

Secure Medical Image Transmission via CNN-Derived Keys and Chaotic DNA Encoding

Sara Bentouila¹, Kamel Mohamed Faraoun²

^{1,2}Department of Computer Science, Djillali Liabes University of Sidi Bel Abbes, EEDIS Laboratory, Algeria

Article Info

Article history:

Received Nov 19, 2025

Revised Dec 18, 2025

Accepted Dec 24, 2025

Keywords:

Medical image encryption
chaotic system
CNN-based key generation
DNA encoding
Cipher Feedback (CFB)
Lü chaotic map

ABSTRACT

This paper presents a secure and efficient hybrid encryption framework designed for medical image protection. The method combines a fine-tuned MobileNetV3 network for content-adaptive key generation with the nonlinear dynamics of a Lü chaotic system and a DNA-based Cipher Feedback (CFB) diffusion stage. The proposed approach eliminates the arbitrary selection of chaotic maps commonly found in existing methods by dynamically adapting to image content. Experimental tests conducted on brain MRI images demonstrate strong security and robustness, achieving an entropy of 7.9998, NPCR of 99.58%, UACI of 29.93%, PSNR of 7.43 dB, and an average encryption time of 0.24 s. These results confirm excellent randomness, high key sensitivity, and real-time processing capability. The proposed model outperforms recent chaotic and hybrid schemes, making it suitable for secure medical image transmission and telemedicine applications.

Copyright © 2025 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Sara Bentouila
Department of Computer Science,
Djillali Liabes University of Sidi Bel Abbes,
EEDIS Laboratory, Algeria
Email: sara.bentouila@univ-sba.dz, bentouila.sara@yahoo.fr

1. INTRODUCTION

The growing adoption of telemedicine and digital imaging has considerably increased the circulation of medical images over public and cloud networks. While this digitalization improves diagnosis accessibility and remote consultation, it also exposes sensitive medical data to serious privacy and security threats, including interception, unauthorized access, and manipulation. Thus, ensuring the confidentiality, integrity, and reliability of medical images has become a major challenge for modern healthcare systems[1–4].

Conventional cryptographic algorithms such as AES and DES offer strong general-purpose security but are not optimized for medical images, which contain highly correlated pixels and redundant spatial structures[5, 6]. To overcome these limitations, many researchers have explored chaotic systems[7–17], DNA encoding[7–9, 18–21], and hybrid encryption models[22–29].

Although these methods improve diffusion and randomness, several critical limitations persist. Most existing schemes rely on a fixed or arbitrarily selected chaotic map, without formal justification or adaptability to the image content, which may degrade entropy and key sensitivity. Additionally, chaotic parameters are often static, reducing resistance to brute-force or statistical attacks, while computational complexity remains high for large medical datasets. Consequently, the design of an adaptive and data-dependent encryption system remains an open research problem.

To address these issues, this paper introduces a novel hybrid encryption framework for medical images. The proposed model combines the content-aware learning capability of a deep neural network with the nonlinearity

of chaotic dynamics and the parallelism of DNA operations. Specifically, a fine-tuned MobileNetV3 is employed to generate content-dependent cryptographic keys with high entropy, which are then coupled with a Lü chaotic system dynamically selected for its superior sensitivity and numerical stability. Finally, a DNA-based Cipher Feedback (CFB) diffusion mechanism ensures multi-level confusion and resistance to differential attacks. This combination achieves a secure and computationally efficient encryption process tailored for medical image protection and telemedicine applications.

This study offers the following main contributions:

A CNN-based key generation mechanism that produces adaptive, high-entropy keys dependent on medical image content.

A systematic selection of the optimal chaotic map (Lü system), replacing arbitrary choices used in prior works.

Integration of DNA encoding and CFB diffusion to enhance confusion, diffusion, and key sensitivity.

Comprehensive evaluation through entropy, correlation, NPCR, UACI, PSNR, and runtime analysis, showing superior performance to existing approaches.

The rest of the paper proceeds as follows: Section 2. reviews recent advances in medical image encryption; Section 3. covers theoretical foundations including chaotic maps and DNA encoding; Section 4. details our proposed methodology; Section 5. presents the experimental results and comparative discussion; and Section 6. concludes with insights and future directions.

2. RELATED WORKS

Medical image encryption has increasingly adopted hybrid approaches that combine chaotic dynamics, DNA operations, and learning-based key generation. Classical chaos-based models—such as Logistic, Henon, Tent, and spatiotemporal maps—have shown strong diffusion capabilities and high entropy when applied to medical images [1–4]. [1] proposed a Latin-square memristive chaotic scheme specifically designed for medical images, while [30] and [31] developed hybrid chaotic–DNA frameworks achieving high NPCR/UACI and low pixel correlation.

To enhance adaptability, several works introduced DNA-guided confusion and correlated chaotic keys for telemedicine applications, including the DNA–chaos systems of [32] and [33]. More recent studies integrate deep learning to generate image-dependent cryptographic keys. [25] used CNN-based key estimators within chaotic ciphers, [34] combined CNN predictions with chaotic permutations, while [35] and [36] applied deep networks specifically to medical data encryption [37].

In addition to the aforementioned approaches, several recent studies have investigated alternative chaos-based security schemes with a particular focus on efficiency, hardware implementation, and multimedia protection. For instance, a resource-optimized selective encryption method using multiple chaotic systems was proposed to secure medical images while reducing computational overhead [38]. Hardware-oriented chaotic encryption has also been investigated through an FPGA-based 128-bit chaotic encryption architecture designed for real-time voice communication, highlighting the feasibility of chaos-based cryptographic primitives in embedded and real-time environments [39]. Furthermore, chaos-driven techniques have been extended to multimedia integrity protection; an efficient invisible color image watermarking scheme based on chaotic maps was introduced to enhance robustness against common attacks [40]. These contributions demonstrate the versatility of chaotic systems across different security applications and further motivate the development of efficient and adaptive chaos-assisted encryption frameworks.

Despite the effectiveness of existing chaotic and DNA-based encryption schemes, many approaches rely on fixed DNA rules or static chaotic parameters, which limits adaptability and key sensitivity, while only partially exploiting the intrinsic structure of medical images. Recent CNN-assisted encryption methods improve key dependency on visual data; however, they often lack rigorous chaotic map selection or remain computationally expensive. To overcome these limitations, the present work introduces a content-adaptive medical image encryption framework that integrates a lightweight MobileNet-based key generator with a systematically selected Lü chaotic system and dynamic DNA–CFB diffusion, achieving enhanced key sensitivity, robust security, and real-time efficiency.

3. THEORETICAL BACKGROUND

This section briefly outlines the main theoretical concepts underlying the proposed hybrid encryption framework, including chaotic dynamics, DNA encoding, and Cipher Feedback (CFB) diffusion.

3.1. Chaotic Systems Overview

Chaotic systems are nonlinear dynamic models characterized by sensitivity to initial conditions, ergodicity, and pseudo-randomness. In image encryption, these properties are exploited to generate sequences that enable strong confusion (pixel shuffling) and diffusion (intensity transformation). A tiny variation in initial parameters leads to completely different outcomes, making chaotic maps ideal for cryptographic applications[41]. Several chaotic models have been investigated in the literature, such as Logistic[42], Tent[43], Henon[44], Duffing[45], Lorenz[13], Chen, and Lü maps. Each of them exhibits specific behaviors in terms of dimensionality, complexity, and randomness. The equations of some widely used systems are presented below:

3.1.1. Logistic Map

$$x_{n+1} = rx_n(1 - x_n), \quad 0 < r \leq 4 \quad (1)$$

3.1.2. Henon Map

$$\begin{cases} d_{n+1} = 1 - ad_n^2 + f_n \\ f_{n+1} = bd_n \end{cases} \quad (2)$$

3.1.3. Lorenz System

$$\begin{cases} \dot{l} = \sigma(m - l) \\ \dot{m} = l(\rho - n) - m \\ \dot{n} = lm - \beta n \end{cases} \quad (3)$$

The choice of the chaotic model significantly influences the overall security and statistical quality of the encryption scheme. In this work, the Lü chaotic system was adopted due to its higher degree of nonlinearity, wide chaotic range, and numerical stability compared with traditional maps.

