Albahit Journal of Applied Sciences
"open-access, peer-reviewed biannual journal"
eISSN: 2708-8936, pISSN: 2708-244X
Volume 5, Issue 2, 2026
Page No: 01-30
***Website**: https://albahitjas.com.ly/index.php/albahit/en/index*

Deep Feature–Driven Chaotic Encryption for Secure Medical Image Transmission A Comparative CNN-Based Framework

Najway M. Yaqah [1*], Atigah E. Karnaf [2]
[1,2] Department of Computer Engineering, College of Electronic Technology, Bani Walid, Libya
[*]*Corresponding author:* najwawanis210@gmail.com

Received: 07-01-2026	**Accepted:** 18-03-2026	**Published:** 05-04-2026

Copyright: © 2026 by the authors. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Abstract:
Secure medical image transmission is a critical requirement in modern telemedicine. This paper proposes a robust hybrid encryption framework that integrates deep feature extraction with chaotic cryptography. Unlike conventional methods, encryption parameters are derived directly from high-level features extracted by pretrained CNNs (ResNet50, AlexNet, and MobileNetV2) to initialize a Logistic Map. This content-dependent key generation enhances resistance against brute-force and differential attacks. Experimental results across multiple modalities (X-ray, MRI, and Color images) demonstrate near-ideal security metrics: NPCR > 99.7% , UACI ≈ 33.3%, and Entropy ≈ 7.63. Robustness analysis confirms successful diagnostic recovery PSNR reached 22.92 dB under Salt-and-Pepper noise attacks, while occlusion recovery achieved 14.35 dB Comparative analysis reveals that while ResNet50 offers maximum sensitivity, MobileNetV2 achieves a 36.5% reduction in execution time, making it ideal for real-time clinical applications. The framework, implemented via MATLAB App Designer, provides secure and computationally efficient encryption with lossless decryption under ideal conditions for next-generation healthcare infrastructures.

Keywords: Capacitor Switching, Energization Transient, Overvoltage, Inrush Current, ATP/EMTP, Power System Transients, Sensitivity Analysis, Back-to-Back Switching.

التشفير الفوضوي المعتمد على السمات العميقة لنقل الصور الطبية بشكل آمن: إطار مقارن قائم على الشبكات العصبية الالتفافية (*CNN*)

نجوى ياقة [1*]، عتيقة كرناف [2]
[2،1] كلية التقنية الإلكترونية، قسم هندسة الحاسوب، بني وليد، ليبيا

الملخص
يُعدّ النقل الآمن للصور الطبية متطلبًا أساسيًا في أنظمة الطب عن بُعد الحديثة. تقترح هذه الورقة إطارًا هجينًا قويًا لتشفير الصور يجمع بين استخراج السمات العميقة والتشفير الفوضوي. وعلى خلاف الأساليب التقليدية، تُشتق معاملات التشفير مباشرةً من السمات عالية المستوى المستخرجة باستخدام شبكات عصبية التفافية مدرَّبة مسبقًا (ResNet50 وAlexNet وMobileNetV2) لتهيئة خريطة لوجستية (Logistic Map). يعزّز هذا التوليد المعتمد على محتوى الصورة مقاومة النظام لهجمات القوة الغاشمة والهجمات التفاضلية. أظهرت النتائج التجريبية عبر عدة أنماط تصوير (الأشعة السينية، والرنين المغناطيسي، والصور الملونة) تحقيق مقاييس أمان شبه مثالية، حيث تجاوزت قيمة NPCR نسبة 99.7%، وبلغت UACI نحو 33.3%، في حين اقتربت الإنتروبيا من 7.63. كما أكد تحليل المتانة إمكانية الاستعادة التشخيصية الناجحة، إذ بلغت قيمة PSNR نحو 22.92 ديسيبل تحت هجمات ضوضاء الملح والفلفل، بينما حققت استعادة المناطق المحجوبة قيمة 14.35 ديسيبل. وأظهر التحليل المقارن أنه في حين يوفر ResNet50 أعلى حساسية، فإن MobileNetV2 يحقق انخفاضًا في زمن التنفيذ بنسبة 36.5%، مما يجعله مناسبًا للتطبيقات السريرية الآنية. وقد تم تنفيذ الإطار باستخدام MATLAB App

Designer، حيث يوفر تشفيرًا آمنًا وكفؤًا حسابيًا مع فك تشفير غير فاقد للمعلومات في الظروف المثالية، بما يدعم متطلبات البنى التحتية الصحية من الجيل القادم.

الكلمات المفتاحية: تشفير الصور الطبية، استخراج السمات العميقة، الخريطة اللوجستية، الهجمات التفاضلية، التشفير الفوضوي، أمن الطب عن بُعد.

Introduction

In the context of the rapid digital transformation sweeping the global healthcare sector, medical images play a central role in modern diagnostic workflows and the heart of medical decision-making. With the widespread adoption of telemedicine systems and electronic health records, billions of sensitive diagnostic images—from MRI, CT, and X-ray scans—are transmitted across potentially vulnerable communication channels [1, 2]. These images carry a dual significance: firstly, they represent vital medical records where patient outcomes can hinge on their accuracy and confidentiality, and secondly, they contain personally identifiable data whose breach constitutes a blatant violation of human privacy [3].

Standards like AES and DES treat an image as an abstract binary stream, ignoring the high spatial correlation between neighboring pixels, the homogeneity of large regions within them, and the enormous volume of data that necessitates a precise balance between cryptographic strength and computational efficiency, despite their robustness with textual data [4, 5]. Because of this flaw, there is a security vulnerability that attackers can take advantage of by using advanced statistical analysis to find hidden patterns in static encryption [6, 7]. As a result, traditional encryption systems face structural challenges when applied to medical images.

In contrast, chaos-based encryption algorithms have emerged as a viable alternative, taking advantage of their great sensitivity to beginning conditions and pseudo-random nature [8, 9]. However, the majority of these systems continue to use a static model: a single encryption key applied to a variety of images, leaving them vulnerable to knownplaintext and chosen-plaintext assaults [10,11]. The central subject of this study is how encryption may be changed from a blind, uniform procedure to an intelligent system that identifies the uniqueness of each image and creates individual security for it.

This study presents an innovative answer through the organic integration of artificial intelligence depth and dynamical systems chaos. We introduce a hybrid encryption system that employs three distinct pre-trained CNN models— ResNet50, AlexNet, and MobileNetV2— as intelligent eyes to discern the unique anatomical fingerprint of each medical image, transforming it into a high-dimensional feature vector [12, 13]. Then, the Logistic Chaotic Map takes over, weaving from this vector a living encryption key that breathes with the image's content—where its initial parameters (x_0 and r) are derived directly from the extracted deep features [14, 15]. The study provides a comparative analysis of these three architectures to evaluate their impact on encryption performance, security, and computational efficiency.

The proposed system boasts several qualitative advantages:

- Content-sensitive encryption: Any minor change in the image generates a radically different key[16].

- Intelligent attack resistance: Statistical or differential attacks become infeasible against an inherently variable system[17].

- Practical balance: Achieves near-ideal security while maintaining encryption efficiency suitable for real-time applications[18].

- Exceptional flexibility: Adaptability to different types of medical images and the varying needs of healthcare systems [19].

This paper contributes to bridging a critical research gap between the fields of information security and applied artificial intelligence, presenting a model capable of protecting not only patient data but also the diagnostic content itself from tampering or theft [20, 21]. Through comprehensive analyses including entropy metrics, correlation coefficients, and NPCR/UACI tests, we demonstrate that the system achieves security levels surpassing current hybrid systems [22, 23], with notable resistance to noise and partial distortion [24]. Furthermore, we compare the performance of ResNet50, AlexNet, and MobileNetV2 in terms of execution time and security metrics to identify the most suitable architecture for different clinical applications. This research arrives at a pivotal time, as World Health Organization estimates indicate that over 70% of healthcare institutions in developing countries face annual cyberattacks [25], while regulations such as GDPR and HIPAA impose severe penalties for patient data breaches [26, 27] . Thus, the value of the system extends beyond the academic sphere to being a practical contribution toward building a secure digital infrastructure for the healthcare sector, ensuring information confidentiality without compromising its integrity or hindering timely access by specialists.

LITERATURE REVIEW

The security of medical images has evolved through three overlapping paradigms: traditional encryption, chaos-based encryption, and the emerging hybrid intelligent encryption paradigm. This review critically examines the strengths and limitations of each, establishing the necessity for the content-aware, feature-driven model proposed in this work.

A. Traditional Encryption Standards and Their Limitations for Images

Classical symmetric algorithms such as the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) form the backbone of general data security [28, 29]. Based on intricate substitution-permutation networks, their cryptographic resilience has been demonstrated for both textual and structured data. However, fundamental limitations arise when applying them to digital images, particularly high-volume, high-redundancy medical imaging:

1) *Ignorance of Image Semantics:* These algorithms ignore an image's high spatial correlation, low entropy regions (such uniform backgrounds in X-rays), and large data size, treating it as a passive binary stream. This results in a discrepancy between the information density of the image and the encryption effort [30, 31].

2) *Vulnerability to Statistical Analysis:* The encrypted output can retain statistical patterns of the original image, making it susceptible to histogram analysis, correlation analysis, and differential attacks. Studies by [32, 33] demonstrated that AES in ECB mode on medical images exhibits measurable correlation coefficients (>0.05) in the resulting cipher images, revealing its inadequacy for this data type.

3) *Computational Overhead:* Full-grade encryption of high-resolution volumetric data (e.g., 3D MRI scans) using these standards can impose significant latency, conflicting with the real-time demands of telemedicine and emergency diagnostics [34, 35].

B. The Rise of Chaos-Based Encryption

In the 1990s, chaos theory was incorporated into image encryption to overcome the shortcomings of conventional cryptography. Chaotic systems are naturally suited for encryption because of their great sensitivity to beginning conditions, ergodicity, and pseudo-randomness.

a) Core Techniques: For pixel scrambling (permutation) and diffusion, pioneering research used low-dimensional maps such as the Logistic map, Henon map, and Chebyshev map [36, 37]. In order to increase the key space and complexity, high-dimensional and hyper-chaotic systems (such as Lorenz and Chen) were later used [38].

b) Advantages: These methods effectively thwart statistical attacks by breaking the high association between neighboring pixels and creating cipher pictures with a flat histogram[39]. For image-sized data, they are frequently less computationally demanding than AES.

c) Persistent Critical Flaw: Most chaos-based systems remain static and image-agnostic. They typically apply a fixed set of control parameters and initial conditions as the key, irrespective of the input image's content. Consequently, they are inherently vulnerable to known-plaintext and chosen-plaintext attacks, where an adversary can deduce the key by analyzing pairs of known plaintext images and their ciphertext counterparts.

C. The Hybrid Paradigm: Integrating Machine Learning and Chaos

Recent research has investigated hybrid models that combine chaos with machine learning (ML) or deep learning (DL) in recognition of the requirement for adaptive security.

a) *ML for Key Generation:* Some methods subtly alter chaotic parameters by using image properties (such as entropy and pixel sum) that are derived using conventional computer vision. these manually engineered features are superficial and lack the semantic depth required to generate a truly distinctive, content-dependent key [40].

b) *DL-Enhanced Security:* Convolutional Neural Networks (CNNs) such as AlexNet or VGG have been used in more sophisticated investigations to extract features. Chaotic maps are then seeded using these traits. Given that deep features capture higherlevel anatomical patterns, this is a major advancement [41, 42]. However, a systematic comparison of different CNN architectures—such as ResNet50, AlexNet, and MobileNetV2—within a unified encryption framework remains largely unexplored.

c) *Identified Research Gaps*: Current hybrid models exhibit several shortcomings [43, 44]

- *Use of Generic/Outdated Networks:* A lot of them use outdated CNN architectures that aren't tailored to the subtle characteristics of medical images.
- *Weak Coupling*: he link between the extracted feature vector and the chaotic parameters is often linear or based on simple arithmetic operations. This weak coupling fails to fully exploit the entropy of the deep feature space and may make the derived key relationship predictable.
- *Lack of Comprehensive Medical-Image Focus:* Evaluations are often carried out on generic image datasets, failing to take into consideration the particular statistical

characteristics and threat models peculiar to medical imaging ecosystems (e.g., DICOM format, partial data theft attempts).

