COA Weakness in image encryption scheme

Metric	Description	COA Indicator
Histogram analysis	Shows pixel intensity distribution	Peaks in histogram = weak encryption (COA vulnerable)
Entropy	Measures randomness	Ideal value: 7.999 for 8-bit image if less then (COA vulnerable)
Correlation	Adjacent pixel dependency	deal: ~0 (in encrypted image)
NPCR & UACI	Measures diffusion	Low values = weak diffusion (COA vulnerable)

Known-Plaintext Attack (KPA): In a Known-Plaintext Attack, the attacker has access to a set of plaintexts $\{pi\}$ and their corresponding cipher texts$\{ci\}$, encrypted using an unknown key k.The objective of the KPA is to determine the secret key k, or to derive an equivalent key k', such that:

$$E_k(p_i) = c_i \quad \forall i \quad (6)$$

Or, alternatively, to develop a method that decrypt new cipher texts without needing the original key. The attacker exploits the relation $c_i = E_k(p_i)$ to build a system of equations involving the unknown key k. If enough such equations exist, the attacker can solve for k. Let's suppose the cipher is:

$$c_i = p_i \oplus k \quad (7)$$

This is a simple but common operation in lightweight image encryption. If both pi and ci are known, then:

$$k = c_i \oplus p_i \quad (8)$$

This reveals the key directly. The KPA is powerful and practical, especially in image encryption where parts of the image may be predictable. XOR-based schemes and schemes with static or linear transformations are especially vulnerable. Proper design must ensure high diffusion, nonlinearity, and key-dependence to resist KPA.

Chosen-Plaintext Attack (CPA): In a Chosen-Plaintext Attack, the attacker can choose arbitrary plaintexts $p_1, p_2, \ldots, p_n$, input them into the encryption system, and obtain corresponding cipher texts $c_1, c_2, \ldots, c_n$, where:

$$c_i = E_k(p_i) \tag{9}$$

The goal is to analyze how the encryption function E_k behaves under specific plaintext changes in order to reveal the secret key k, internal structure, or allow future decryption. A simple example illustrates the CPA. Let the encryption function be:

$$E_k(p) = P(p \oplus k) \tag{10}$$

p is 4-byte plaintext block, k is 4-byte secret key, $\oplus$ is XOR operation and P is fixed byte permutation function. P swaps 1st and 4th bytes, and 2nd and 3rd bytes. And the secret key is $k = [11,22,33,44]$ in decimal. Let:

$$p_1 = [0,0,0,0]$$

Then

$$p_1 \oplus k = [11,22,33,44]$$

And

$$c_1 = P([11,22,33,44]) = [44,33,22,11]$$

Now attacker has known:

$$p_1 = [0,0,0,0]$$

And observed

$$c_1 = [44,33,22,11]$$

Now by applying P^{-1} to cipher text we get the key.

3. M. Fawad et al. encryption Scheme

A clear understanding of any encryption scheme is necessary for cryptanalysis. Therefore, in this section, we will discuss the foundations of the cryptosystem, by presenting a concise overview of the underlying encryption scheme. The article [16] proposes a lightweight and efficient medical image encryption scheme. The encryption scheme utilizes multiple chaotic systems Henon Chaotic Map (HCM), Brownian Motion (BM), and Chen's Chaotic System (CSS). These chaotic systems generate permutation vectors and maps for XOR operation. The grayscale image is divided into 8×8 blocks, which undergo pixel and block shuffling by utilizing chaos-based sequences. To induce confusion, the image is XORed with a chaos-based matrix, having the same dimensions as the image. Extensive experiments validate the scheme's performance using statistical metrics such as histogram uniformity, correlation coefficients, information entropy (≈8), NPCR, UACI, and NIST randomness tests, all indicating strong resistance to differential and statistical attacks. Additionally, the scheme demonstrates low computational complexity, making it suitable for real-time or resource-constrained environments. The overall encryption scheme comprises of the following sequential transformation:

$$E(p) = \alpha_{conf} \odot \alpha_{diff}\ (p) \tag{11}$$

Where $p \in M_{m\times n}\ (Z_{256})$ the input is plain image, α_{diff} is the shuffling driven by HCM map based permutation and α_{conf} is the confusion driven by the BM generated multiplication map and CSS generated XOR map. A step-by-step method of the proposed cryptosystem is outlined in the subsequent section of the write-up.