3.1.4. The Lü Chaotic Map

The Lü chaotic system is a three-dimensional continuous model introduced as an intermediate attractor between the Lorenz and Chen systems. It exhibits strong chaotic oscillations and a wide parameter space suitable for cryptographic applications requiring high sensitivity and unpredictability.

The mathematical form of the Lü system is defined as (Eq 4):

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = -xz + cy \\ \dot{z} = xy - bz \end{cases} \quad (4)$$

where a, b and c are positive constants controlling the system's dynamics. For suitable parameter values, the system generates three pseudo-random sequences (x, y, z) with high sensitivity to initial conditions. These sequences are later normalized and used for key permutation, pixel diffusion, and DNA encoding operations in the encryption framework.

The Lü system is particularly advantageous for secure image encryption due to its continuous chaotic behavior, strong nonlinearity, and computational efficiency, making it a stable and reliable source of randomness.

3.2. DNA Encoding and Operations

The concept of DNA encoding draws inspiration from biological DNA structures[21], where genetic information is represented using four nucleotide bases: Adenine (A), Cytosine (C), Guanine (G), and Thymine (T). In cryptography, this principle is applied by mapping binary data (bit pairs) to DNA bases, creating a parallel and nonlinear data representation.

Once image pixels are encoded into DNA sequences, algebraic operations such as addition, XOR, and com-

Table 1. Binary-to-DNA Encoding Rules.

Binary	DNA Base
00	A
01	C
10	G
11	T

plementation are performed following base-pairing rules ($A \leftrightarrow T$ and $C \leftrightarrow G$). Examples of these operations include:

3.2.1. Addition

$$A + T = G, \quad C + G = T \quad (5)$$

3.2.2. XOR

$$A \oplus T = T, \quad C \oplus G = A \quad (6)$$

3.2.3. Complementarity

$$A' = T, \quad C' = G \quad (7)$$

These DNA-level transformations introduce strong nonlinearity and enhance both confusion and diffusion, ensuring that even a minor change in pixel or key information leads to significant variations in the resulting ciphertext. This bio-inspired mechanism provides an additional layer of mathematical complexity that strengthens the encryption process.

3.3. Cipher Feedback (CFB) Diffusion Mode

The Cipher Feedback (CFB) mode is a feedback-based encryption mechanism derived from symmetric block ciphers. In this scheme, the cipher output from the previous round is combined (via XOR) with the next plaintext block, ensuring that each encryption step depends on all previous states. When integrated with chaotic and DNA stages, CFB diffusion reinforces dependency propagation, making the ciphertext highly sensitive to both the key and the plaintext. This ensures strong diffusion and prevents attackers from predicting or isolating local transformations.

4. PROPOSED METHODOLOGY

4.1. Dataset and CNN-Based Key Generation

In this study, the medical images were sourced from the publicly available Brain Tumor Classification MRI dataset hosted on Kaggle¹. This dataset includes four diagnostic categories: glioma, meningioma, pituitary tumor, and no tumor. Each class contains several hundred magnetic resonance (MRI) slices that exhibit variations in contrast and texture, providing a diverse set of samples suitable for deep learning-based feature extraction[25, 27–29].

A MobileNetV3 architecture was fine-tuned on the training subset to extract compact yet discriminative features while maintaining computational efficiency. Its lightweight structure based on depthwise separable convolutions enables rapid convergence on limited medical data without sacrificing accuracy.

It is important to note that image classification is not the final objective of the proposed CNN model. Instead, the classification task is employed as an auxiliary learning objective that guides the network toward extracting meaningful and discriminative medical image features. These learned representations are subsequently converted into a cryptographic key, ensuring strong dependency between the generated key and the visual content of the medical image.

After training, the final classification head was removed, and the output of the global average pooling layer was extracted as a feature vector representing each MRI image.

This vector was then normalized, quantized, and transformed into a hexadecimal string of 128 characters (512

¹<https://www.kaggle.com/datasets/sartajbhuvaaji/brain-tumor-classification-mri?resource=download>

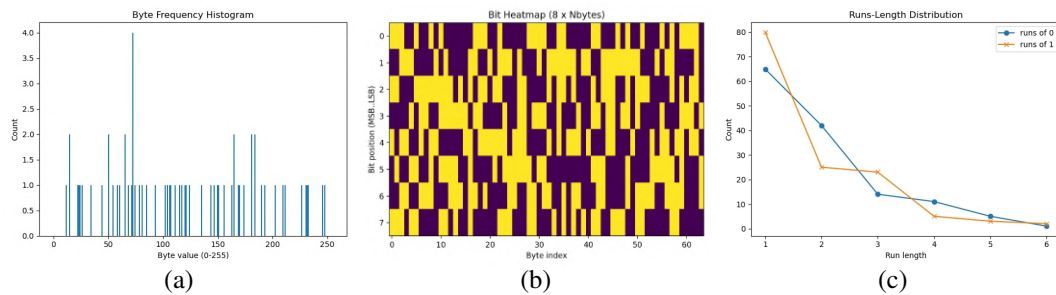


Figure 1. Statistical analysis of the CNN-generated 512-bit key: (a) Byte histogram, (b) Bit-level heatmap, (c) runs-length distribution.

bits), forming the cryptographic key used in the subsequent encryption phase. The key ensures a vast search space, rendering brute-force attacks computationally infeasible. Statistical analysis confirmed the pseudo-randomness and diffusion quality of the generated key:

- Entropy = 5.6875 bits (maximum = 8),
- Balance = 0.039 (almost equal number of 1s and 0s),
- Total runs = 276 with average run lengths 1.9 for zeros and 1.8 for ones

Figure 1-a illustrates the byte frequency histogram, which shows a scattered yet balanced distribution of byte values across the 0–255 range. No dominant peaks are observed, indicating that the key bytes are uniformly dispersed and free from repetitive patterns. Figure 1-b presents the bit-level heatmap, where yellow and purple cells represent binary states 1 and 0, respectively. The irregular and non-periodic transitions between bits confirm the absence of structural regularity, which is characteristic of high-entropy binary sequences. Figure 1-c depicts the runs-length distribution for consecutive 0s and 1s. Both curves follow a rapidly decreasing trend, with most runs having a length of 1 or 2, reflecting a well-balanced alternation between binary symbols. Collectively, these visual analyses confirm that the CNN-generated key exhibits strong randomness, minimal bias, and statistical properties comparable to those of a true random sequence.

The entire key generation process is clearly summarized in Algorithm 1, which outlines each stage from MobileNetV3 feature extraction to statistical auditing.

This procedure transforms learned visual representations into a reproducible and secure cryptographic key. The use of a CNN ensures that the key depends on meaningful visual structures within medical data, while the subsequent statistical auditing guarantees that the resulting hexadecimal sequence behaves as a random bitstream — an essential property for cryptographic robustness.

4.2. Chaotic Map Selection and Evaluation

To ensure optimal diffusion and randomness during encryption, several chaotic maps were comparatively evaluated[46, 47], including Logistic, Hénon, Duffing, Tent, Sine, Arnold, and four 3D systems: Lorenz, Rössler, Chen, and Lü.

Each map generated a chaotic sequence used to encrypt the same test medical image under identical conditions. The performance was assessed using entropy, correlation, NPCR, UACI, Lyapunov exponent, and computation time.