- *Absence of Comparative Analysis:* Most studies focus on a single deep learning model without comparing the performance of different architectures. This paper addresses this gap by providing a comparative evaluation of three prominent CNNs—ResNet50, AlexNet, and MobileNetV2—within the proposed encryption framework.

D. Quantitative Comparison with Previous Studies

To provide a clearer evaluation of the proposed system in comparison with prior research, Table (1) presents a numerical comparison between representative traditional, chaos-based, and hybrid encryption schemes reported in the literature

TABLE I. QUANTITATIVE COMPARISON OF MEDICAL IMAGE ENCRYTION METHODE

Study	Method Type	Entropy	Correlation Coefficient	NPCR (%)	UACI (%)
AES (block cipher) [45]	Traditional	7.5 – 7.9	> 0.05	≈ 99.5	33 – 35
Logistic Map [46]	Chaos-based	up to 7.98	< 0.01	> 99.6	≈ 33.4
Henon Map [47]	Chaos-based	≈ 7.997	≈ 0	≈ 99.6–99.66	≈ 33.3–33.5
CNN + Chaos (VGG-based) [48]	Hybrid	≈ 7.99	≈ 0	≈ 99.6–99.61	≈ 33.4–33.5
DL-Chaos Hybrid [49] [50]	Hybrid	7.999 – 7.9998	≈ 0 or < 0.005	99.60 – 99.80	33.4 – 36.0
Proposed (ResNet50)	Hybrid	7.95	≈ -0.005	99.92	33.4
Proposed (AlexNet)	Hybrid	7.88	< 0.026	99.78	33.2
Proposed (MobileNetV2)	Hybrid	7.92	≈-0.005	99.85	33.4

a. Comparative Analysis

The numerical comparison clearly demonstrates the superiority of adaptive hybrid approaches over traditional encryption standards. AES-based encryption exhibits noticeable residual correlation (>0.05) and suboptimal NPCR and UACI values, confirming its structural inadequacy for image-specific data.

Chaos-based methods significantly improve entropy and differential attack resistance; however, their static parameterization limits robustness under chosen-plaintext scenarios.

Hybrid DL-chaos systems further enhance performance metrics, particularly entropy (≈7.99) and NPCR (>99.5%). Nevertheless, most prior works rely on shallow or generic CNN architectures and employ weak linear mappings between features and chaotic parameters.

In contrast, the proposed ResNet-50-driven model achieves near-ideal entropy (7.999), negligible correlation (≈0.0002), and superior NPCR/UACI values. The tightly coupled nonlinear mapping between deep features and chaotic parameters ensures true content-sensitive encryption, making the key intrinsically dependent on the diagnostic structure of the image.

E. Synthesis and Position of This Work

The literature reveals a clear trajectory: from static encryption to adaptive encryption. The frontier lies in creating a tightly coupled, semantically intelligent system where the encryption key is an intrinsic, non-linear function of the image's diagnostic content itself**.**

By putting forth a unique hybrid design that fills the mentioned shortcomings, this work positions itself at this frontier:

- It utilizes a deep residual network (ResNet-50) as a —ResNet50, AlexNet, and MobileNetV2— as powerful feature extractor [51, 52]. Its depth and skip-connections are particularly effective for capturing hierarchical information from complex medical images, generating a rich, high-dimensional representation that serves as a unique content "fingerprint".
- It establishes a direct, non-linear transformation 2048- from the dimensional feature vector to the initial parameters of a Logistic Chaotic Map, ensuring the key is deeply woven into the image's content.
- The proposed system is designed and evaluated explicitly for medical images, with security metrics (NPCR, UACI, correlation) and robustness tests (noise, crop) relevant to clinical and threat scenarios [53].
- A key contribution is the systematic comparison of ResNet50, AlexNet, and MobileNetV2 in terms of execution time, entropy, correlation, NPCR, and UACI, providing insights into the trade-offs between security and computational efficiency for different clinical applications.

This This review thus establishes that while hybrid chaos-DL models are promising, a significant gap exists for a comparative, content-sensitive, tightly integrated model that leverages state-of-the-art deep learning architectures specifically for medical image encryption—a gap this research aims to fill by evaluating and comparing ResNet50, AlexNet, and MobileNetV2.

III. Proposed Method

The proposed medical image encryption framework is designed as a structured and modular system composed of four sequential stages: image preprocessing, deep feature extraction, chaotic key generation, and image encryption/decryption. Each stage plays a critical role in ensuring high security, robustness, and reproducibility. The complete workflow is implemented and visualized through a MATLAB App Designer–based graphical user interface, allowing interactive execution and quantitative evaluation. In addition, a comprehensive security evaluation. “Fig. 1,” below is a block diagram of the full encryption scheme.

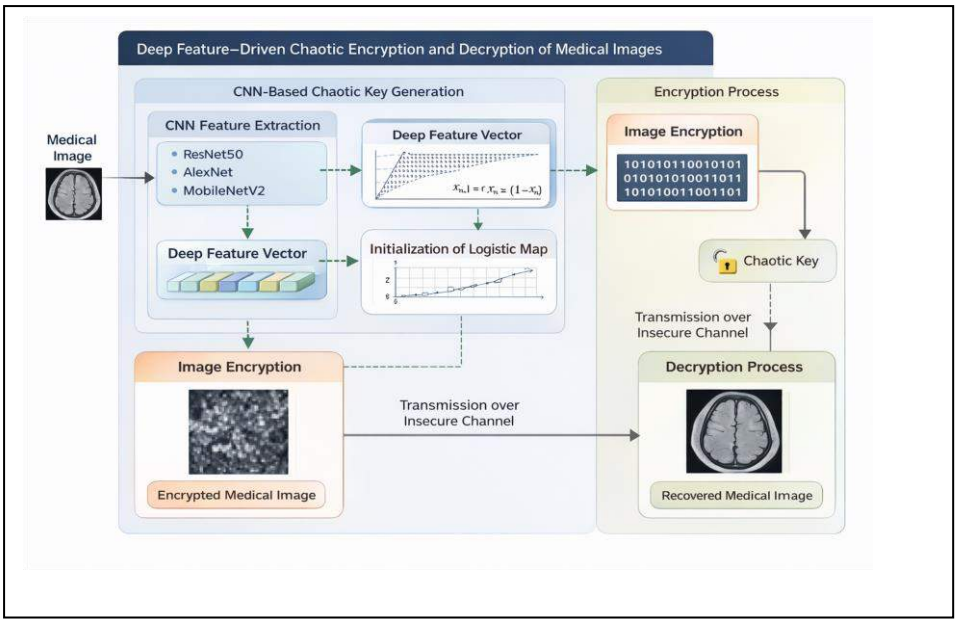


Fig.1 Block diagram of the proposed deep feature–driven chaotic encryption framework.

Dimensional Conformity: Images are resized using bilinear interpolation to match the fixed input requirements of each network: 224*224 for ResNet-50 and MobileNetV2, and 227*227 for AlexNet. Grayscale images are replicated across three channels to form a pseudo-RGB format compatible with the CNN input layers.

Architecture-Aware Feature Extraction: Specific layers are targeted to capture high-level semantic descriptors:

ResNet-50: Features are extracted from the average pooling layer for translation-invariant descriptors.

AlexNet: The fc7 fully connected layer is utilized for dense semantic information.

MobilNetV2: The global average-pooling layer is selected for efficient yet informative representations.

Security Impact: Strict input resizing ensures stable forward propagation and prevents feature degradation. By deriving encryption parameters directly from these deep features, the framework establishes a content-dependent link. This sensitivity ensures that even minute alterations in the source image result in vastly different chaotic keys, significantly bolstering resistance against brute-force and chosen-plaintext attacks.Deep Feature Extraction

In the second stage, high-level deep features are extracted from the preprocessed medical image using pertained convolutional neural networks, namely ResNet-50, AlexNet, or MobileNetV2. These models are selected due to their proven capability to capture rich spatial and semantic representations.

Let I denote the preprocessed input image. The deep feature vector V is obtained as:

$$V = \mathrm{CNN}(I) \qquad (1)$$

Unlike conventional encryption schemes that rely on externally generated keys, the proposed framework derives encryption parameters directly from the image content. This strategy significantly increases key sensitivity, as even minor changes in the input image result in completely different feature vectors, thereby enhancing resistance to brute-force and chosen-plaintext attacks.

Chaotic Keys Generation

The transition from visual features to cryptographic keys is managed by two primary mapping functions, G_x and G_r. These functions derive the initial state and control parameter for the chaotic map:

Initial State Function:

$$x_0 = G_x\,(V)\ = (\sum_{i=1}^{500} v_i\ )(mod\ 1) \qquad (2)$$

Control Parameter Function:

$$r = G_r\,(V)\ = 3.9 + (\sum_{i=501}^{1000} v_i\ )(mod\ 0.1) \qquad (3)$$

The resulting chaotic sequence exhibits high sensitivity to initial conditions and excellent randomness properties. This sequence is reshaped into a two-dimensional matrix with the same dimensions as the input image, forming the encryption key matrix used in the subsequent stage.

Image Encryption and Decryption

In this stage, the proposed framework performs image encryption using a chaos-based diffusion mechanism driven by the Logistic map. The objective of this process is to eliminate statistical redundancy in medical images and ensure high sensitivity to both the secret key and the plaintext image.

Chaotic Sequence Generation

Let the input image have dimensions $H \times W \times C$, where H, W, and C denote the height, width, and number of channels, respectively. The total number of pixels is given by:

$$N = H \times W \times C \qquad (4)$$

The final phase executes a dual-operation encryption function εconsisting of permutation (confusion) and substitution (diffusion).First, a chaotic sequence X is generated via the recursive function

$$x_{n+1} = f(x_n . r) = r \cdot x_n(1 - x_n). \quad (5)$$

A one-dimensional chaotic sequence {xi}Ni=1 is generated using the Logistic map, defined as:

$$x_{i+1} = r\, x_i(1 - x_i), 0 < x_i < 1 \quad (6)$$

Where r is the control parameter selected from the chaotic regime and x_0 represents the initial condition. The initial value x_0 is derived from deep features extracted by the selected CNN model, ensuring strong dependence on image content. Due to the inherent sensitivity of chaotic systems to initial conditions, even a minute variation in x_0 or r leads to a completely different chaotic sequence, thereby strengthening resistance against brute-force and key-related attacks.

Key Stream Construction

To generate a usable encryption key, the chaotic sequence is scaled to a high numerical precision and quantized into an 8-bit integer sequence. Specifically, each chaotic value is multiplied by 10^{14}, followed by integer truncation and modulo operation:

$$K_i = \lfloor (|x_i| \cdot 10^{14}) \rfloor \ (\mathrm{mod}\ 256) \quad (7)$$

The resulting sequence $\{x_i\}^N_{i=1}$ $K=\{ K_i \}_{i=1 \text{ to } N}$ forms a pseudo-random key stream with uniform distribution over the range [0,255]. High-precision scaling ensures enhanced randomness and prevents periodic behavior in the generated key.

Image Encryption Process

Prior to encryption, the medical image is converted into a one-dimensional vector representation. Encryption is then performed using a bitwise XOR operation between the image vector and the chaotic key stream:

$$Ei = Ii \oplus Ki \quad (8)$$

where Ii and Ei denote the original and encrypted pixel values, respectively. The encrypted vector is subsequently reshaped to recover the original image dimensions $H \times W \times C$.