3.1 Encryption Procedure

The proposed encryption scheme secures grayscale medical images using a chaos-based substitution-permutation network (SPN), achieving confusion and diffusion through multiple chaotic systems: Henon Map, Brownian Motion, and Chen's System. The process consists of several well-defined stages:

a. Preprocessing: Image Blocking

The image is resized into 512×512 dimensions and is partitioned into 8×8 block. Let $I \in Z^{512\times512}$ be a grayscale image with 8-bit pixel values. The image is divided into 64×64=4096 blocks of size 8×8, denoted as:

$$I = \bigcup_{k=1}^{4096} B_k \qquad B_k \in z^{8\times8} \tag{12}$$

b. Diffusion through intra block shuffling

The Henon Chaotic Map (HCM) is a 2D discrete-time system defined by:

$$\begin{cases} x_{n+1} = 1 - \mathrm{a}x_{\mathrm{n}}^2 + y_n \\ \quad . \\ y_{n+1} = \quad bx_n \end{cases} \tag{13}$$

Where $a = 1.4, b = 0.3$, and (x_0, y_0) are the initial conditions. For each block, generate a sequence of 8×8=64 chaotic values $\{x_i\}$ by iterating the map. These values are sorted, and their sorted indices define a permutation vector, which is applied to rearrange pixels within the block. This introduces diffusion.

c. Inter-Block Shuffling

After intra-block shuffling, the entire set of 4096 blocks is shuffled again using a chaotic sequence. Let Q be a permutation vector of length 4096. Apply Q to the sequence of blocks:

$$I_{perm} = permute(\{B_k^{shuffled}\}, Q) \tag{14}$$

This achieves further diffusion at a global level, obscuring image structure.

d. Confusion via Brownian Motion-Based Masking

A 3D Brownian motion (BM) model is simulated using:

$$\begin{cases} X = rsin(a)\cos(b) \\ Y = rsin(a)sin(b) \\ \quad z = r\cos(a) \end{cases} \qquad for\ r = 2, a \in [0,\pi], b \in [0,2\pi] \tag{15}$$

The BM simulation generates sequences $\{T1(i,j)\}, \{T2(i,j)\}, \{T3(i,j)\} \in R^{512\times512}$ corresponding to three directions (X, Y, Z). After discarding transient values, the retained chaotic values are processed:

$$\begin{cases} V_k = 10^{14} \cdot T_k, & k = 1,2,3 \\ x_k = abs\big(round(v_k)\big) mod\ 256 \end{cases} \quad (16)$$

This gives $Y_k = X_k mod\ 256 \in Z_{256}^{512\times512}$, interpreted as mask matrices. These matrices are used to perform pixel-wise multiplication with the previously shuffled image I_{perm} .

$$Z_k = I_{perm} \odot Y_k \quad (17)$$

e. Final Confusion via Chen's Chaotic System through XOR

The Chen chaotic system is defined by:

$$\begin{cases} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = (c - a)x - xz + cy \\ \frac{dz}{dt} = xy - bz \end{cases} \quad (18)$$

Where $a = 35, b = 3, c = 28$. The system is discretized (e.g., using Euler's method) and it is iterated to generate 2D chaotic sequences for encryption.

Let $C_k \in Z_{256}^{512\times512}$ be the final Chen-derived key stream. The cipher image is produced by bitwise XOR of the diffused image Z_k with the chaos mask:

$$E_k = Z_k \oplus C_k \quad (19)$$

This step reintroduces confusion and prevents statistical recovery of pixel values.