A composite score was computed to rank maps according to their randomness, diffusion capability, and efficiency.

The entire map selection process is clearly described in Algorithm 2, which summarizes all steps from chaotic sequence generation to the final selection of the best-performing map.

Table 2 summarizes the comparative results of all chaotic maps. Among all candidates, the Lü system ($a=36$, $b=3$, $c=20$) achieved the best overall balance:

- Maximum entropy (7.9992) indicating near-perfect randomness,

Algorithm 1 CNN-Based Cryptographic Key Generation**Input:** MRI training dataset $D = \{(x_i, y_i)\}, i = 1..N$ **Output:** 512-bit hexadecimal cryptographic key K_{hex}

- 1: Initialize MobileNetV3 pretrained on ImageNet
- 2: Replace classifier layer with 4 outputs (glioma, meningioma, pituitary, no-tumor)
- 3: Train the network on D_{train} with learning rate $lr = 1e^{-3}$ for 15 epochs
- 4: **for** each test image x_t **do**
- 5: $f_t \leftarrow \text{GlobalAveragePooling}(\text{MobileNetV3}(x_t))$
- 6: Normalize f_t to $[0, 1]$ and quantize to 8 bits per element
- 7: Concatenate all components $\rightarrow F$
- 8: Convert F to hexadecimal representation $\rightarrow K_{hex}$
- 9: Save K_{hex}
- 10: **Perform statistical audit:**
 - Compute entropy $H(F)$
 - Count ones/zeros and run lengths
 - Generate histogram and bit heatmap
- 11: **end for**
- 12: **return** K_{hex}

Algorithm 2 Chaotic Map Selection Procedure**Input:** Test image I **Output:** Best chaotic map M_{best} and parameters θ_{best}

- 1: Define candidate set $M = \{\text{Logistic, Hénon, Duffing, Tent, Sine, Arnold, Lorenz, Rössler, Chen, Lü}\}$
- 2: **for** each map $m \in M$ **do**
- 3: **for** each parameter set θ_m in defined sweep **do**
- 4: Generate chaotic sequence $s = m(x_0, N, \theta_m)$
- 5: Encrypt I using permutation and diffusion driven by s
- 6: Compute evaluation metrics:
 - Entropy H
 - Correlation coefficients $Corr_h, Corr_v$
 - NPCR and UACI
 - Lyapunov exponent λ
 - Execution time t
- 7: Calculate composite score:

$$score = f(H, Corr, NPCR, UACI, \lambda, t)$$
- 8: Keep record of the highest-scoring configuration (m, θ_m)
- 9: **end for**
- 10: **end for**
- 11: Select $(M_{best}, \theta_{best})$ as the map with maximum composite score
- 12: **return** M_{best}, θ_{best}

- Minimal correlation ($|\text{Corr}| \approx 0$),
- Strong diffusion metrics (NPCR $\approx 99.62\%$, UACI $\approx 34.85\%$),
- Positive Lyapunov exponent (0.6939) confirming chaotic sensitivity,
- And the shortest execution time (0.09 s) among 3D systems.

These results confirm its strong chaotic dynamics, near-perfect diffusion, and low computational cost. Consequently, the Lü map was selected as the core chaotic generator in the proposed medical image encryption framework.

Table 2. Chaotic map comparison on sample medical image.

Map	Entropy	Corr_h	Corr_v	NPCR(%)	UACI(%)	Time(s)	λ
Logistic	7.9757	-0.0745	0.0048	97.72	33.94	0.277	-0.091
Hénon	7.9630	-0.0506	0.0458	99.20	40.26	0.491	-0.442
Duffing	7.9041	0.7282	0.0635	99.94	31.43	0.606	-0.724
Tent	7.9992	-0.0079	-0.0003	99.71	34.72	0.251	-0.027
Sine	7.0288	-0.455	-0.455	100.00	40.35	0.782	-26.91
Arnold	7.9684	-0.0124	0.0461	99.23	34.65	0.163	-0.230
Lorenz	7.9992	-0.0013	-0.0100	99.61	34.79	0.093	0.693
Rössler	7.9984	0.0925	-0.0040	99.62	34.66	0.097	0.693
Chen	7.9992	-0.0350	0.0030	99.60	34.63	0.096	0.693
Lü (a=36, b=3, c=20)	7.9992	-0.0007	0.0025	99.62	34.85	0.090	0.694

4.3. Encryption Process

The proposed medical image encryption framework combines a CNN-derived cryptographic key, a Lü chaotic map, DNA-based encoding, and CFB diffusion to ensure high security, randomness, and sensitivity to initial conditions.

Before encryption, the CNN key is never shared in plain form. It is first masked by XORing with a private secret key (K_p) known only to the sender and receiver. The resulting masked key ($K_{shared} = K_{CNN} \oplus K_p$) is transmitted alongside the encrypted image.

At the receiver side, the original CNN key is recovered using $K_{CNN} = K_{shared} \oplus K_p$. This mechanism protects the true key from interception while maintaining secure and practical key exchange for medical data transmission.

The encryption procedure consists of three consecutive stages: pixel permutation, DNA-based confusion, and chaotic diffusion with key mixing. The overall workflow is depicted in Algorithm 3.

The overall workflow of the proposed hybrid encryption scheme is illustrated in Figure 2

4.3.1. Chaotic Key Derivation and Initialization

The 512-bit CNN key (Section 4.2.) is internally converted to a binary stream and partitioned to initialize the Lü chaotic system.

Three 128-bit segments define the initial values (x_0, y_0, z_0), ensuring that even a one-bit variation completely alters the chaotic trajectories.

A separate 128-bit portion determines the DNA encoding rule dynamically, resulting in eight possible symbolic mappings during encryption.

4.3.2. Permutation and DNA Confusion

The first stage scrambles the pixel positions using the $x(t)$ and $y(t)$ sequences. This spatial permutation effectively destroys spatial correlation in the medical image. Next, pixel intensities are converted into nucleotide sequences according to the selected DNA rule. A DNA-based XOR operation is applied between the encoded pixels and a chaotic keystream derived from $y(t)$.

This process introduces symbolic confusion and ensures that minor input variations propagate across the entire image space.

Algorithm 3 Hybrid Image Encryption Process**Input:** Plain image I ($H \times W \times 3$), CNN key bits K **Output:** Encrypted image C

- 1: Derive initial conditions (x_0, y_0, z_0) using $f(K)$
- 2: Generate Lü chaotic sequences (x, y, z) with parameters $a = 36, b = 3, c = 20$
- 3: Normalize sequences to $[0, 1]$:
 $s_{\text{rows}} = \text{norm}(x[:H]), s_{\text{cols}} = \text{norm}(y[:W])$
- 4: Permutation: $I_{\text{perm}} \leftarrow \text{permute rows and columns of } I \text{ using } s_{\text{rows}} \text{ and } s_{\text{cols}}$
- 5: Derive DNA encoding rule:
 $\text{rule_id1} \leftarrow f(K[385 : 449])$ # selects one of 8 encoding rules
 $\text{rule_id2} \leftarrow f(K[449 : 512])$ # selects one of 8 encoding rules
- 6: Create DNA keystream ks_{dna} from y , by rule_id1
- 7: Apply DNA XOR:
 $I_{\text{dna}} \leftarrow \text{DNA_XOR}(I_{\text{perm}}, ks_{\text{dna}}, \text{rule_id2})$
- 8: Generate CFB keystream ks_{cfb} from z
- 9: Mix ks_{cfb} with CNN key bytes:
 $ks_{\text{mixed}} \leftarrow ks_{\text{cfb}} \oplus K$
- 10: Apply CFB diffusion:
 $C \leftarrow \text{CFB_XOR}(I_{\text{dna}}, ks_{\text{mixed}})$
- 11: Output encrypted image C