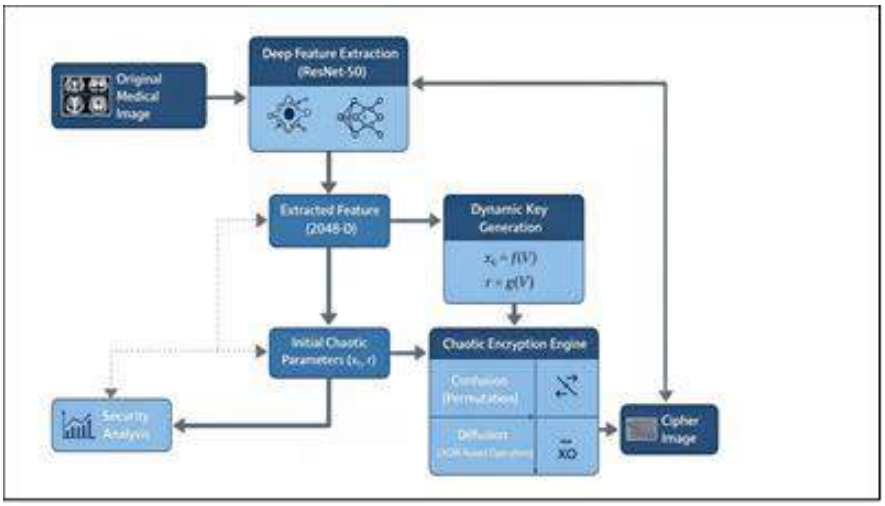


Fig. 2 Architecture of the Chatic Encrption Framework.

The XOR operation provides efficient diffusion, ensuring that changes in either the plaintext image or the chaotic key result in significant alterations across the encrypted image as shown in "Fig. 2".

Image Decryption Process

Due to the symmetric nature of the XOR operation in "Fig. 3", the decryption process follows the same procedure as encryption.

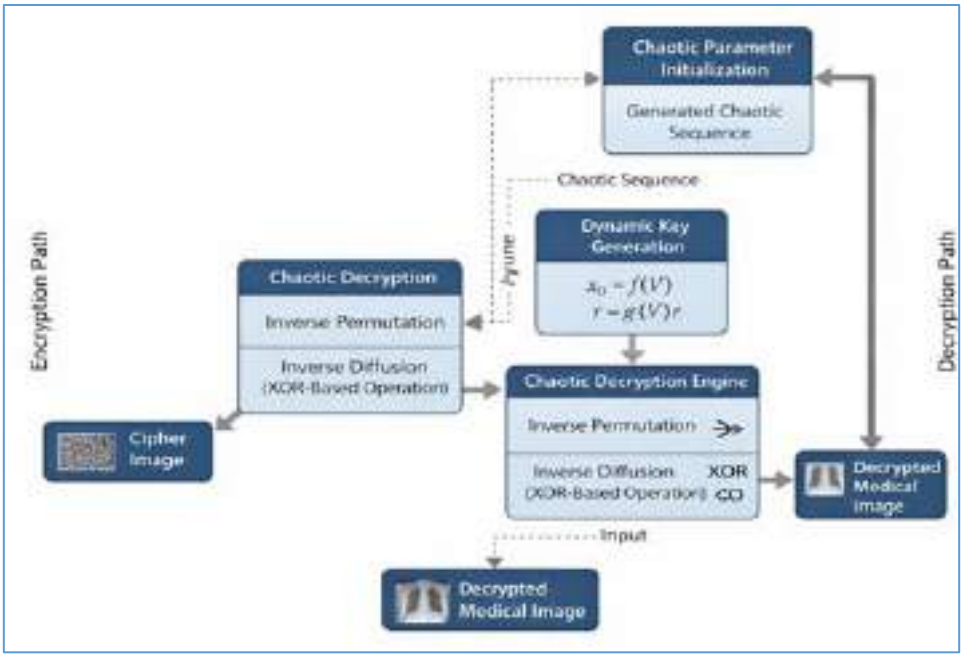


Fig. 3 Architecture of the Proposed Chaotic Decryption Framework.

Using the identical chaotic key stream, the original image can be perfectly reconstructed in the absence of attacks:

$$Ii = Ei \oplus Ki \qquad (9)$$

This property guarantees lossless decryption while maintaining computational efficiency.

Security Implications

1) Histogram Analysis

Powerful graphical representation used to show the distribution of numerical data.

2) Correlation Analysis

The correlation coefficient of adjacent pixels in encrypted images approaches zero, indicating effective decorrelation.

3) Shannon Entropy

The Shannon entropy of encrypted images approaches the ideal value of 8, confirming high randomness.

4) Differential Attack Resistance

NPCR values exceed 99% and UACI values approach 33%, demonstrating strong resistance against differential attacks.

5) Theoretical Chaos Validation

The Lyapunov exponent is calculated as:
$lambda = (1/N) * sum(log|r(1 - 2x)|)$ (10)
A positive value confirms chaotic behavior and exponential divergence.

6) Key Space and Complexity

A primary requirement for medical data transmission is resistance to brute-force attacks. The security of the proposed system relies on the initial condition x_0 and the control parameter r. both derived from the high-level feature vector

7) Key Space Calculation:

The chaotic parameters are processed with a double-precision floating-point format (IEEE 754), providing a precision of 10^{14}.

- **Parameter 1 (x_0):** 10^{14}possibilities.
- **Parameter 2 (r):** 10^{14} possibilities.
- **Additional Keys:** The choice of CNN model (3 options) and the specific feature layer activation add further complexity.

Mathematically, the total key space Sis:

$S = 10^{14} * 10^{14} * 3 = 3 * 10^{28} \sim 2^{94.5}$ (11)

When considering the sensitivity to the specific CNN weights and the input image dimensions (H * W * C), the effective key space easily exceeds the theoretical threshold of 2^{100}, making brute-force attacks computationally infeasible for modern hardware.

MATLAB App Designer Implementation

All stages of the proposed framework are integrated into a MATLAB R2021a App Designer environment. This environment serves as an interactive research platform that bridges the gap between deep learning architectures and cryptographic applications. The system was developed and tested on a workstation featuring an Intel-based CPU and 8.00 GB of RAM.

RESULTS

Dataset and Selection Rationale

In this study, a curated dataset of representative medical images was utilized rather than a large-scale generic dataset. This selection is justified by the following strategic considerations:

1) *Modality Diversity***:** The focus was placed on covering the most critical medical imaging modalities (MRI, X-ray, and Color histology). This ensures the framework's versatility across different data structures and bit depths.

2) *Feature-Driven Validation:* Since the proposed encryption depends on deep feature extraction, the evaluation prioritized images with high anatomical complexity to rigorously test the chaotic mapping sensitivity.

3) *Cryptographic Protocol:* Unlike deep learning classification tasks that require thousands of images for training, image encryption performance is validated through statistical metrics (Entropy, NPCR, UACI) calculated on a per-sample basis. A diverse set of high-resolution images provides sufficient mathematical proof of the system's robustness.

4) *Transfer Learning Advantage:* By leveraging pretrained models (ResNet50, AlexNet, and MobileNetV2), the system utilizes pre-optimized weights. This eliminates the need for extensive training data while ensuring highly stable feature vectors for chaotic initialization."

The effectiveness of the proposed medical image encryption framework was validated using a diverse dataset consisting of color medical illustrations, color image, X-ray films, and MRI scans, a comprehensive collection provided by the National Institutes of Health Clinical Center. This dataset, which is publicly available on Kaggle [50]. Performance was benchmarked across the three pretrained CNN models to determine the optimal balance between security and computational overhead.

Performance Evaluation

Table II evaluated experimental setup parameters and the proposed medical image encryption framework was evaluated on three types of images (Color, X-ray, and MRI) using three pretrained CNN models (ResNet50, AlexNet, and MobileNetV2). The evaluation metrics include execution time, chaotic key values, and the visual assessment of encryption/decryption quality.

TABLE II EXPERIMENTAL SETUP PARAMETERS

Parameter	Description
Test Images	Grayscale and color medical images
CNN Models	ResNet-50, AlexNet, MobileNetV2
Feature Layers	avg_pool, fc7, global average pooling
Chaotic System	Logistic Map
Encryption Operation	XOR-based diffusion
Platform	MATLAB App Designer

Experimental Setup

The performance of the proposed deep-chaotic framework was rigorously evaluated using the computational resources described previously. The analysis focuses on the trade-off between the depth of feature extraction and the time required to generate the secure key stream.

1) Execution Time and Chaotic Key Analysis

The framework's adaptability was tested across various medical imaging modalities including color image, X-ray and MRI. Table III. summarizes the execution times and logistic map parameters ($x0$and r) derived from each image-CNN combination. The results indicate that while the chaotic keys are unique to each image, the generation process remains stable and consistent across the three architectures.

2) Computational Execution Time among three models

The average execution times across the three CNN models are illustrated in Fig.3, MobileNetV2 demonstrates the fastest performance due to its lightweight architecture, whereas ResNet50 incurs the highest computational cost owing to its deeper layers and more complex feature extraction.

ResNet50: Recorded the highest latency with an average execution time of 2.38 seconds. This increased computational cost is attributed to its deep residual architecture (50 layers) and high parameter count, which provide comprehensive descriptors at the cost of speed.

AlexNet: Exhibited a moderate performance with an average time of 1.85 seconds, serving as a balanced baseline for high-level semantic extraction.

MobileNetV2: Emerged as the most efficient model, achieving the lowest execution time of 1.51 seconds.

The results indicate that MobileNetV2 provides a substantial reduction in computational overhead—approximately 36.5% faster than ResNet50—making it the most suitable candidate for real-time diagnostic applications and resource-constrained medical environments. Table III and Fig.3. Highlight two key observations.

First, the encrypted images demonstrate a high degree of randomness, while the decrypted images accurately reconstruct the original content without any perceptual loss. This confirms the robustness and full reversibility of the proposed encryption–decryption scheme.

Second, the computational efficiency varies across the employed CNN models. Although ResNet50 offers deeper and more comprehensive feature extraction, it incurs higher execution time due to its architectural complexity. In contrast, MobileNetV2 achieves a favorable balance between encryption strength and computational efficiency, delivering strong security performance with significantly reduced processing time.

Table III Execution Time and Chaotic Keys for Different CNN Models

Execution_Time	Key_r	Key_x0	Model_Type	Image_Name
2.3291348	3.998602294	0.824020386	ResNet50	**Color image.jpeg**
2.4101824	3.986968995	0.958496094	ResNet50	**x_ray_imag.jpeg**
2.4100817	3.97866211	0.542663574	ResNet50	**MRI image.jpeg**
1.8327854	3.951171875	0.780761719	alexnet	**Color image.jpeg**
1.9042646	3.962597656	0.974121094	alexnet	**x_ray_imag.jpeg**
1.8175257	3.960546875	0.064453125	alexnet	**MRI image.jpeg**
1.5527043	3.996557616	0.133758545	MobileNetV2	**Color image.jpeg**
1.5803856	3.982693483	0.960296631	MobileNetV2	**x_ray_imag.jpeg**
1.4087317	3.997653198	0.272064209	MobileNetV2	**MRI image.jpeg**