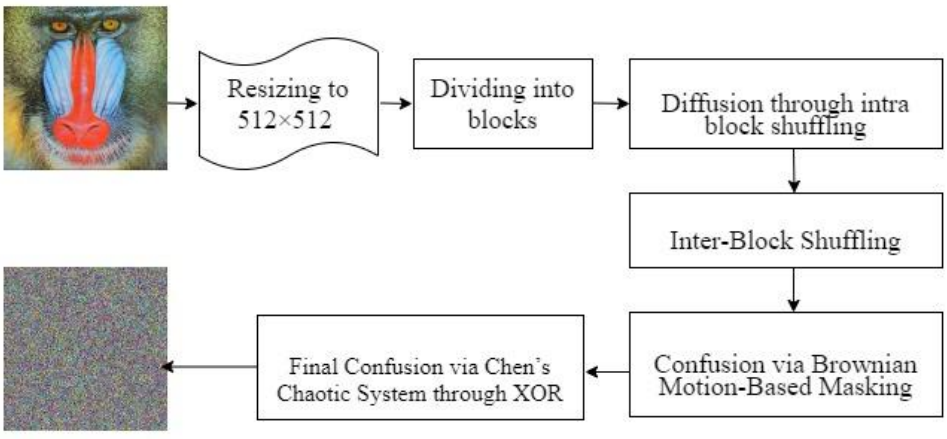

Figure 1: Equivalent structure of the understudy encryption scheme

Figure 1 represents an equivalent structure of the understudy encryption framework where the original image is first resized and divided into blocks. The encryption process applies multiple layers of confusion and diffusion, starting with intra-block shuffling, followed by inter-block shuffling, and then masking through Brownian motion. Finally, Chen's chaotic system is used

for additional confusion through XOR, resulting in a highly encrypted image. Our cryptanalysis goal is to locate where those blocks end up after inter-block shuffling, find out the intra-block permutation used inside each of them, and recover the masks applied to those blocks so we can invert the XOR stages.

4. Cryptanalysis

In this section, we present a cryptanalysis of the encryption scheme proposed in [16], performed without access to the secret key. This analysis is grounded in Kerckhoffs's Principle, which asserts that a cryptographic system should remain secure even when all details of the algorithm are publicly known—except for the secret key. Guided by this principle, modern encryption schemes are designed with the assumption that only the key must remain confidential. The primary objective of this cryptanalysis is to uncover potential flaws and vulnerabilities in the existing scheme, highlighting limitations that could compromise secure communication. Based on these findings, recommendations for improvement are also provided to enhance the overall robustness of the encryption method.

4.1 Recovery of CSS generated Matrix for bitwise XOR operation

The plaintext is chosen such that the plain-text is not changed by the pixels and blocks permutation process and the multiplication operation. Therefore, after the insertion of the chosen plaintext, the CCS generated Bitwise XOR Operation matrix is achieved. The detail of the first chosen plaintext is as follows:

Shuffling: Let the plaintext be: $P \in Z_2^{512\times512}$ where $P_{i,j} = 0\ \forall i,j$ **.** Now this plaintext is divided in to B_k as in Eq. (12). Each block B_k is a matrix of all zeros. Shuffling pixel positions within each block using some permutation function π:

$$B_k{}' = \pi(B_k)$$

Since all entries in B_k is zero, permutation has no effect:

$$B_k{}' = B_k = \mathbf{0_{8\times8}}$$

Rearranging the position of the blocks across the image using a second permutation ρ, let $P' = \rho(\{B_k{}'\})$. Again, all blocks are zero, so:

$$P' = P = 0_{512\times512}$$

Multiplication with BM-generated Matrix: Let $M \in Z_2^{512\times512}$ a binary matrix generated using a chaotic map often referred to as BM-generated matrix.

$$E = M \odot P'$$

Here, $\odot$ denotes element-wise multiplication. Since $P' = 0$, regardless of what M contains:

$$E_{i,j} = M_{i,j} \cdot 0 = 0 \qquad \forall i,j \Rightarrow E = 0_{512\times512}$$

XOR with CCS-generated Chaotic Map: Let $K \in Z_2^{512\times512}$ be the key stream or confusion map generated using CCS

$$C = E \oplus K = 0 \oplus K = K$$

The cipher text is exactly equal to the key stream:

$$C = K$$

The figure 2 shows how chosen-plaintext cryptanalysis can be used to recover the Chen's Chaotic System matrix used in the encryption scheme. By feeding an all-zero plaintext through the encryption process, the attacker can bypass the effects of shuffling and directly expose the key-stream generated by Chen's chaotic system. Once this key-stream is known, it can be reused to decrypt or forge cipher-texts, which is a serious weakness of the scheme.