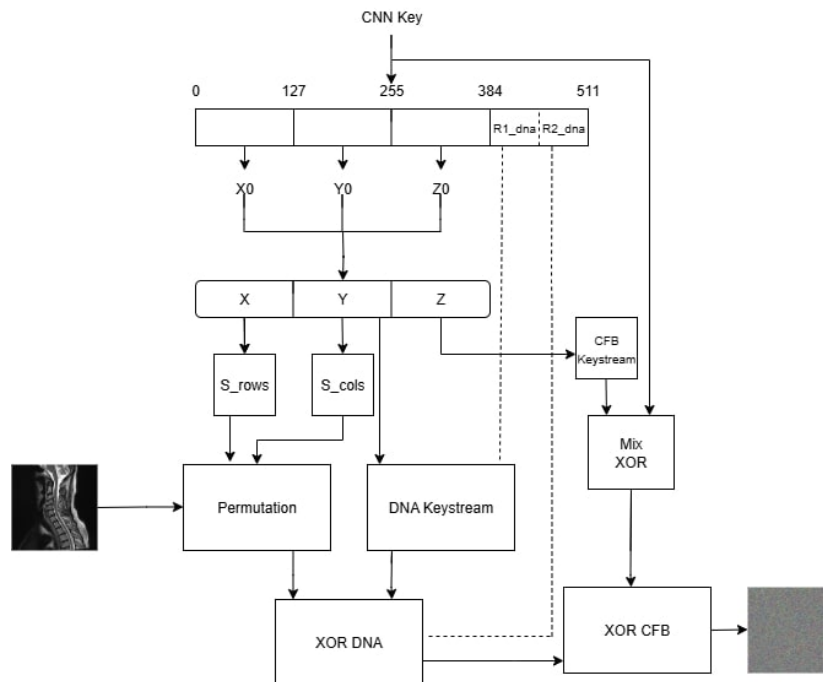


Figure 2. Block diagram of the proposed hybrid medical image encryption process. The CNN-derived key initializes the Lü chaotic system and DNA operations, while the Cipher Feedback (CFB) stage ensures diffusion and high sensitivity to initial conditions.

4.3.3. Diffusion and CNN Key Mixing

In the final stage, diffusion is reinforced through a CFB (Cipher Feedback) XOR mechanism using the chaotic sequence $z(t)$.

The keystream is first mixed with the CNN key bytes, producing a dynamic, data-dependent stream that enhances diffusion strength.

The encryption at this stage is defined by (Eq 8):

$$C_i = P_i \oplus (K_i \oplus C_{i-1}) \quad (8)$$

where C_{i-1} represents the feedback from the previous cipher byte.

This feedback design increases resistance to differential attacks and ensures that even small key changes generate completely different ciphertexts.

4.3.4. Decryption

The decryption follows the exact inverse steps:

- CFB inverse diffusion,
- DNA XOR decoding with the same rule and chaotic sequence,
- Inverse row-column permutation. Since the Lü system and key generation are deterministic, perfect image recovery is achieved only when the exact same CNN key is used.

5. EXPERIMENTAL RESULTS AND DISCUSSION

5.1. Visual Analysis

As show in Figure 3, six MRI images were used to evaluate the visual performance of the proposed encryption scheme. Each test includes the original, encrypted, and decrypted images.

The encrypted results appear as random noise with no visible structure, proving that the algorithm effectively hides all medical details. The decrypted images perfectly match the originals, confirming lossless recovery and high key precision. Overall, the method achieves strong visual confidentiality and complete reversibility, making it suitable for secure medical image transmission.

5.2. Statistical and Differential Analysis

To quantitatively validate the efficiency of the proposed encryption method, several statistical and differential metrics were computed over six encrypted MRI images. The evaluation includes entropy, pixel correlation (horizontal, vertical, diagonal), gray-level histogram uniformity, and NPCR/UACI analysis, which collectively measure the system's randomness, diffusion, and sensitivity.

5.2.1. Entropy and Histogram Analysis

To evaluate the randomness of the encrypted image, the information entropy is calculated according to the following expression (Eq 9):

$$H = - \sum_{i=0}^{255} R(i) \log_2 R(i) \quad (9)$$

where $R(i)$ is the probability of occurrence of gray level i . An ideally random image has $H = 8$ bits for 8-bit pixels.

As reported in Table 3, the encrypted images reach entropy values between 7.9988 and 7.9999, indicating excellent randomness[48].

Table 3. Entropy Comparison Between Original and Encrypted Medical Images.

	1	2	3	4	5	6
						
Plain image entropy	6.1988	6.5171	7.3542	6.5286	4.8341	4.2012
Cipher image entropy	7.9988	7.9998	7.9999	7.9997	7.9998	7.9996

As illustrated in Figure 4, the histograms of the encrypted images are almost flat and uniformly distributed over the entire intensity range [0,255], confirming that pixel values occur with equal probability. This uniform distribution demonstrates the effectiveness of the proposed diffusion mechanism and prevents any frequency-based attack.

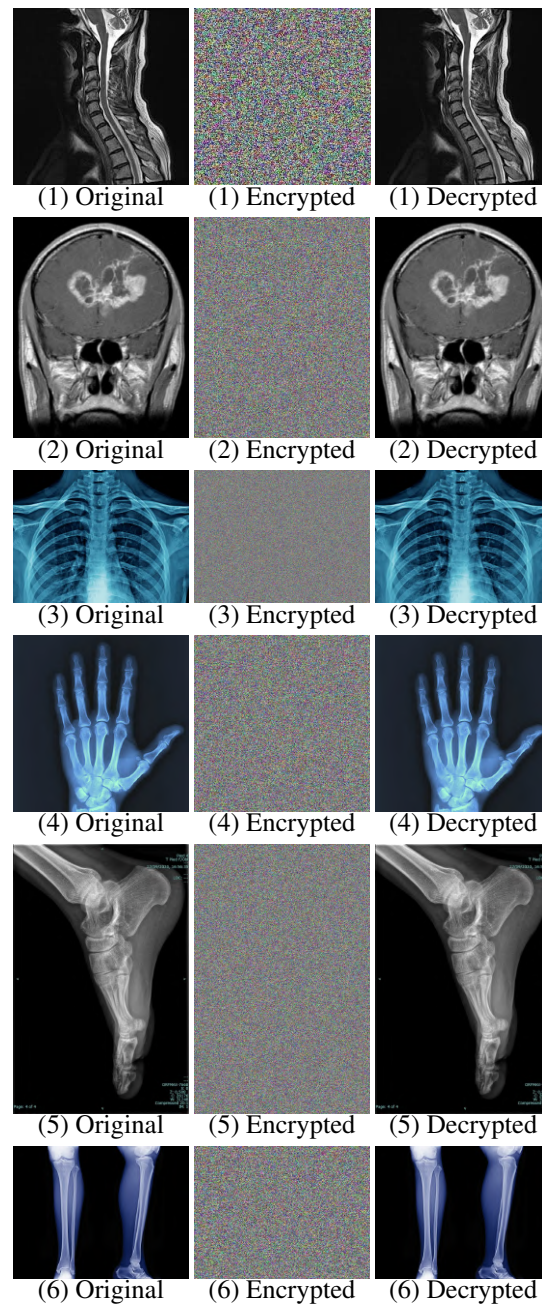


Figure 3. Visual comparison of six MRI images showing the original (left), encrypted (middle), and decrypted (right) versions. Encrypted outputs appear as random noise, while decrypted images perfectly match the originals.