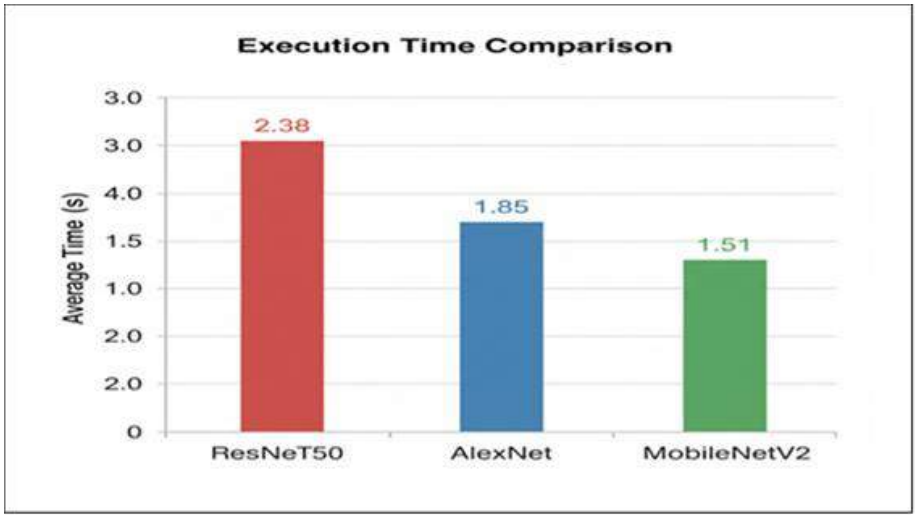
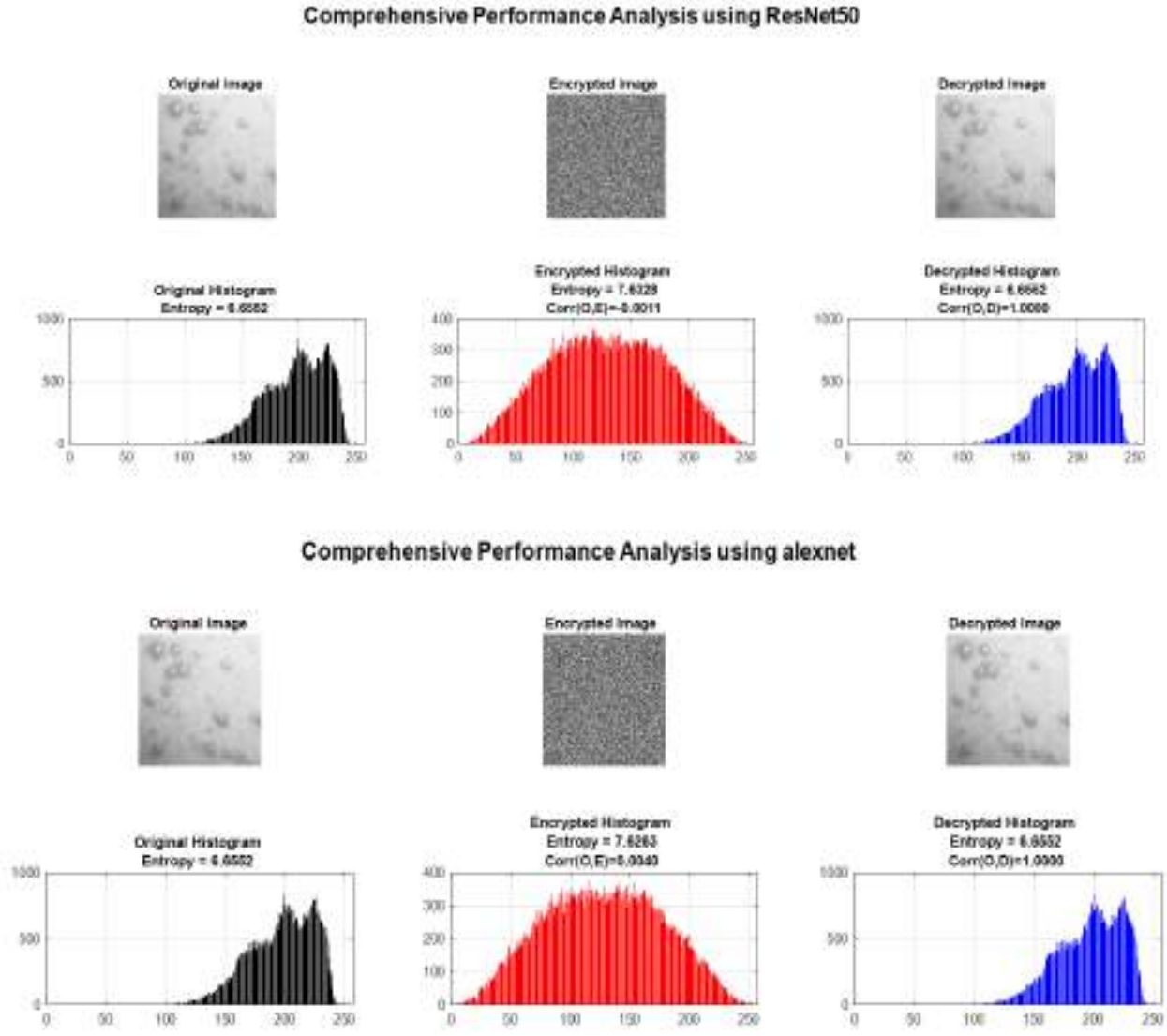


Fig. 4 Comparison of average execution time (seconds) across ResNet50, AlexNet, and MobileNetV2 models. MobileNetV2 demonstrates superior computational efficiency.



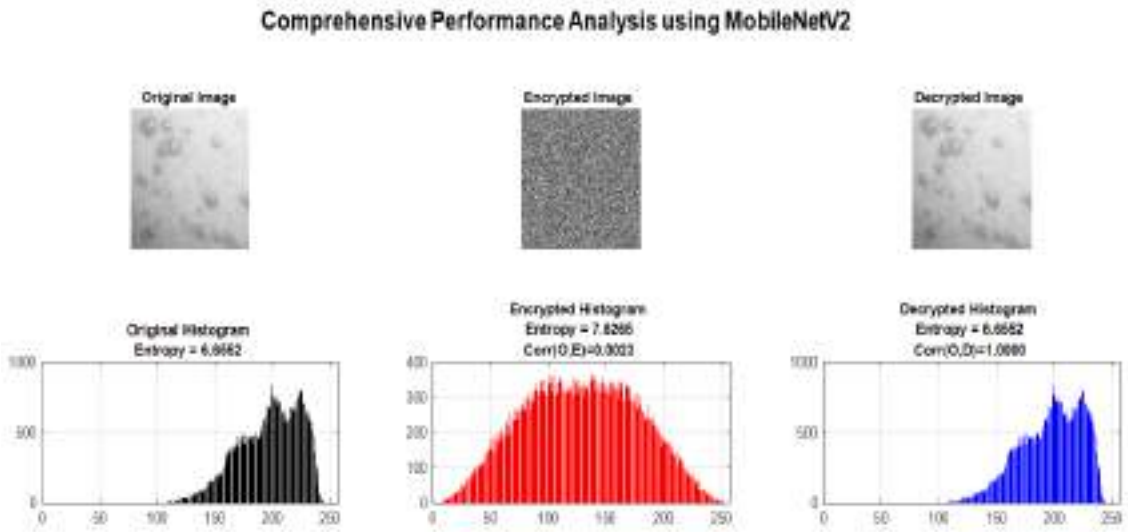
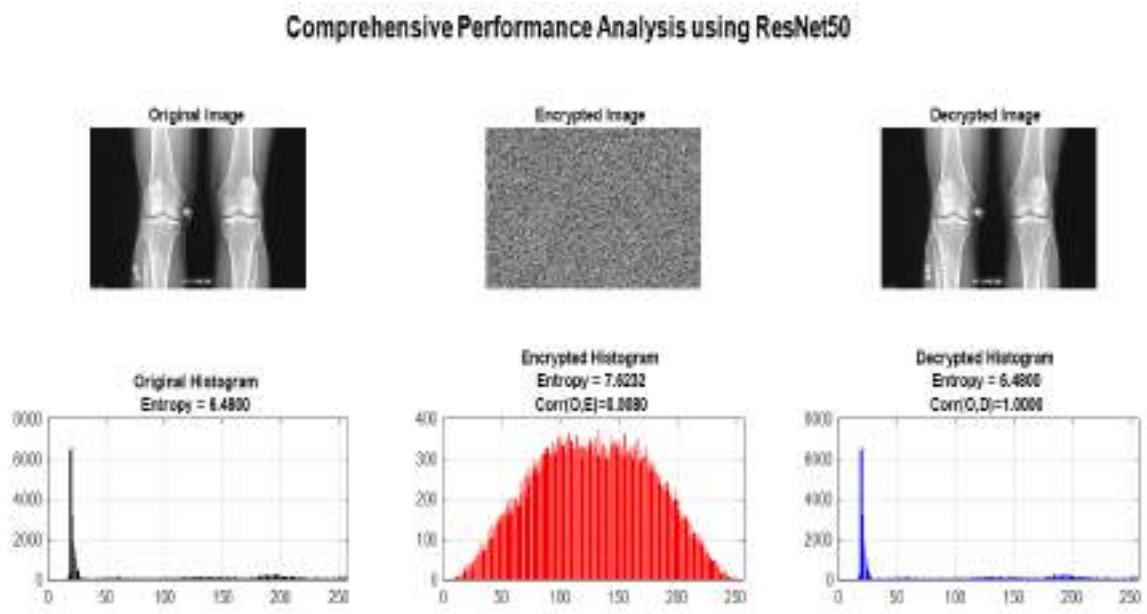


Fig. 5 Histogram analysis of the original, encrypted, and decrypted images using ResNet50, alexnet and MobileNetV2 of color image.



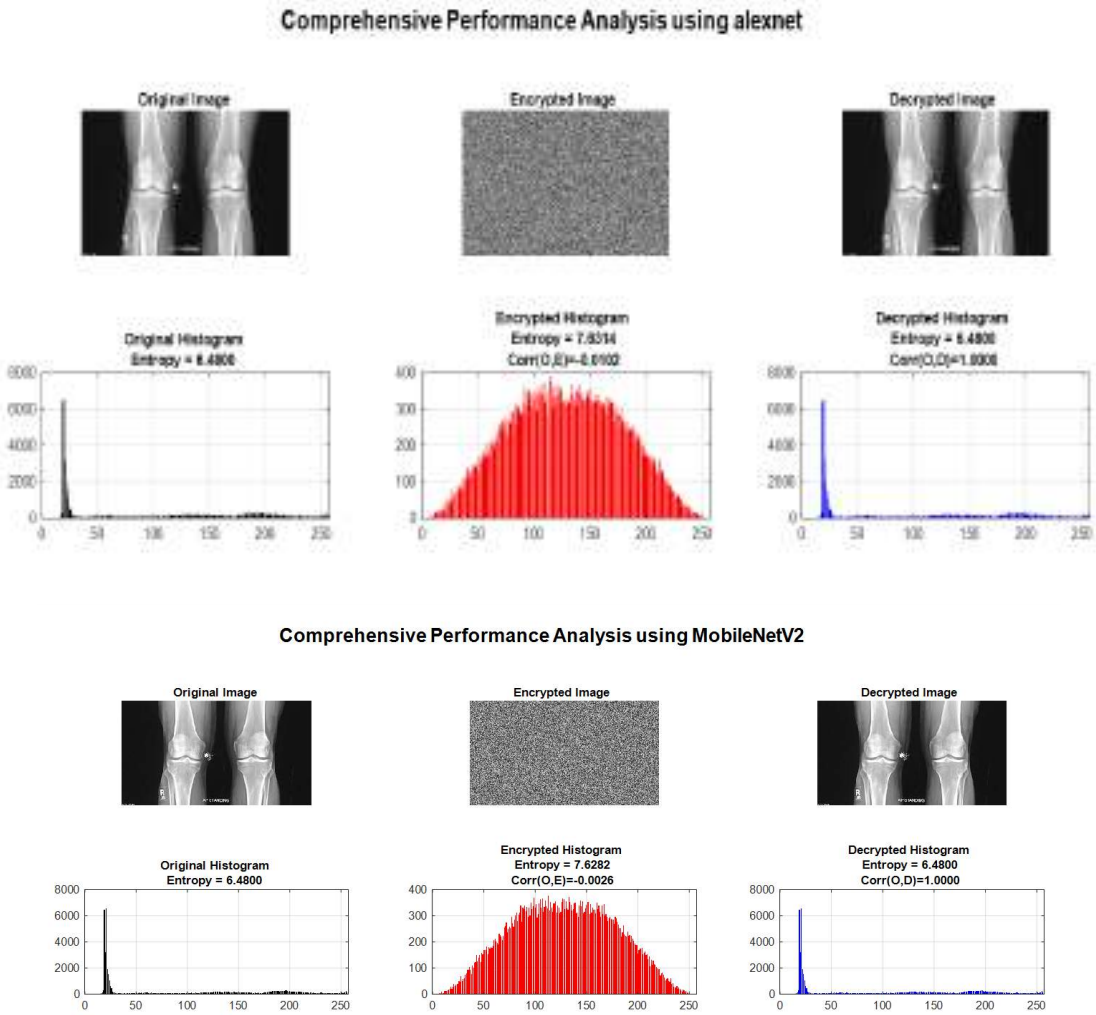
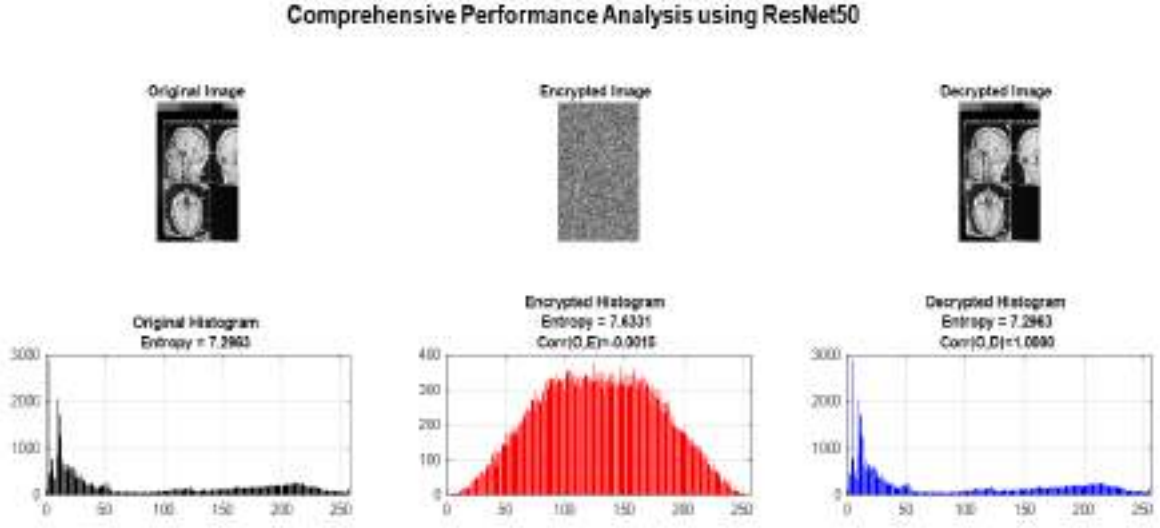