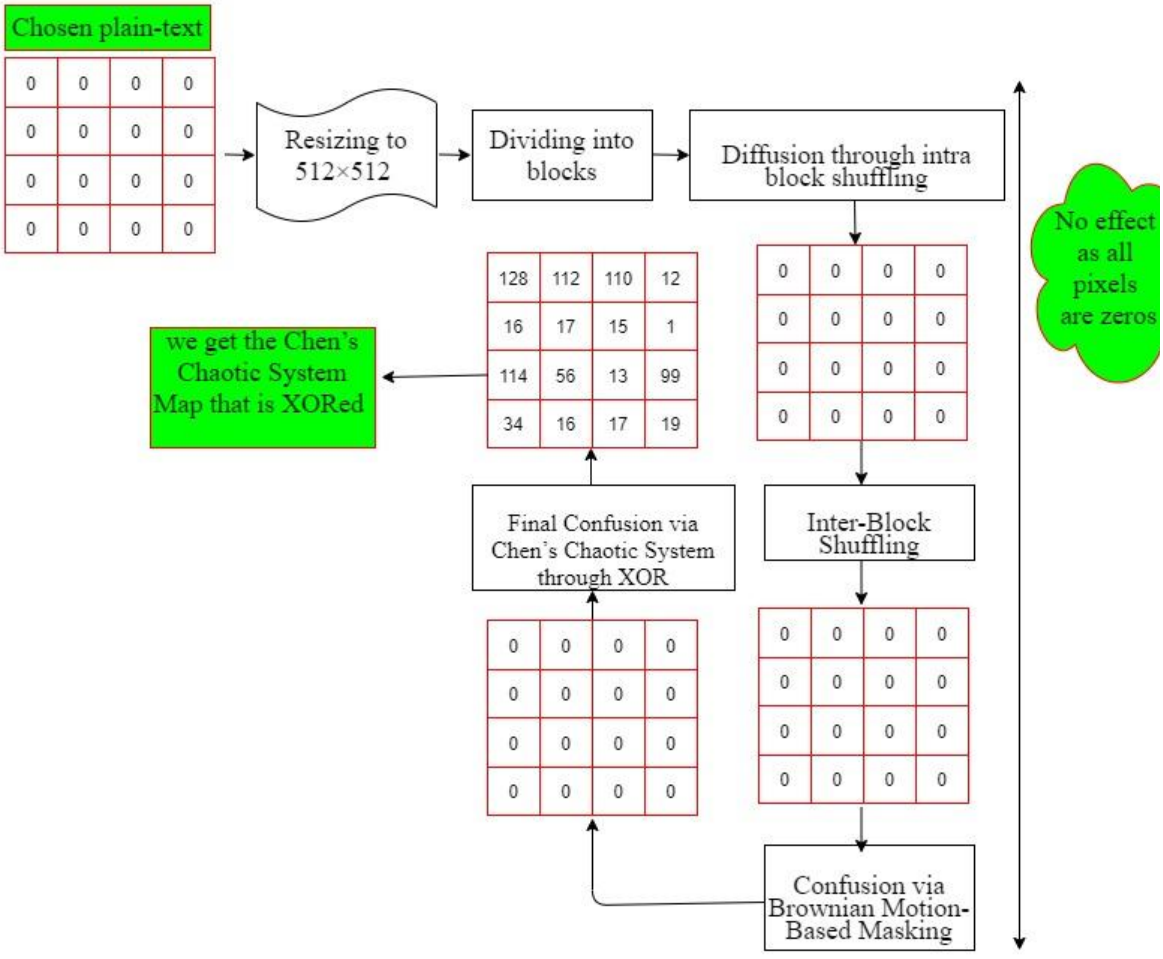

Figure 2: Recovery of CSS generated Matrix for bitwise XOR operation

4.2 Recovery of BM generated multiplication matrix

The plaintext is chosen such that the plain-text is not changed by the pixels and blocks permutation process and we get the multiplication matrix generated by BM. The detail of the first chosen plaintext is as follows:

Let's the chosen plain text image is defined as:

$P \in Z_2^{512\times512}$ where $P_{i,j} = 1 \quad \forall i,j$

Inter and Intra Block Shuffling: Let the shuffling function (inter + intra) be denoted by:

$$P' = \rho(\pi(P))$$

Since P is all ones, shuffling don't change any values:

$$P' = P = 1_{512\times512}$$

Element-wise Multiplication with BM-generated Matrix: Now apply element-wise multiplication (denoted by $\odot$):

$$E = P' \odot M = 1 \odot M = M$$

So the result after this step is exactly the BM-generated matrix:

$$E = M$$

XOR with CCS-generated Map: Final encryption step:

$$C = E \oplus K = M \oplus K$$

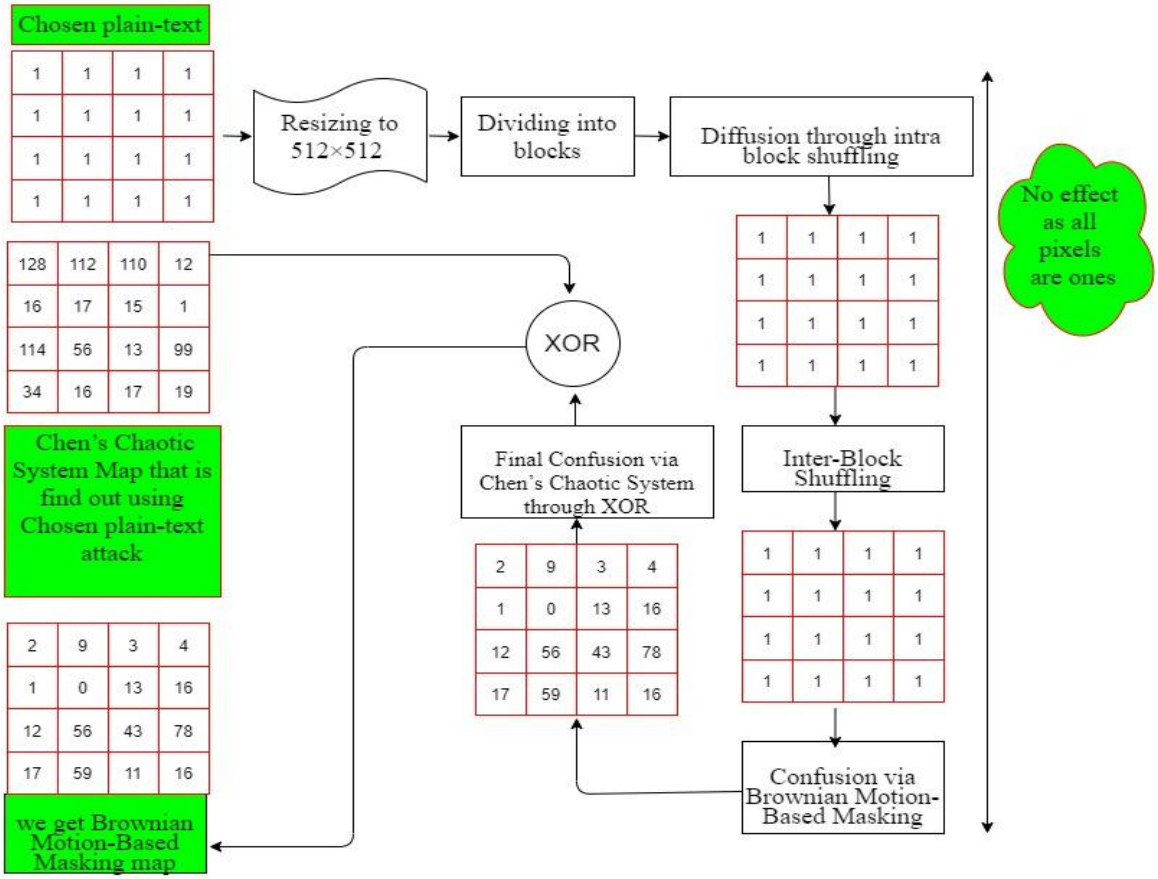

Figure 3: Recovery of BM generated multiplication matrix

Since in a previously chosen-plaintext attack we already extracted$K$, and now you have the new cipher text C, the extracted the BM-generated matrix is:

$$M = C \oplus K$$

The Figure 3 is showing how a chosen-plaintext attack with all-one input can be used to recover the Brownian Motion (BM)–based masking matrix used in the encryption scheme. By encrypting an all-one plaintext image, the attacker directly recovers the Brownian motion–based masking map by utilizing the earlier attack all-zero input that reveals the Chen's chaotic map.