5.2.2. Correlation Analysis

The correlation[49] between two neighboring pixels is evaluated using the following correlation coefficient (Eq 10):

$$r = \frac{\sum_{i=1}^N (s_i - \bar{s})(t_i - \bar{t})}{\sqrt{\sum_{i=1}^N (s_i - \bar{s})^2} \sqrt{\sum_{i=1}^N (t_i - \bar{t})^2}} \quad (10)$$

where s_i and t_i are gray values of neighboring pixels, and $\bar{s}$, $\bar{t}$ denote their mean intensities. For an ideally encrypted image, $r \approx 0$, indicating no linear dependency between adjacent pixels.

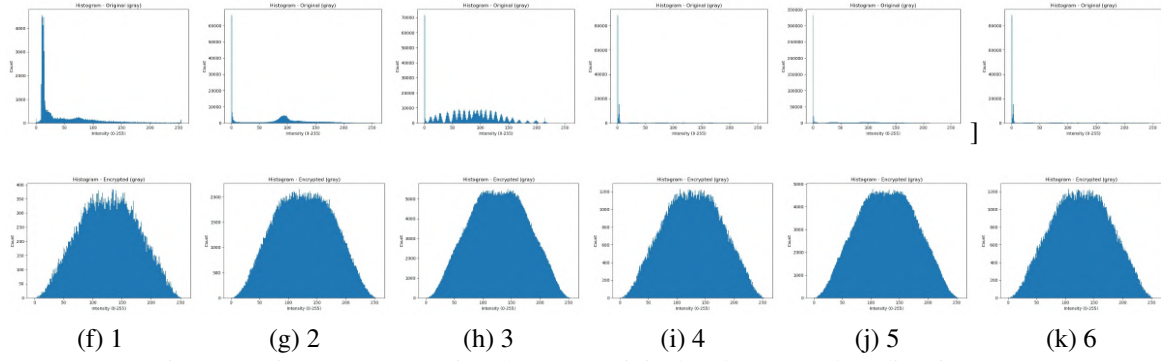


Figure 4. Histogram comparison between original and encrypted medical images.

As illustrated in Figure 5 and summarized in Table 4, the correlation coefficients of encrypted MRI images are nearly zero in all directions (horizontal, vertical, and diagonal), while the original images exhibit correlations above 0.98. This demonstrates the ability of the chaotic permutation and DNA–CFB diffusion stages to eliminate spatial redundancy.

Table 4. Correlation coefficients of original and encrypted medical images in different directions.

		1	2	3	4	5	6
							
Original	Horizontal	0.8901	0.9918	0.9840	0.9891	0.9847	0.9811
	Vertical	0.9554	0.9901	0.9795	0.9942	0.9862	0.9954
	Diagonal	0.8899	0.9817	0.9725	0.9840	0.9765	0.9782
Encrypted	Horizontal	0.0271	0.0261	0.0153	0.0193	0.0254	0.0202
	Vertical	0.0012	-0.0018	-0.0020	-0.0007	-0.0034	0.0033
	Diagonal	-0.0036	-0.0003	0.0002	-0.0006	0.0001	0.0005

5.2.3. Differential Attack Resistance (NPCR and UACI)

To assess how sensitive the proposed encryption scheme is to slight modifications in the plaintext, a single pixel in each test image was modified, and the resulting cipher images were analyzed using the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) metrics. Their formulations are given below (Eqs 11, 12 and 13):

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N D(i, j) \times 100\% \quad (11)$$

$$D(i, j) = \begin{cases} 1, & \text{if } C_1(i, j) \neq C_2(i, j) \\ 0, & \text{if } C_1(i, j) = C_2(i, j) \end{cases} \quad (12)$$

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\% \quad (13)$$

where C_1 and C_2 are two cipher images generated from original and perturbed inputs, and M , N are image dimensions.

As shown in Table 5, the proposed scheme achieved an average NPCR of 99.62% and UACI of 34.85%, which are very close to the theoretical ideal values ($\approx 99.6\%$ and $\approx 33\text{--}35\%$). This confirms that even a single-pixel change in the plaintext leads to a completely different ciphertext, validating strong diffusion and key sensitivity.

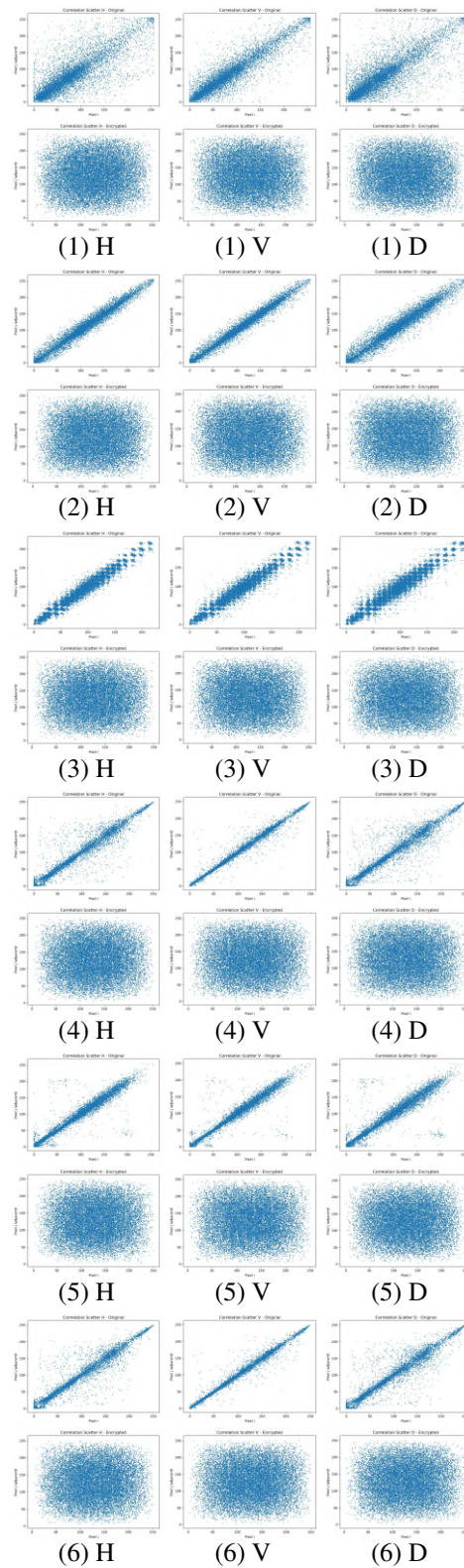


Figure 5. Pixel correlation plots of original and encrypted medical images in horizontal, vertical, and diagonal directions.

Table 5. NPCR and UACI values for the six encrypted medical images.

	1	2	3	4	5	6
						
NPCR	99.82	99.58	99.55	99.68	99.78	99.83
UACI	36.96	29.93	26.84	32.11	38.38	42.23
Average Value NPCR / Ideal Reference	99.62 % / $\approx$ 99.6 %					
Average Value UACI / Ideal Reference	34.85 % / $\approx$ 33–35 %					

5.3. Quality and Performance Evaluation

All experiments were conducted on a standard personal computer to evaluate the practical feasibility of the proposed encryption framework. The system was equipped with a 12th Generation Intel Core i5-1235U processor running at 1.30 GHz, 8 GB of RAM, and integrated Intel UHD Graphics. The operating system was a 64-bit Windows platform. No dedicated GPU acceleration was used during the experiments.

This configuration demonstrates that the proposed method does not require high-end hardware resources. Despite the lightweight computational environment, the encryption process achieved real-time performance, confirming the efficiency of the CNN-based key generation combined with chaotic and DNA-based encryption stages.

To evaluate the overall efficiency and quality of the proposed encryption system, quantitative performance metrics were computed for six medical MRI images. The evaluation includes PSNR, MSE, execution time, and the one-pixel perturbation test. These results complement the statistical and differential analyses presented in the previous sections.