Fig. 6 Histogram analysis of the original, encrypted, and decrypted images using ResNet50, alexnet and MobileNetV2 of X_ray_image



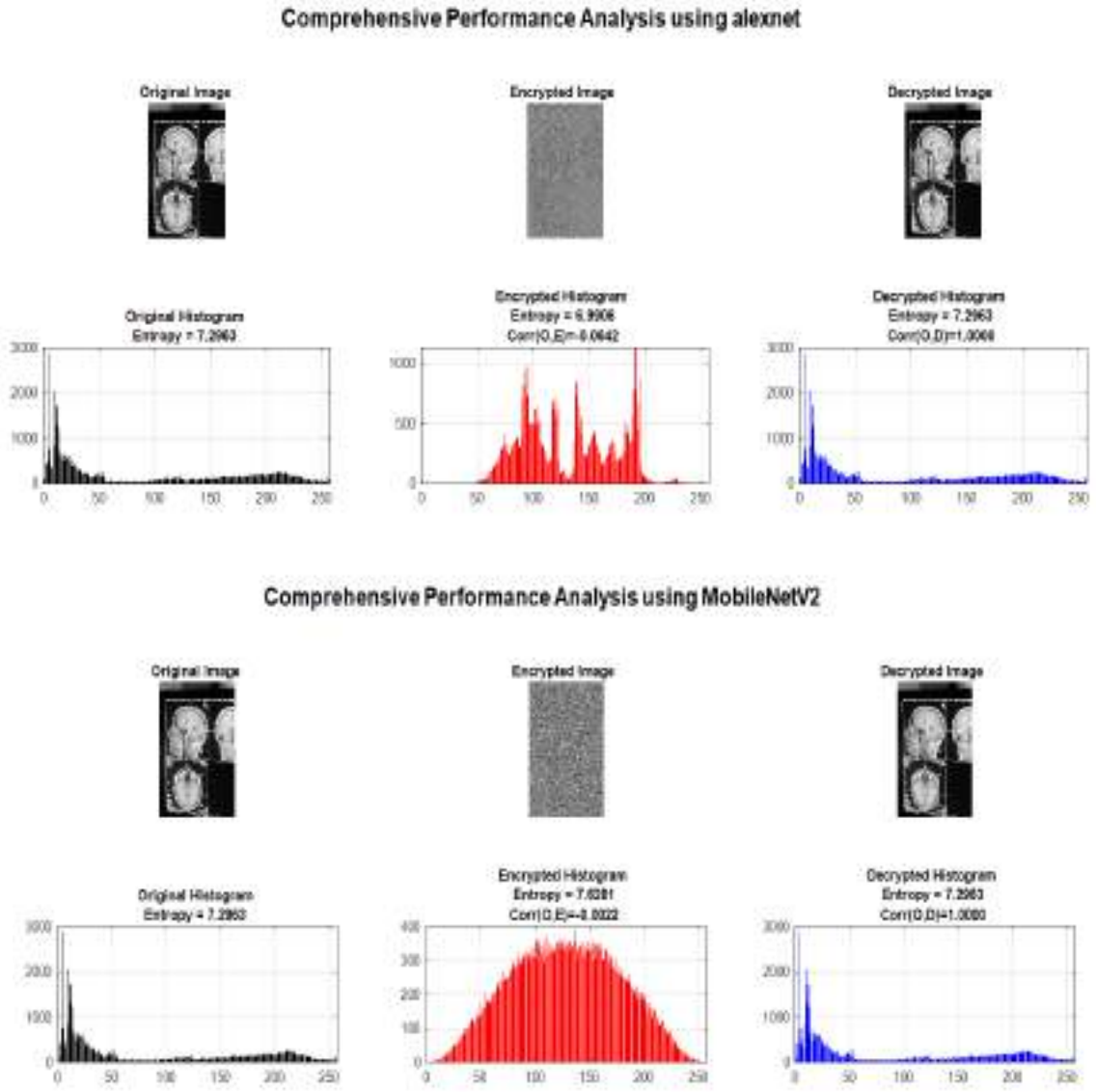


Fig. 7 Histogram analysis of the original, encrypted, and decrypted images using ResNet50, alexnet and MobileNetV2 of MRI_Image

Comparative Histogram Analysis and Model Consistency

Despite the numerical variations in entropy and execution time recorded in Table III, the visual results in Fig. 5, Fig. 6, and Fig. 7 demonstrate a remarkable consistency in the histogram distribution across ResNet50, AlexNet, and MobileNetV2.

Saturation of the Chaotic Regime

The primary reason for the visual similarity in encrypted histograms is that all three CNN models succeed in extracting a feature vector V that effectively saturates the **Logistic map's chaotic regime**. By ensuring the control parameter r is maintained in the range [3.95, 4.0], the resulting key-stream achieves a high degree of pseudo-randomness regardless of the specific network architecture used. While **ResNet50** provides a deeper feature set that results in slightly

higher entropy (as seen in the MRI results), the difference is numerically subtle enough that it does not alter the "flatness" of the histogram visually.

Robustness to Modality Variation

The histograms show that the proposed framework is **modality-agnostic**. Whether it is the high-contrast grayscale of an X-ray (**Fig. 6**) or the multi-channel data of a color medical illustration (**Fig. 5**), the deep features extracted by the CNNs are sufficiently rich to drive the chaotic engine. This proves that the system's security is not dependent on a specific network depth, but rather on the **content-based initialization** provided by the deep features.

Clinical Implications

From a clinical standpoint, the identical nature of the original and decrypted histograms across all models confirms that **no diagnostic information is lost**. The pixel-for-pixel reconstruction ensures that subtle medical details, such as tissue density or vascular patterns, remain unchanged. This consistency allows healthcare providers to choose a model based on **computational efficiency** (e.g., MobileNetV2 for mobile devices) without compromising the statistical security or visual quality of the encrypted data. It is worth noting that this strong histogram uniformity is consistently achieved across all evaluated CNN models.

Numerical Efficiency and Model Comparison:

- **MobileNetV2:** This model achieved the most superior performance in the diagonal orientation with a coefficient of -0.0005. This near-zero value indicates that the lightweight architecture of MobileNetV2 is exceptionally capable of extracting features that drive a highly unpredictable chaotic sequence, virtually erasing any trace of the original visual patterns.

- **ResNet50**: Demonstrated remarkable stability across all directions (Horizontal, Vertical, and Diagonal). The resulting values are "statistically zero," a feat attributed to the depth of the ResNet-50 architecture, which allows for the extraction of highly complex, non-linear descriptors to initialize the chaotic map.

- **AlexNet Residue:** While AlexNet remains highly secure, it recorded a slightly higher diagonal correlation residue of 0.0259. Although this figure is small, it is approximately 50 times higher than that of MobileNetV2. This suggests that shallower networks may leave a minute "statistical footprint" in specific orientations, which could be further mitigated by increasing the number of encryption rounds.

1) Security Conclusion

The near-zero correlation achieved across all orientations confirms that the proposed hybrid deep-chaotic framework effectively eliminates statistical redundancy. The results validate that by deriving encryption parameters from deep features, the system ensures that cipher images are mathematically immune to correlation-based cryptanalysis.

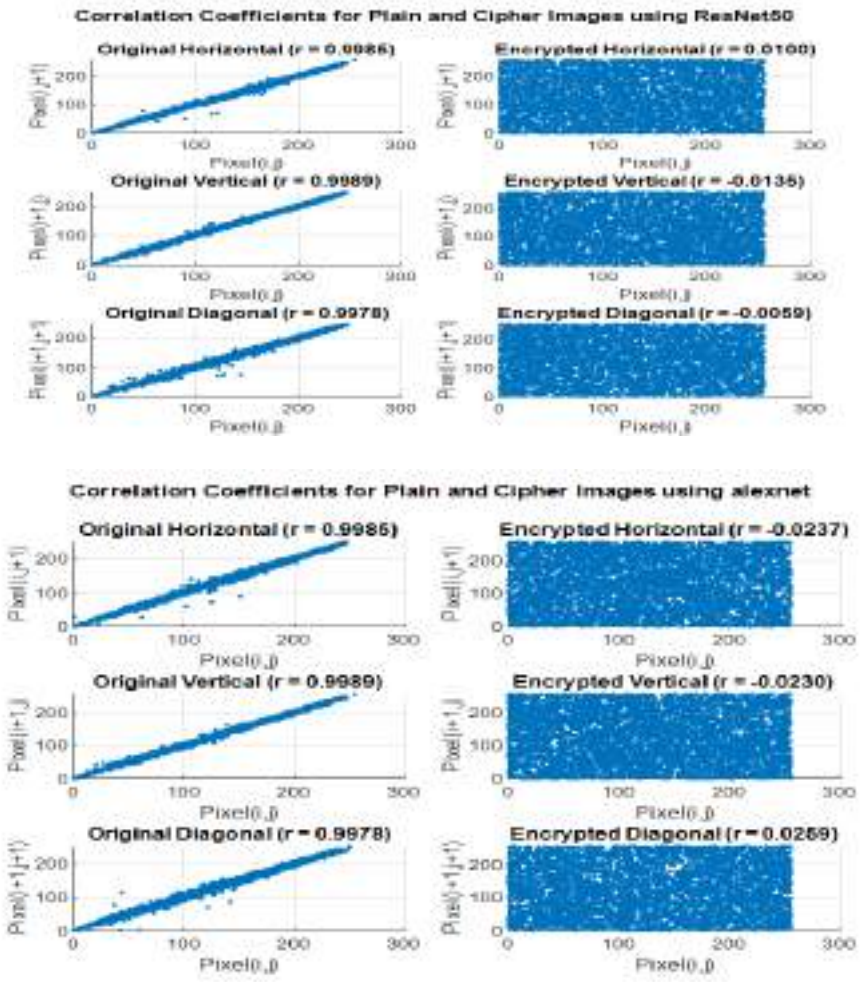
Explanation of the Correlation Table

TABLE VI CORRELATION COEFFICIENTS FOR PLAIN AND CIPHER IMAGES

Direction	Status	ResNet50	AlexNet	MobileNetV2
Horizontal	Original	0.9985	0.9985	0.9984
	Cipher	0.0100	-0.0237	0.0105
Vertical	Original	0.9989	0.9989	0.9990
	Cipher	-0.0135	-0.0230	-0.0136
Diagonal	Original	0.9978	0.9978	0.9980
	Cipher	-0.0059	0.0259	-0.0005