4.3 Recovery of block shuffling

Let:

- Image size: 512×512
- Block size: 8×8
- Total number of blocks: $N = \left(\frac{512}{8}\right)^2 = 64 \times 64 = 4096$

Let's the chosen plain text image is defined as:

$$P \in Z_2^{512\times512}$$

Each 8×8 block is assigned a unique constant or unique pattern.

$$P = \bigcup_{i=1}^{4096} B_i \qquad where\ each\ \ B_i \in z^{8\times8}\ is\ a\ unique\ pattern$$

a. Intra-block Shuffling (Preserves Block Identity): Let the intra-block shuffling within a block Bi be:

$$B_i{}' = \pi b(B_i)$$

Since each block has a unique value or pattern, the shuffled block $Bi'$is still uniquely identifiable, just with rearranged pixels. Reconstructed image after intra-block shuffling:

$$P' = \bigcup_{i=1}^{4096} Bi'$$

b. Inter-block Shuffling (Block Permutation): Inter-block shuffling reorders the position of these shuffled blocks. Let ρ_b be the permutation function:

$$\boldsymbol{P''} = \rho_b(\boldsymbol{P'}) = \bigcup_{i=1}^{4096} B'_{\sigma_i}$$

Where $\sigma: \{1,2,\dots,4096\} \to \{1,2,\dots,4096\}$ is the block permutation function. Our goal is to recover σ.

c. Multiplication and XOR: Now we perform encryption

$$E = P'' \odot M$$
$$C = E \oplus K$$

Since both M and K are known (from earlier cryptanalysis steps), we can compute:

$$P'' = (C \oplus K) \oslash M$$

This gives us the shuffled image P''.

d. Recover the Block Permutation σ: Since each original block B_i had a unique pattern, match every Bi' inside P'' back to its original block location. By comparing, each 8×8 block in P'' , With the set of known original blocks, the permutation vector is recovered

$\sigma(i) = index\ of\ B_i\ in\ P''$

4.4 Recovery of Pixel shuffling

To reveal the intra-block pixel permutation, using a chosen-plaintext attack, the plaintext is designed in such a way that only one block (e.g., the first one) contains unique values. Then, after tracking how those values are permuted in the cipher text, the permutation vector is recovered. Let: Block size: 8×8⇒64, Image size: 512×512⇒4096 blocks. The chosen plaintext have first block has known unique values 0 to 63, and the rest will have all zero.

$$B_0 = \begin{bmatrix} 0 & 1 & \cdots & 7 \\ 8 & 9 & \cdots & 15 \\ \vdots & \vdots & \ddots & \vdots \\ 56 & 57 & \cdots & 63 \end{bmatrix}$$

Let's flatten it to a 1D vector in row-major order:

$$v = [0,1,2,\ldots,63]$$

Other blocks in P have 0 pixels values. Let the unknown permutation applied to the block be represented as a permutation vector π, which maps indices. Then the shuffled block v' is:

$$v' = \pi(v)$$

Since the original $v = [0,1,2,\ldots,63]$, the position of value iii in v' gives $\pi^{-1}(i)$:

$$\pi^{-1}(i) = position\ of\ value\ i\ in\ v'$$

Let $M \in Z_2^{512\times512}$ and $X \in Z_2^{512\times512}$ be the block multiplication matrix (BM) and chaotic XOR vector (CCS). Then the final encrypted block is:

$$c = M \cdot v' \oplus X$$

Since both M and X are known, we can reverse, by removing XOR

$$y = c \oplus X$$

And remove multiplication

$$v' = M^{-1} \cdot y$$

v' is the shuffled vector, which contains the permuted values 0 to 63.

5. Computational Complexity of the analysis

In this section, we evaluate the time and space complexity of the cryptanalysis techniques used to recover the key components of the encryption scheme, namely the XOR matrix (CCS), the multiplication matrix (BM), the block-level permutation (inter-block shuffling), and the pixel-level permutation (intra-block shuffling). The computational complexity is expressed in terms of the image size $n \times n$ where $= 512$, and the number of 8×8 blocks.