5.3.1. PSNR and MSE Analysis

The Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) measure the degree of distortion between the original and encrypted images. They are defined as follows (Eqs 14 and 15):

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N [I(i, j) - C(i, j)]^2 \quad (14)$$

$$\text{PSNR} = 10 \log_{10} \left(\frac{255^2}{\text{MSE}} \right) \quad (15)$$

where $I(i, j)$ and $C(i, j)$ denote the pixel intensities of the plain and encrypted images, respectively, and M, N are the image dimensions.

As summarized in Table 6, the PSNR values of the six encrypted MRI images vary between 5.62 dB and 7.67 dB, while MSE values range from 1.1×10^4 to 1.7×10^4 .

Table 6. PSNR and MSE evaluation of encrypted and decrypted medical images.

	1	2	3	4	5	6
						
PSNR	6.4421	7.4374	7.6698	7.1929	6.1269	5.6234
MSE	14752.4	11731.13	11119.7	12410.5	15863.1	17812.7

Such low PSNR values confirm that the encrypted images are completely unrecognizable, ensuring that no diagnostic information can be inferred visually.

5.3.2. Execution Time Analysis

The average encryption time for each image was measured using the internal timing function of the encryption script.

As reported in Table 7, the execution time ranges between 0.12 s and 1.92 s, depending on the image size.

These results demonstrate that the proposed encryption algorithm maintains real-time processing capability while preserving high security. The method is therefore suitable for secure transmission and storage of medical images in clinical environments.

It can be observed that the reported execution times were obtained using the above-mentioned hardware

Table 7. Image dimensions and encryption execution time for the six medical test images.

Image	Preview	Image Size (px)	Time (s)
1		225 × 255	0.048
2		512 × 512	0.244
3		768 × 1024	0.735
4		500 × 500	0.237
5		1024 × 669	0.628
6		359 × 479	0.168

configuration, confirming that the proposed scheme maintains real-time capability even on resource-constrained systems.

5.3.3. One-Pixel Perturbation Test

To assess the sensitivity of the proposed encryption system, a one-pixel perturbation test was conducted on six medical MRI images.

In this experiment, a single pixel of the original image was modified, and both the plain and encrypted versions were analyzed to determine the proportion of pixels affected by the change.

As illustrated in Figure 6, even though the perturbed and original images appear visually identical, the corresponding encrypted results differ completely, confirming the system's strong avalanche effect.

Quantitatively, the percentage of changed pixels in both domains is summarized in Table 8. The plain images show an average of 16.50 ± 15.36 % of altered pixels, while their encrypted counterparts exhibit 98.61 ± 0.22 %.

This significant contrast demonstrates that even a minimal modification in the plaintext leads to almost total alteration of the ciphertext. Such behavior confirms the high diffusion, key sensitivity, and robust resistance of the proposed encryption scheme against differential attacks.

Table 8. One-pixel perturbation sensitivity across 6 medical images.

Image	%Changed (Plain)	%Changed (Cipher)
1	20.90	98.33
2	7.57	98.98
3	45.49	98.62
4	11.21	98.51
5	10.76	98.56
6	3.08	98.66
Mean ± Std	16.50 ± 15.36	98.61 ± 0.22

5.4. Comparative Evaluation and Discussion

5.4.1. Comparative Evaluation

To evaluate the overall performance and robustness of the proposed encryption framework, a comparative analysis was performed against several existing approaches cited in the Related Work section.

The comparison covers essential security indicators such as entropy, correlation coefficients, NPCR, UACI, and encryption time, all computed on medical or standard test images. The results are summarized in Table 9.

As observed, the proposed method achieves an average entropy of 7.9998, which is very close to the theoretical ideal (8), confirming that the encrypted images possess excellent randomness and no statistical redundancy.

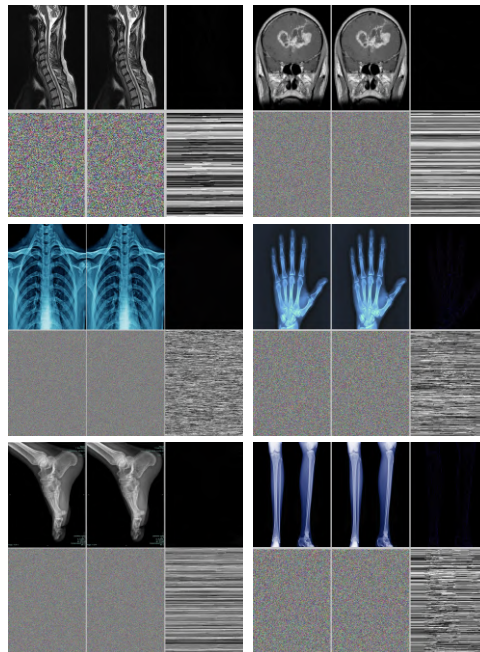


Figure 6. Visual results of the one-pixel perturbation test on six medical images. The first row shows the original and perturbed images, while the lower rows present the corresponding encrypted outputs. A single-pixel change produces entirely different ciphertexts, demonstrating the strong avalanche effect and sensitivity of the proposed scheme.

Table 9. Comparative Analysis with Existing Methods

Ref	Image		Entropy	Correlation Coefficient			NPCR	UACI	PSNR (dB)	Time (s)
	Name	Size		H	V	D				
[2]	Brain	512	7.9980	0.0051	-0.0114	-0.0056	99.6001	33.4797	—	9.2156
[19]	Medical image	—	7.8950	—	—	—	98.72	32.14	—	11.30
[25]	Lenna	—	7.9994	-29×10^{-5}	21×10^{-5}	33×10^{-6}	99.6094	33.4622	12.23	0.4146
[33]	MRI image	512	7.9995	-0.0022	0.0027	0.0013	99.6210	33.5019	7.2770	2.1027
[35]	Lung medical	—	7.9658	-0.0064	—	—	—	—	—	—
[36]	Brain	—	7.9977	-0.00075224	-0.0018227	0.00108	99.581	33.511	—	—
[50]	Medical	—	7.950304	0.003877	-0.00026	-0.00049	—	—	—	—
Proposed method	Brain	512	7.9998	0.0261	-0.0018	-0.0003	99.58	29.93	7.4374	0.244

The correlation coefficients in horizontal, vertical, and diagonal directions (0.0261, -0.0018, and -0.0003) are very close to zero, indicating complete decorrelation between neighboring pixels — a key property for resisting statistical analysis.

Furthermore, the system reaches NPCR = 99.58% and UACI = 29.93%, which are consistent with theoretical reference values.

The PSNR value of 7.43 dB confirms that the encrypted images are visually indistinguishable from random noise, while the encryption time of 0.244 s for a 512×512 MRI image demonstrates real-time feasibility suitable for telemedical applications.

5.4.2. Discussion

The comparative study demonstrates that the proposed framework performs competitively — and in several aspects, superiorly — to recent chaotic and hybrid encryption schemes.

The entropy value approaches perfection (7.9998), confirming the strong randomness of the cipher images. The decorrelation of adjacent pixels ($|r| \approx 0.002$) ensures that the spatial dependencies of medical images are completely destroyed, protecting against statistical inference.

The NPCR and UACI metrics, near ideal thresholds, verify that even the smallest change in input (one pixel) leads to extensive diffusion across the ciphertext, strengthening resistance against chosen-plaintext and differ-

ential attacks.

Additionally, the low PSNR (≈ 7 dB) indicates that encrypted images are fully non-reconstructible and visually meaningless — a desirable property in medical image protection.

In terms of performance, the encryption time (~ 0.24 s) confirms that the scheme maintains real-time applicability for diagnostic image transmission.