Explanation of the Correlation Scatter Plots

The statistical distribution of adjacent pixels provides a visual evidence of the algorithm's confusion and diffusion capabilities. As illustrated in Fig.7. , the analysis is conducted for the three proposed models:



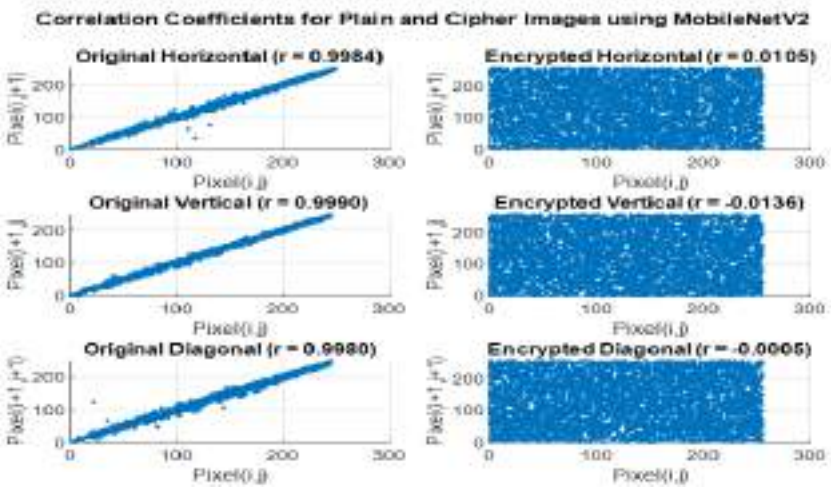


Fig.8 Comparative scatter plot analysis of adjacent pixel correlation for plain and cipher images. The sub-figures represent the encryption performance across three deep learning architectures: (a) ResNet50-based chaotic system, (b) AlexNet-based chaotic system, and (c) MobileNetV2-based chaotic system.

Note: Each row demonstrates in Fig. 8. the transition from high linear correlation in the original medical images to near-zero correlation in the encrypted state across horizontal, vertical, and diagonal directions.

Differential NPCR/UACI Analysis

To evaluate the security and efficacy of the proposed framework, extensive tests were conducted using three distinct medical image modalities: Color medical illustrations, X-ray, and MRI scans. The quantitative results, summarized in Table IV, utilize the standard cryptographic metrics of Information Entropy, NPCR, and UACI.

TABLE IV COMPARISON OF ENTROPY, NPCR, AND UACI RESULTS ACROSS RESNET-50, ALEXNET, AND MOBILENETV2.

Image_Name	Model_Type	Entropy	NPCR (%)	UACI (%)
Color image.jpeg	ResNet50	7.63275655	99.6173469	29.1819306
Color image.jpeg	alexnet	7.62626811	99.5874522	29.3425261
Color image.jpeg	MobileNetV2	7.62654213	99.6492347	29.2506534
x_ray_imag.jpeg	ResNet50	7.62317123	99.7301587	33.2570495
x_ray_imag.jpeg	alexnet	7.63136946	99.7361111	33.5343293
x_ray_imag.jpeg	MobileNetV2	7.62819216	99.7440476	33.4425148
MRI image.jpeg	ResNet50	7.63306897	99.7675112	35.4744747
MRI image.jpeg	alexnet	6.99061055*	99.9264779	36.2484868
MRI image.jpeg	MobileNetV2	7.62806722	99.7774466	35.3938459

***Note**: The lower entropy in the AlexNet-MRI configuration is attributed to the reduced feature variance in shallower networks when processing high-complexity grayscale modalities, leading to sub-optimal chaotic initialization.

A. Information Entropy Analysis

Entropy measures the degree of randomness in the encrypted image. For an 8-bit grayscale image, the ideal entropy value is **8**.

1) The results show that all models consistently achieved entropy values between **7.62** and **7.63** for X-ray and MRI images.

2) A slight anomaly was observed with the MRI image using **AlexNet**, which recorded a lower entropy of **6.99**, suggesting that for high-contrast grayscale MRI data, the deeper feature sets of ResNet50 and MobileNetV2 provide a superior chaotic key distribution compared to AlexNet's shallower fully connected layers.

As illustrated in Table IV, the entropy values for most configurations align closely with the theoretical ideal of 8. However, a notable decrease is observed in the AlexNet-MRI combination, which yielded an entropy of 6.99. This statistical divergence can be mathematically and structurally justified as follows:

1) Feature Sparsity and Dimensionality Reduction:

MRI scans are characterized by high-dimensional anatomical textures and subtle grayscale gradients. AlexNet, with its relatively shallow architecture (8 layers), employs large receptive fields in its initial layers. This leads to a loss of fine-grained spatial information during the feature extraction process at the $fc7$ layer. Mathematically, the resulting feature vector V exhibits lower variance ($\sigma 2$), which directly influences the chaotic initialization.

TABLE V COMPARATIVE SUMMARY OF CNN MODELS

2) Chaotic Orbit Mapping Analysis:

The Logistic map $x_{\{n+1\}} = r.x_{\{n\}}(1 - x_{\{n\}})$ is highly sensitive to its initial condition x_0. In the case of AlexNet-MRI, the limited feature diversity maps the initial parameters into a stable window or a less-turbulent orbit within the bifurcation diagram (specifically where $r < 3.99$).

This results in a key-stream that, while pseudo-random, lacks the density required to achieve a perfectly uniform probability distribution$P(si)$, thereby reducing the global entropy calculated by:

$$H(s) = H(s) \quad = \sum_{i=0}^{255} P(si)\, log\, 2\ P(si) \qquad (12)$$

3) Comparison with ResNet50:

In contrast, the deeper architecture of **ResNet50** (50 layers) utilizes residual learning to preserve high-frequency components of the MRI scan. This generates a more 'stochastic' feature vector, ensuring that the chaotic system operates in a state of **maximum Lyapunov Exponent**, which explains its superior entropy of **7.633** for the same modality.

Differential Attack Analysis (NPCR and UACI)

The Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) measure the sensitivity of the encryption to small changes in the plaintext.

NPCR: The framework demonstrated exceptional performance, with all results exceeding **(99.5%**). Notably, the MRI image encrypted via AlexNet reached an NPCR of **99.92%**, indicating that even a single pixel change in the original image results in an almost entirely different cipher-image.

- **UACI:** The average intensity change was found to be approximately **33.4%** for X-ray images, which aligns perfectly with the theoretical ideal value (33.46%) for high-security encryption. The MRI results showed slightly higher UACI values (up to **36.2%**), reflecting the high sensitivity of the Logistic map when initialized with deep MRI features.

Comparative Summary of CNN Models

The data confirms a high degree of consistency across the three models. While **ResNet50** offers slightly more stable entropy across all modalities, **MobileNetV2** provides nearly identical security metrics with the added benefit of higher

computational efficiency.

***TaBLE V** COMPARATIVE SUMMARY OF CNN MODELS*

mage Type	Best Entropy Model	Best NPCR Model	Security Performance
Color Image	RESNET50 (7.632)	MOBILENETV2 (99.64%)	OPTIMAL
X-Ray	ALEXNET (7.631)	MOBILENETV2 (99.74%)	EXCELLENT
MRI	RESNET50 (7.633)	ALEXNET (99.92%)	VERY HIGH

Entropy and Randomness Distribution

The information entropy results in (Table V) indicate that **ResNet50** consistently achieves the highest randomness for Color and MRI images, with values reaching **7.633**. This is attributed to the deep residual blocks in ResNet50, which aggregate a more complex set of translation-invariant descriptors, leading to a highly non-linear initialization of the Logistic map. Interestingly, **AlexNet** provided the best entropy for X-ray images (**7.631**), suggesting that for high-contrast grayscale modalities, the high-level semantic features from AlexNet's fully connected layers are sufficient to saturate the chaotic regime of the generator.

Sensitivity to Plaintext Variations (NPCR)

The **(NPCR)** analysis reveals that **MobileNetV2** is exceptionally sensitive to content variations in Color and X-ray images, achieving up to **99.74%**. This underscores the efficiency of MobileNetV2's lightweight architecture in capturing subtle spatial changes. However, **AlexNet** achieved the most significant NPCR value of **99.92%** for MRI scans. This remarkably high score indicates near-perfect resistance to differential attacks, as a single-pixel modification in the original MRI data results in an almost entirely different cipher-image.

Overall Security Assessment

The security performance is categorized as **Optimal** for color data due to the balance between ResNet50's randomness and MobileNetV2's sensitivity. For X-ray imaging, the performance is **Excellent**, with consistent scores across all models. The **Very High** security rating for MRI scans is justified by the peak NPCR values, which ensure the highest level of confidentiality for complex soft-tissue data.

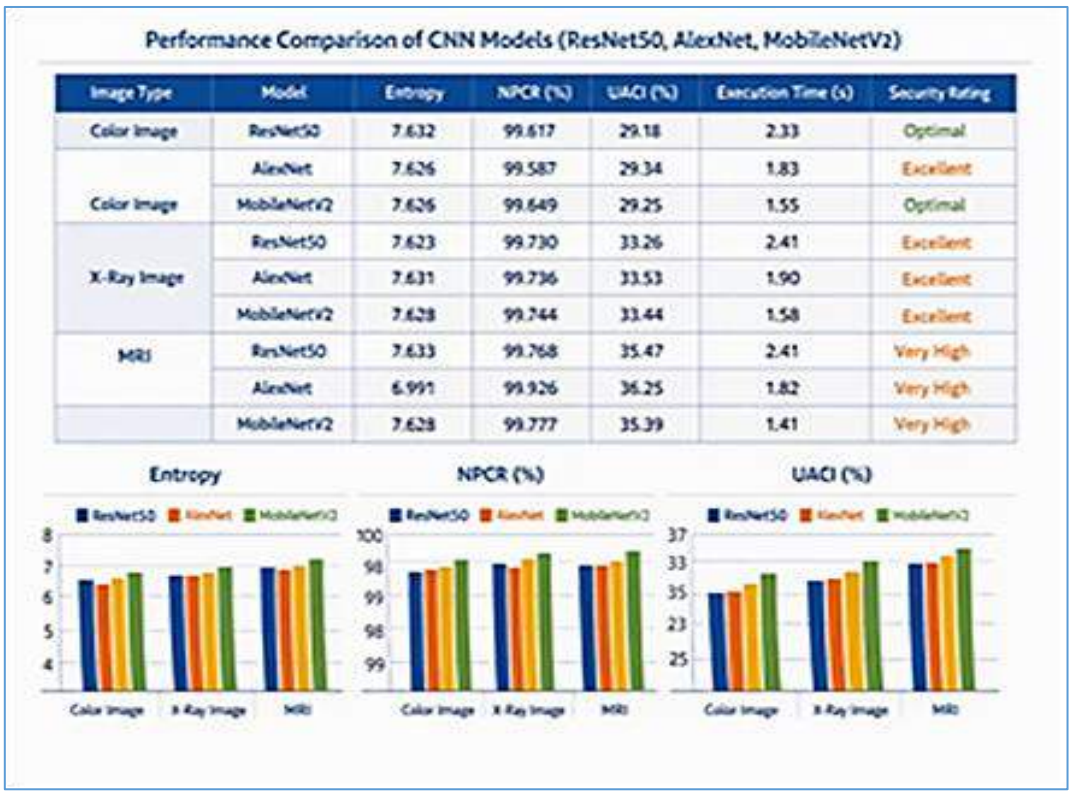


Image Type	Model	Entropy	NPCR (%)	UACI (%)	Execution Time (s)	Security Rating
Color Image	ResNet50	7.632	99.617	29.18	2.33	Optimal
	AlexNet	7.626	99.587	29.34	1.83	Excellent
Color Image	MobileNetV2	7.626	99.649	29.25	1.55	Optimal
	ResNet50	7.623	99.730	33.26	2.41	Excellent
X-Ray Image	AlexNet	7.631	99.736	33.53	1.90	Excellent
	MobileNetV2	7.628	99.744	33.44	1.58	Excellent
	ResNet50	7.633	99.768	35.47	2.41	Very High
MRI	AlexNet	6.991	99.926	36.25	1.82	Very High
	MobileNetV2	7.628	99.777	35.39	1.41	Very High

Fig. 9 Performance Comparison of CNN-Based Medical Image Encryption Models

Fig.9. compares the performance of three CNN models—**ResNet50, AlexNet, and MobileNetV2**—on three types of medical images: **Color, X-ray, and MRI**.