5.1 Computational Complexity for XOR Matrix (CCS)

In this attack only the chosen plaintext, comprising of all zeros are given as input. The image passes through permutation and multiplication, but since it's all zero, the result stays zero. So when the encryption does the final XOR step, the cipher text is exactly the secret key. Since this attack requires no computation beyond submission of a single plaintext and directly observes the cipher text as the key stream K, the Time Complexity is $O(n^2)$ that is due to the single XOR with the key stream. The Space Complexity is $O(n^2)$which is due to the storage of the key stream K.

5.2 Computational Complexity for of BM Multiplication Matrix

In this attack only the chosen plaintext, comprising of all 1 are given as input. The image passes through permutation but since all pixels are similar, so the result stays 1, to compute the BM Requires one XOR operation for each pixel as in Eq.() the Time Complexity is $O(n^2)$ that is due to the single XOR. The Space Complexity is $O(n^2)$which is due to the storage of the full matrix M.

5.3 Computational Complexity of Inter block shuffling

To recover the block-level permutation σ, a chosen-plaintext attack is designed in which each 8×8 block of the input image contains a unique and identifiable pattern. After encryption, the known XOR matrix K and multiplication matrix M are used to reverse the final encryption step by computing.

$$P'' = (C \oplus K) \oslash M$$

which gives the shuffled image. Since each original block has a unique pattern, each one can be matched with its counterpart in the shuffled image to determine the new positions of the blocks. This allows recovery of the permutation function σ by identifying where each original block ended up. The comparison of each block against all others results in $O(n^4)$ complexity. And the space complexity remains $O(n^2)$due to the need to store full image data.

5.4 Computational complexity of intra block shuffling

To recover the intra-block (pixel-level) permutation π, a chosen-plaintext is constructed where only the first 8×8 block contains unique values from 0 to 63, while all other blocks are filled

with zeros. This ensures that only the first block is affected by the pixel-level shuffling, multiplication. After encryption, the XOR matrix X and the block-wise multiplication matrix M are known from earlier steps, allowing the attacker to isolate the shuffled block by computing.

$$v' = M^{-1} \cdot (C \oplus X)$$

where v' is the shuffled version of the known vector v. Since the original values are known, comparing the position of each number in v' with its original position in v reveals the permutation vectorπ. This recovery process involves one matrix inversion $O(64^3)$, one matrix-vector multiplication $O(64^2)$, and a search operation $O(64\cdot)$,, resulting in a total time complexity of approximately $O(10^5)$,, which is practically fast due to the small block size. The space complexity is $O(64^2)$, as only a single block needs to be processed and stored.

The proposed cryptanalysis method is computationally efficient, as each step in the attack utilizes simple and low-complexity operations to fully recover critical components of the encryption scheme.

6. Improvement Suggestions

The security of the proposed scheme can be significantly enhanced by introducing several design refinements. First, the parameters of the chaotic maps (a,b,c) should be incorporated into the secret key and randomly selected within their respective chaotic ranges for each session. This would expand the effective key space and prevent attackers from assuming fixed parameter values. A key-expansion mechanism can then be employed to derive distinct round keys from a single master key, thereby strengthening resistance against brute-force and related-key attacks. Furthermore, the overall SPN structure comprising shuffling, masking, and XOR operations should be iterated over multiple rounds, with each round driven by an independent round key. This round-based design would introduce inter-round dependencies, ensuring that the compromise of one round does not expose the others, and substantially increasing the complexity of chosen-plaintext or analytical attacks. Finally, the inclusion of a substitution stage based on dynamically generated, key-dependent S-boxes is recommended. Such S-boxes would inject strong nonlinearity into the encryption process, enhancing confusion and further obfuscating statistical relationships between the plaintext and cipher-text. Together, these improvements would provide a more robust cryptographic structure without compromising computational efficiency.

7. Conclusion

This work examined the security of a chaos-based lightweight image encryption scheme designed for medical image protection. By reconstructing an equivalent version of the scheme and applying a chosen-plaintext attack, we successfully extracted the core key components and demonstrated that the scheme can be broken without prior knowledge of the secret key. The findings highlight critical design weaknesses, particularly in how the permutation and confusion stages interact, making the scheme vulnerable to key recovery. In light of these vulnerabilities, we provided practical recommendations to improve its security, such as integrating stronger substitution layers, increasing key space diversity, and introducing dependency on plaintext for enhanced diffusion. This study emphasizes that statistical performance alone is insufficient to validate encryption security and reinforces the necessity of thorough cryptanalysis when designing image encryption systems for real-world use.