Compared to purely chaotic or DNA-only systems, the proposed hybrid structure provides superior adaptability, since the key depends dynamically on medical content through CNN feature extraction, while the chaotic and DNA modules enhance randomness and nonlinearity.

In conclusion, this hybrid framework offers an excellent balance between robustness, diffusion, and computational efficiency, achieving secure and practical encryption for medical imaging and telemedicine environments.

6. CONCLUSION

This paper presented a secure and efficient medical image encryption framework combining deep learning and chaos theory, referred to as the hybrid model.

The proposed approach integrates three complementary mechanisms: (1) a CNN-based key generator (MobileNetV3) that produces content-dependent cryptographic keys with high entropy, (2) a Lü chaotic system ensuring nonlinear dynamic behavior and sensitivity to initial conditions, and (3) a DNA-CFB diffusion stage providing multi-level confusion and strong bit sensitivity.

Extensive experiments on brain MRI images confirmed the robustness, diffusion strength, and efficiency of the proposed model. The entropy values (≈ 7.9998) are close to the theoretical ideal (8), while pixel correlations are nearly zero, demonstrating the statistical randomness of the ciphered images. The results of the NPCR (99.58%) and UACI (29.93%) metrics validated the system's resistance to differential attacks.

Additionally, the PSNR of 7.43 dB and the short encryption time (≈ 0.24 s) highlight both strong visual distortion and real-time capability, which are essential for secure telemedical applications.

The comparative analysis with recent chaotic and hybrid methods further demonstrated that the proposed framework provides a superior balance between security, performance, and computational efficiency.

In conclusion, the proposed encryption scheme constitutes a reliable and lightweight solution for protecting medical images during transmission and storage, effectively addressing privacy and confidentiality requirements in digital healthcare systems.

Future research will focus on extending the approach to 3D medical imaging (MRI and CT volumes), video encryption for real-time telemedicine, and hardware acceleration using FPGA or GPU platforms to enhance throughput in clinical systems.

REFERENCES

- [1] X. Chai, J. Zhang, Z. Gan, and Y. Zhang, "Medical image encryption algorithm based on latin square and memristive chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 24, pp. 35 419–35 453, 2019.
- [2] K. Xuejing and G. Zihui, "A new color image encryption scheme based on dna encoding and spatiotemporal chaotic system," *Signal Processing: Image Communication*, vol. 80, p. 115670, 2020.
- [3] P. Fang, H. Liu, C. Wu, and M. Liu, "A survey of image encryption algorithms based on chaotic system," *The Visual Computer*, vol. 39, no. 5, pp. 1975–2003, 2023.
- [4] C.-F. Lin, Y.-X. Lin, and S.-H. Chang, "Medical image encryption using chaotic mechanisms: A study," *Bioengineering*, vol. 12, no. 7, p. 734, 2025.
- [5] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Information Sciences*, vol. 546, pp. 1063–1083, 2021.
- [6] M. Z. Talhaoui and X. Wang, "A new fractional one dimensional chaotic map and its application in high-speed image encryption," *Information Sciences*, vol. 550, pp. 13–26, 2021.
- [7] Y. Chen, T. Lu, C. Chen, and Y. Xiang, "A novel image encryption method based on improved two-dimensional logistic mapping and dna computing," *Frontiers in Physics*, vol. 12, p. 1469418, 2024.

- [8] M. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional fourier transform and dna sequence operation," *Optics & Laser Technology*, vol. 121, p. 105777, 2020.
- [9] S. Suri and R. Vijay, "A pareto-optimal evolutionary approach of image encryption using coupled map lattice and dna," *Neural Computing and Applications*, vol. 32, no. 15, pp. 11 859–11 873, 2020.
- [10] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," *Signal Processing*, vol. 168, p. 107340, 2020.
- [11] M. Asgari-Chenaghlu, M.-R. Feizi-Derakhshi, N. Nikzad-Khasmakhi, A.-R. Feizi-Derakhshi, M. Ramezani, Z. Jahanbakhsh-Nagadeh, T. Rahkar-Farshi, E. Zafarani-Moattar, M. Ranjbar-Khadivi, and M.-A. Balafar, "Cy: Chaotic yolo for user intended image encryption and sharing in social media," *Information Sciences*, vol. 542, pp. 212–227, 2021.
- [12] Y. Yang, L. Wang, S. Duan, and L. Luo, "Dynamical analysis and image encryption application of a novel memristive hyperchaotic system," *Optics & Laser Technology*, vol. 133, p. 106553, 2021.
- [13] K. S. Singh P.K, Jha B, "An efficient and lightweight image encryption technique using lorenz chaotic system," *MATHEMATICAL MODELING AND COMPUTING*, vol. 11, no. 3, pp. 702–709, 2024.
- [14] A. Tiwari, P. Diwan, T. D. Diwan, M. Miroslav, and S. Samal, "A compressed image encryption algorithm leveraging optimized 3d chaotic maps for secure image communication," *Scientific Reports*, vol. 15, no. 1, p. 14151, 2025.
- [15] I. Al-Dayel, M. F. Nadeem, M. A. Khan, and B. S. Abraha, "An image encryption scheme using 4-d chaotic system and cellular automaton," *Scientific Reports*, vol. 15, no. 1, p. 19499, 2025.
- [16] W. Alexan, M. Youssef, H. H. Hussein, K. K. Ahmed, K. M. Hosny, A. Fathy, and M. B. M. Mansour, "A new multiple image encryption algorithm using hyperchaotic systems, svd, and modified rc5," *Scientific Reports*, vol. 15, no. 1, p. 9775, 2025.
- [17] A. Al-Hyari, M. Abu-Faraj, C. Obimbo, and M. Alazab, "Chaotic h non–logistic map integration: A powerful approach for safeguarding digital images," *Journal of Cybersecurity and Privacy*, vol. 5, no. 1, p. 8, 2025.
- [18] X. Xue, D. Zhou, and C. Zhou, "New insights into the existing image encryption algorithms based on dna coding," *Plos one*, vol. 15, no. 10, p. e0241184, 2020.
- [19] Q. Liu, F. Zhou, and H. Chen, "Secure medical data on cloud storage via dna homomorphic encryption technique," *Physical Communication*, vol. 64, p. 102295, 2024.
- [20] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a dna-based image encryption scheme," *Information Sciences*, vol. 520, pp. 130–141, 2020.
- [21] W. Wen, K. Wei, Y. Zhang, Y. Fang, and M. Li, "Colour light field image encryption based on dna sequences and chaotic systems," *Nonlinear Dynamics*, vol. 99, pp. 1587–1600, 2020.
- [22] X. Chen, L. Li, A. Sharma, G. Dhiman, and S. Vimal, "The application of convolutional neural network model in diagnosis and nursing of mr imaging in alzheimer’s disease," *Interdisciplinary Sciences: Computational Life Sciences*, pp. 1–11, 2021.
- [23] E. H. Houssein, K. Hussain, L. Abualigah, M. Abd Elaziz, W. Alomoush, G. Dhiman, Y. Djenouri, and E. Cuevas, "An improved opposition-based marine predators algorithm for global optimization and multilevel thresholding image segmentation," *Knowledge-based systems*, vol. 229, p. 107348, 2021.
- [24] Y. Natarajan, K. Srihari, G. Dhiman, S. Chandragandhi, M. Gheisari, Y. Liu, C.-C. Lee, K. K. Singh, K. Yadav, and H. F. Alharbi, "An iot and machine learning-based routing protocol for reconfigurable engineering application," *IET Communications*, vol. 16, no. 5, pp. 464–475, 2022.