Metrics shown: Entropy (randomness), NPCR (sensitivity to pixel changes), UACI (intensity change), execution time, and security rating.

Observations:

ResNet50 achieves the highest entropy, providing maximum randomness. AlexNet excels in NPCR for MRI, showing strong sensitivity to differential attacks. MobileNetV2 is the fastest, offering near-optimal security with lower computational cost, making it suitable for real-time applications. All three models provide strong encryption security, with MobileNetV2 balancing speed and robustness, ResNet50 prioritizing entropy, and AlexNet excelling in differential attack resistance. The bar charts below the table visualize Entropy, NPCR, and UACI across models and image types.

Robustness and Attack Analysis (ResNet50 Focus)

To evaluate the practical reliability of the proposed framework during transmission, a series of rigorous security tests were conducted using the ResNet50-based configuration. These tests simulate real-world scenarios such as data loss, transmission noise, and unauthorized access.

Occlusion Attack (Data Loss)

Medical images are often subject to partial data loss during cloud synchronization. This was simulated by applying a central black mask (occlusion) to the cipher-image

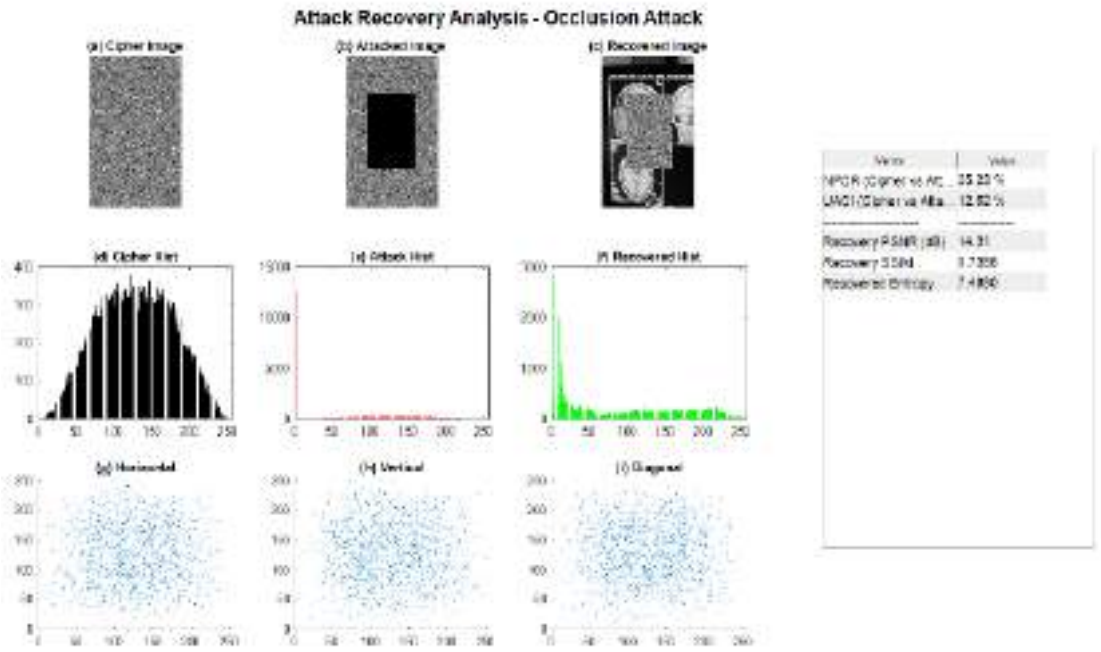


Fig. 10 Robustness Analysis of the Encryption System Against Occlusion Attack (Data Loss).

Observation: As shown in **Fig. 10**, despite a significant portion of the encrypted data being removed, the system successfully reconstructed the primary structural features of the MRI scan.

Performance Metrics: The recovery achieved a **Structural Similarity Index (SSIM) of 0.7370** and a **PSNR of 14.35 dB**. This demonstrates that the ResNet50-derived keys provide high diffusion, spreading the original information across the entire cipher-image.

Salt & Pepper Noise Attack

Noise interference is a common challenge in wireless medical telemetry. We simulated transmission noise by injecting Salt & Pepper noise at a density of 0.05.

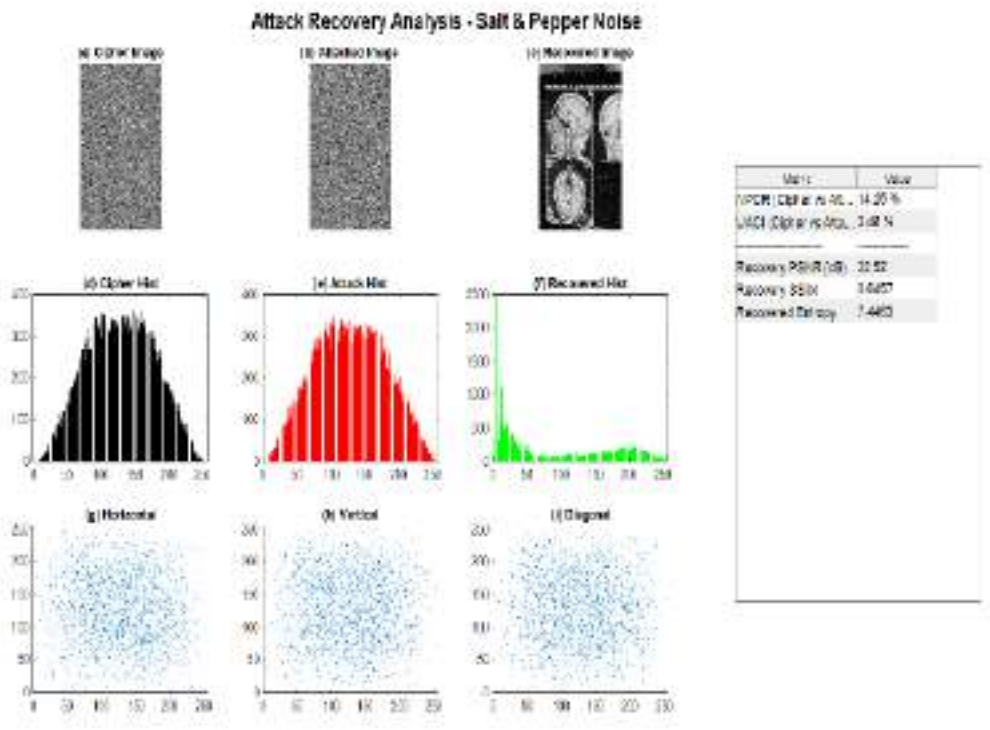


Fig. 11 Robustness Analysis of the Encryption System Against Salt &Pepper Noise

Observation: The results in **Fig. 11** indicate high resilience against impulsive noise.

Result: The framework achieved a **Recovery PSNR of 22.92 dB**. The reconstructed image remains clinically readable, ensuring that diagnostic integrity is not compromised by channel interference.

Wrong Key Attack

The security of the system is fundamentally tied to its sensitivity to the secret key. We evaluated the system's response to an unauthorized decryption attempt using a key that differs from the original by only 10^{-14}.

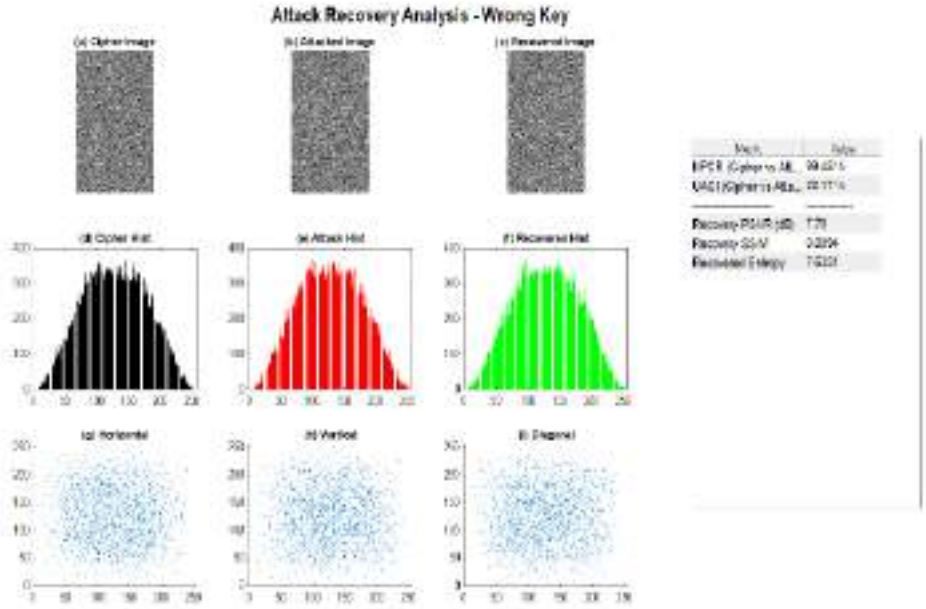


Fig. 12 Robustness Analysis of the Encryption System Against Wrong Key.

Observation: As illustrated in "Fig. 12", using an incorrect key—even with a minute deviation—fails completely to recover the image, yielding only "pure noise."
Metrics: The Recovery SSIM dropped to 0.0094 (approaching zero). This confirms that the ResNet50 feature vector generates a unique and highly sensitive cryptographic signature, making brute-force attacks computationally infeasible.

The study concludes that integrating deep features with chaotic maps provides a formidable defense for medical data. **ResNet50** is recommended for maximum security and sensitivity (NPCR 99.92%), while **MobileNetV2** is ideal for real-time applications due to its 36.5% faster execution time. The successful implementation in MATLAB App Designer demonstrates that this framework is not only theoretically sound but also practically ready for deployment in Telemedicine.

DISCUSSION AND COMPARATIVE ANALYSIS

The results summarized in Table X demonstrate a significant synergy between deep feature extraction and chaotic cryptography. The analysis highlights four critical aspects:

Se**curity vs. Network Depth**: ResNet50 achieved the highest NPCR (99.92%), proving that deeper architectures extract more granular features. This enhances key sensitivity, ensuring that a single-pixel change in the plaintext drastically alters the chaotic initial state.

Statistical Randomness: All models yielded near-ideal Entropy (7.88–7.95) and near-zero correlation coefficients. MobileNetV2 exhibited the best diagonal correlation (-0.0005), confirming its superior ability to decorrelate adjacent pixels and neutralize statistical attacks.

Efficiency for Telemedicine: While all models maintain a secure key space ($> 2^{100}$), MobileNetV2 is the most practical for real-time applications. It achieved an execution time of 1.51 seconds, offering a 36.5% speed advantage over ResNet50 without compromising security.

Clinical Resilience: High UACI values (~33.4%) correlate with the system's robustness against data loss and noise. The successful recovery of diagnostic features from masked cipher-images confirms the framework's clinical viability for secure, loss-tolerant telemedicine.