Declaration of conflict of interest:

The author(s) declared no potential conflicts of interest(s) with respect to the research, authorship, and/or publication of this article.

Funding:

The author(s) received no financial support for the research, authorship and/or publication of this article.

Publisher's Note:

IDEA PUBLISHERS (NASIJ) stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

References

Ali, A. H., Gbashi, E. K., Alaskar, H., & Hussain, A. J. (2024). A lightweight image encryption algorithm based on secure key generation. *IEEE Access, 12*, 95871–95883. https://doi.org/10.1109/ACCESS.2024.3414334

Alawida, M. (2024). A novel DNA tree-based chaotic image encryption algorithm. *Journal of Information Security and Applications, 83*, 103791. https://doi.org/10.1016/j.jisa.2024.103791

Chen, J., Chen, L., & Zhou, Y. (2020). Cryptanalysis of a DNA-based image encryption scheme. *Information Sciences, 520*, 130–141. https://doi.org/10.1016/j.ins.2020.02.024

Jackson, J., & Perumal, R. (2025). A robust image encryption technique based on an improved fractional order chaotic map. *Nonlinear Dynamics, 113*(7), 7277–7296. https://doi.org/10.1007/s11071-024-10480-7

Khan, M., Aljuaydi, F., Said, L., & Amin, M. (2025). A secure chaotic cryptosystem for thermal imaging: Logistic map-based encryption with substitution-diffusion and spatial decorrelation. *Journal of Radiation Research and Applied Sciences, 18*(2), 101546. https://doi.org/10.1016/j.jrras.2025.101546

Kumar, S., & Sharma, D. (2024). A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. *Artificial Intelligence Review, 57*, 87. https://doi.org/10.1007/s10462-024-10719-0

Liu, W., Wang, H., Chen, Y., & Sun, K. (2024). A new image encryption scheme based on block compressive sensing and chaotic laser system for IoT. *The European Physical Journal Plus, 139*(6), 473. https://doi.org/10.1140/epjp/s13360-024-05221-z

Liu, X., Zheng, S., & Yang, J. (2026). Color image encryption scheme based on a novel 2D-CLCM chaotic system and RNA encoding. *Mathematics and Computers in Simulation, 239*, 340–360. https://doi.org/10.1016/j.matcom.2025.06.009

Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S., Jan, S. U., Qayyum, A., & Buchanan, W. J. (2022). A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. *Wireless Personal Communications, 127*, 1405–1432. https://doi.org/10.1007/s11277-021-08584-z

Mathivanan, P., & Maran, P. (2024). Color image encryption based on novel kolam scrambling and modified 2D logistic cascade map (2D LCM). *The Journal of Supercomputing, 80*(2), 2164–2195. https://doi.org/10.1007/s11227-023-05539-y

Singh, D., Kaur, H., Verma, C., Kumar, N., & Illés, Z. (2025). A novel 3-D image encryption algorithm based on SHA-256 and chaos theory. *Alexandria Engineering Journal, 122*, 564–577. https://doi.org/10.1016/j.aej.2025.03.026

Tiwari, A., Diwan, P., Diwan, T. D., Miroslav, M., & Samal, S. P. (2025). A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image

communication. *Scientific Reports, 15*, 14151. https://doi.org/10.1038/s41598-025-95995-8

Umar, T., Nadeem, M., & Anwer, F. (2024). Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage. *Expert Systems with Applications, 257*, 125050. https://doi.org/10.1016/j.eswa.2024.125050

Wen, H., & Lin, Y. (2024). Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. *Expert Systems with Applications, 237*, 121514. https://doi.org/10.1016/j.eswa.2023.121514

Zhou, R., & Yu, S. (2025). Cryptanalysis on chaotic image cryptosystem of plaintext-related from multiple perspectives. *Nonlinear Dynamics, 113*(20), 28397–28412. https://doi.org/10.1007/s11071-025-11582-6

Zhu, S., & Zhu, C. (2024). A visual security multi-key selection image encryption algorithm based on a new four-dimensional chaos and compressed sensing. *Scientific Reports, 14*, 15496. https://doi.org/10.1038/s41598-024-66320-6