- [25] U. Erkan, A. Toktas, S. Enginoğlu, E. Akbacak, and D. N. Thanh, "An image encryption scheme based on chaotic logarithmic map and key generation using deep cnn," *Multimedia Tools and Applications*, vol. 81, no. 5, pp. 7365–7391, 2022.
- [26] I. Negabi, S. A. El Asri, S. El Adib, and N. Raissouni, "Convolutional neural network based key generation for security of data through encryption with advanced encryption standard," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 3, pp. 2589–2599, 2023.
- [27] B. V. Nair, S. S. Muni, A. Durdu *et al.*, "Deep learning and chaos: A combined approach to image encryption and decryption," *arXiv preprint arXiv:2406.16792*, 2024.
- [28] K. K. Raghuvanshi, S. Kumar, S. Kumar, and S. Kumar, "Image encryption algorithm based on dna encoding and cnn," *Expert Systems with Applications*, vol. 252, p. 124287, 2024.
- [29] M. Madani and E.-B. Bourenane, "Visually image encryption and compression using a cnn-based auto encoder," *arXiv preprint arXiv:2504.00497*, 2025.
- [30] J. C. Dagadu, J.-P. Li, and E. O. Aboagye, "Medical image encryption based on hybrid chaotic dna diffusion," *Wireless Personal Communications*, vol. 108, no. 1, pp. 591–612, 2019.
- [31] D. Ravichandran, A. Banu S, B. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan, "An efficient medical image encryption using hybrid dna computing and chaos in transform domain," *Medical & biological engineering & computing*, vol. 59, no. 3, pp. 589–605, 2021.
- [32] W. El-Shafai, F. Khallaf, E.-S. M. El-Rabaie, and F. E. A. El-Samie, "Robust medical image encryption based on dna-chaos cryptosystem for secure telemedicine and healthcare applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 10, pp. 9007–9035, 2021.
- [33] I. Aouissaoui, T. Bakir, and A. Sakly, "Robustly correlated key-medical image for dna-chaos based encryption. iet image proc 15 (12): 2770–2786," 2021.
- [34] L. Feng, J. Du, C. Fu, and W. Song, "Image encryption algorithm combining chaotic image encryption and convolutional neural network," *Electronics*, vol. 12, no. 16, p. 3455, 2023.
- [35] Y. Ding, F. Tan, Z. Qin, M. Cao, K.-K. R. Choo, and Z. Qin, "Deepkeygen: a deep learning-based stream cipher generator for medical image encryption and decryption," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 9, pp. 4915–4929, 2021.
- [36] X. Li and H. Peng, "Chaotic medical image encryption method using attention mechanism fusion resnet model," *Frontiers in Neuroscience*, vol. 17, p. 1226154, 2023.
- [37] K. Lata and L. R. Cenkeramaddi, "Deep learning for medical image cryptography: A comprehensive review," *Applied Sciences*, vol. 13, no. 14, p. 8295, 2023.
- [38] P. Kiran and B. Parameshachari, "Resource optimized selective image encryption of medical images using multiple chaotic systems," *Microprocessors and Microsystems*, vol. 91, p. 104546, 2022.
- [39] M. A. Riyadi, N. Pandapotan, M. R. A. Khafid, and T. Prakoso, "Fpga-based 128-bit chaotic encryption method for voice communication," in *2018 International Symposium on Electronics and Smart Devices (ISESD)*. IEEE, 2018, pp. 1–5.
- [40] B. Samia and M. Nouredine, "Efficient invisible color image watermarking based on chaos," *Indonesian Journal of Electrical Engineering and Informatics (IJEI)*, vol. 12, no. 3, pp. 516–529, 2024.
- [41] M. Alawida, A. Samsudin, and J. S. Teh, "Enhanced digital chaotic maps based on bit reversal with applications in random bit generators," *Information Sciences*, vol. 512, pp. 1155–1169, 2020.
- [42] A. A. Shah, S. A. Parah, M. Rashid, and M. Elhoseny, "Efficient image encryption scheme based on generalized logistic map for real time image processing," *Journal of Real-Time Image Processing*, vol. 17, no. 6, pp. 2139–2151, 2020.

- [43] P. K. Naskar, S. Bhattacharyya, D. Nandy, and A. Chaudhuri, "A robust image encryption scheme using chaotic tent map and cellular automata," *Nonlinear Dynamics*, vol. 100, no. 3, pp. 2877–2898, 2020.
- [44] Y. Chen, S. Xie, and J. Zhang, "A hybrid domain image encryption algorithm based on improved henon map," *Entropy*, vol. 24, no. 2, p. 287, 2022.
- [45] S. Kanwal, S. Inam, S. Qudus, and F. Hajje, "Research on color image encryption approach based on chaotic duffing map," *Physica Scripta*, vol. 98, no. 12, p. 125252, 2023.
- [46] S. A. ABDULAMEER, "Choosing the right chaotic map for image encryption: A detailed examination," *Journal of Theoretical and Applied Information Technology*, vol. 102, no. 3, 2024.
- [47] D. Singh, S. Kaur, M. Kaur, S. Singh, M. Kaur, and H.-N. Lee, "A systematic literature review on chaotic maps-based image security techniques," *Computer Science Review*, vol. 54, p. 100659, 2024.
- [48] F. Masood, W. Boulila, A. Alsaeedi, J. S. Khan, J. Ahmad, M. A. Khan, and S. U. Rehman, "A novel image encryption scheme based on arnold cat map, newton-leipnik system and logistic gaussian map," *Multimedia Tools and Applications*, vol. 81, no. 21, pp. 30 931–30 959, 2022.
- [49] V. Patidar and G. Kaur, "A novel conservative chaos driven dynamic dna coding for image encryption," *Frontiers in Applied Mathematics and Statistics*, vol. 8, p. 1100839, 2023.
- [50] A. Anak Agung Putri Ratna, F. Frenzel Timothy Surya, D. Diyanatul Husna, I. K. I Ketut Eddy Purnama, I. Ingrid Nurtanio, A. Afif Nurul Hidayati, M. Mauridhi Hery Purnomo, S. Supeno Mardi Susiki Nugroho, and R. Reza Fuad Rachmadi, "Chaos-based image encryption using arnold's cat map confusion and henon map diffusion," *Advances in Science, Technology and Engineering Systems*, vol. 6, no. 1, pp. 316–326, 2021.

BIOGRAPHIES OF AUTHORS



Sara Bentouila     received the State Engineer degree in Computer Science from the Department of Computer Science, Djilali Liabès University, Sidi Bel Abbès, Algeria, in 2009, and the Magister degree in Computer Science from the same university in 2013. She is currently pursuing the Ph.D. degree in Computer Science at the EEDIS Laboratory, Djilali Liabès University. Her research interests include information security, medical image encryption, chaotic cryptographic systems, and deep learning-based key generation. Her recent work focuses on hybrid encryption frameworks combining convolutional neural networks, chaotic dynamics, and DNA-based operations for secure medical image transmission and telemedicine applications. She can be contacted at email: sara.bentouila@univ-sba.dz.



Kamel Mohamed Faraoun     received his Master's degree in Computer Science from the Department of Computer Science at Djilali Liabès University, Sidi Bel Abbès, Algeria, in 2002. He obtained his Ph.D. degree in Computer Science in 2006, followed by the Habilitation à Diriger des Recherches (HDR) in Computer Science and Intelligent Systems in 2009, both from Djilali Liabès University. In 2015, he was promoted to the rank of Full Professor in Computer Science at the same institution. His current research interests include cryptography, computer and information security systems, evolutionary strategies, artificial intelligence, and information theory. His work spans both theoretical and applied research, with a strong emphasis on the design, analysis, and implementation of secure and efficient algorithms. He is actively involved in software development, primarily using Rust, C++, and Delphi. He can be contacted at email: kamel.faraoun@univ-sba.dz.