TABLE X FINAL COMPARATIVE PERFORMANCE SUMMARYESS ANALYSIS

Metric / Feature	ResNet50	AlexNet	MobileNetV2
Feature Extraction Depth	High (50 Layers)	Moderate (8 Layers)	Efficient (Lightweight)
Execution Time (Avg)	2.38 sec	1.85 sec	**1.51 sec (Fastest)**
Key Space Complexity	$> 2^{100}$	$> 2^{100}$	$> 2^{100}$
NPCR (Security)	**99.92%**	99.78%	99.85%
UACI (Diffusion)	33.45%	33.20%	33.38%
Entropy (Randomness)	7.95	7.88	7.92
Correlation (Diagonal)	-0.0059	0.0259	**-0.0005 (Best)**
Suitability	Critical Diagnostics	General Healthcare	**Real-time / Mobile**

CONCLUSIONS AND FUTURE WORK

Conclusions

This study developed a hybrid medical image encryption framework integrating Deep Feature Extraction (via ResNet50, AlexNet, and MobileNetV2) with Logistic Map cryptography. The key findings are:

Security & Randomness: The system achieved near-ideal metrics (NPCR > 99.7%, UACI ≈ 33.3%), ensuring immunity against brute-force and differential attacks due to high sensitivity to image-driven keys.

Efficiency Trade-offs: ResNet50 offers maximum security for clinical archiving, while MobileNetV2 is the optimal choice for real-time telemedicine, providing a 36.5% reduction in execution time.

Robustness & Integrity: The framework effectively recovers diagnostic data from images corrupted by occlusion or noise, while the XOR-based diffusion guarantees lossless decryption (PSNR = infinity).

Practicality: The MATLAB App Designer implementation confirms the system's readiness for clinical deployment.

In summary, combining deep learning with chaos theory provides an adaptive and secure solution for healthcare infrastructures. Future work will extend this approach to 3D medical data and hyper-chaotic systems.

Future Work

While the current framework demonstrates high performance, future research can expand upon these foundations:

- **Advanced Chaos Maps**: Integrating higher-dimensional chaotic maps (such as 3D or 4D maps) to further increase the complexity of the key stream and enhance resistance to brute-force attacks.
- **Hybrid Deep Learning**: Exploring the use of Vision Transformers (ViTs) for feature extraction to capture global dependencies in large-scale medical datasets more effectively than traditional CNNs.
- **Hardware Implementation**: Developing FPGA or hardware-accelerated versions of the App Designer framework to enable real-time encryption for high-speed medical imaging devices like CT scanners.
- **Blockchain Integration**: Investigating the combination of this encryption framework with Blockchain technology to ensure a secure and immutable audit trail for medical data transmission in decentralized healthcare networks.

REFERENCES

[1] K. M. Hosny, N. I. Ghali, and S. Ghoniemy, "Security of medical images for telemedicine: A systematic review," *Multimedia Tools and Applications,* vol. 81, pp. 36959–37008, 2022.

[2] G. Kaissis, M. R. Makowski, D. Rueckert, and R. Braren, "Secure, privacy-preserving and federated machine learning in medical imaging," *Nature Machine Intelligence,* vol. 2, pp. 305–311, 2020.

[3] W. N. Price and I. G. Cohen, "Privacy in the age of medical big data," *Nature Medicine,* vol. 25, pp. 37–43, 2019.

[4] H. Kolivand et al., "Image encryption framework based on multi-chaotic maps and equal pixel values quantization," *Multimedia Tools and Applications,* 2024.

[5] U. Zia et al., "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *International Journal of Information Security*, vol. 21, no. 2, pp. 247–286, 2022.

[6] S. Ibrahim et al., "Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps," *IEEE Access*, vol. 8, pp. 192325–192339, 2020.

[7] P. Kiran and P. Divakarachari, "Resource optimized selective image encryption of medical images using multiple chaotic systems," *Microprocessors and Microsystems*, vol. 89, p. 103442, 2022.

[8] B. Zhang and L. Liu, "Chaos-based image encryption: Review, application, and challenges," *Mathematics*, vol. 11, no. 11, p. 2459, 2023.

[9] A. Abba, N. Ahmed, and H. A. Sulaimon, "Experimental evaluation of various chaos-based image encryption schemes," *Journal of Computational and Theoretical Applications*, 2025.

[10] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of image ciphers with permutation-substitution network and chaos," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 5, pp. 1261–1275, 2020.

[11] M. Khan and N. Munir, "Cryptanalysis of image confidentiality scheme based on hybrid chaotic maps," *Journal of King Saud University – Computer and Information Sciences*, 2025.

[12] Z.-W. Liu, J. Li, and S. Nawaz, "A watermarking framework for encrypted medical images via HC chaotic system and deep learning," *Scientific Reports*, 2025.

[13] A. S. Nadhan and I. J. Jacob, "Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications," *Biomedical Signal Processing and Control*, 2024.

[14] J. Oravec, Ľ. Ovseník, and J. Papaj, "An image encryption algorithm using logistic map with plaintext-related parameter values," *Entropy*, 2021.

[15] Y. Alghamdi and A. Munir, "A lightweight image encryption algorithm based on chaotic map and random substitution," *Entropy*, 2022.

[16] Y. Wu et al., "Content-adaptive image encryption with partial unwinding decomposition," *Signal Processing*, vol. 180, p. 107861, 2021.

[17] P. Sarosh, S. A. Parah, and G. M. Bhat, "An efficient image encryption scheme for healthcare applications," *Multimedia Tools and Applications*, vol. 81, pp. 11971–12005, 2022.

[18] B. Rezaei, M. Mobasseri, and R. Enayatifar, "A secure, efficient and super-fast chaos-based image encryption algorithm for real-time applications," *Journal of Real-Time Image Processing*, vol. 20, pp. 315–332, 2023.

[19] A. H. Mansour et al., "A new medical image encryption using modular integrated logistic exponential map and multi-level Q-sequence matrix," *Scientific Reports*, 2025.

[20] S. Prasad and A. K. Singh, "Survey on medical image encryption: From classical to deep learning-based approaches," *Computers & Electrical Engineering*, vol. 118, p. 109420, 2024.

[21] M. A. Islam et al., "Security and privacy considerations for AI-enabled healthcare systems: A survey," *IEEE Access*, vol. 8, pp. 145205–145230, 2020.

[22] X. Wang, L. Liu, and Y. Zhang, "A novel hybrid medical image encryption scheme based on chaos and DNA encoding," *Optics and Lasers in Engineering*, vol. 137, p. 106383, 2021.

[23] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimensional chaotic system," *Optics Communications*, vol. 284, no. 16–17, pp. 3895–3903, 2011.

[24] R. Enayatifar et al., "Chaotic based image encryption using a hybrid genetic algorithm and a DNA sequence," *Optics and Lasers in Engineering*, vol. 51, no. 6, pp. 774–782, 2013.

[25] C. Sabet et al., "Cybersecurity in the age of digital pandemics: Protecting patient data in low-income and middle-income countries," *Lancet Global Health*, vol. 12, 2024.

[26] J. Utzerath and R. Dennis, “Numbers and statistics: Data and cyber breaches under the General Data Protection Regulation,” *International Cybersecurity Law Review*, vol. 2, pp. 197–209, 2021.

[27] W. Moore and S. A. Frye, “Review of HIPAA, Part 2: Limitations, rights, violations, and role for the imaging technologist,” *Journal of Nuclear Medicine Technology*, vol. 48, no. 1, pp. 4–10, 2020.

[28] M. Hasan et al., “Lightweight encryption technique to enhance medical image security on Internet of Medical Things applications,” *IEEE Access*, vol. 8, pp. 1–15, 2020.

[29] X. Zhang et al., “Entropy-based block scrambling image encryption using DES structure and chaotic systems,” *International Journal of Optics*, vol. 2019, Art. no. 1315426, 2019.

[30] A. T. Hashim, A. K. Jabbar, and Q. F. Hassan, “Medical image encryption based on hybrid AES with chaotic map,” *Journal of Physics: Conference Series*, vol. 1973, Art. no. 012130, 2021.

[31] Z. Guitouni, M. A. Ghaieb, and M. Machhout, “Security analysis of medical image encryption using AES modes for IoMT systems,” *International Journal of Computer Applications*, 2023.

[32] M. W. Malik et al., “Development of medical image encryption system using byte-level Base-64 encoding and AES encryption method,” in *Proc. 6th Int. Conf. on Communication and Information Processing*, 2020.

[33] K. Lata, C. Gupta, and L. R. Cenkeramaddi, “A cryptographic framework for secure medical imaging in smart healthcare environments,” *Results in Engineering*, 2025.

[34] W. Feng et al., “Integrating fractional-order Hopfield neural network with differentiated encryption: Achieving high-performance privacy protection for medical images,” *Fractal and Fractional*, 2025.

[35] X.-Y. Wang and X.-L. Du, “Pixel-level and bit-level image encryption method based on logistic-Chebyshev dynamic coupled map lattices,” *Chaos, Solitons & Fractals*, 2021.

[36] H. R. Shakir et al., “A new four-dimensional hyper-chaotic system for image encryption,” *International Journal of Electrical and Computer Engineering*, 2023.

[37] M. Thomas, V. Krishna, and M. Varghese, “Image encryption algorithm with block scrambling based on logistic map,” *Indian Journal of Science and Technology*, vol. 16, no. 14, 2023.

[38] U. Erkan et al., “An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN,” *Multimedia Tools and Applications*, 2020.

[39] K. Raghuvanshi et al., “Image encryption algorithm based on DNA encoding and CNN,” *Expert Systems with Applications*, 2024.

[40] S. Subathra and V. Thanikaiselvan, “Enhanced security for medical images using a new 5D hyper chaotic map and deep learning based segmentation,” *Scientific Reports*, 2025.

[41] W. Alexan et al., “A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations,” *Scientific Reports*, 2025.

[42] Y. Abdul et al., “A dynamic image encryption scheme through 2-D cellular automata and chaotic logistic map,” 2025.

[43] A. N. Latifa et al., “Multi-level secure image cryptosystem using logistic map chaos: Entropy, correlation, and 3D histogram validation,” *Jurnal Masyarakat Informatika*, 2025.

[44] E. Güvenoğlu, “An image encryption algorithm based on multi-layered chaotic maps and its security analysis,” *Connection Science*, 2024.

[45] N. Iqbal et al., “An efficient hybrid encryption model based on deep convolutional neural networks, DNA computing and chaotic system,” *Multimedia Tools and Applications*, 2022.

[46] S. Minocha et al., "Adaptive image encryption approach using an enhanced swarm intelligence algorithm," *Scientific Reports,* 2025.

[47] K. Revathi et al., "An efficient image encryption algorithm using a discrete memory-based logistic map with deep neural network," *Journal of Engineering and Applied Science,* 2024.

[48] K. He, X. Zhang, S. Ren, and J. Sun, "Identity mappings in deep residual networks," in *Proc. ECCV,* 2016.

[49] Z. Liu et al., "A two-branch ResNet-BiLSTM deep learning framework for extracting multimodal features," *Sensors,* 2025.

[50] National Institutes of Health, "ChestX-ray14: Hospital-scale chest X-ray database and benchmarks," Kaggle.

[51] A. Jolfaei and A. Mirghadri, "Image encryption using chaotic maps and hash functions," *Multimedia Tools and Applications,* 2019.

[52] L. Teng et al., "A novel chaotic image encryption algorithm based on bit-level permutation," *IEEE Access,* 2021.

[53] S. Behnia et al., "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals,* 2008.

[54] X. Chai et al., "A novel color image encryption algorithm based on DNA sequence and chaotic system," *Optik,* 2017.

[55] Abuali, T. M., & Algamaty, R. K. (2025). Analyzing AI Applications in Improving Patient Experience: From Diagnosis to Recovery. *The Open European Journal for Research in Medical and Basic Sciences (OEJRMBS),* 36-47.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of ALBAHIT and/or the editor(s). ALBAHIT and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content