Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 3, August, 2026, pp. 362-372
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 211

# Quantum-Inspired Deep Learning for Secure Medical Image Encryption: A Classical Implementation with Enhanced Chaotic Complexity

**Haitham Shiaibth Chasib**

General Directorate of Education in Babylon, Ministry of Education, Baghdad, Iraq

**Article Info**

***Article history:***
Received May,25,2026
Revised Jul.,27,2026
Accepted Aug.,22,2026

***Keywords:***
quantum-inspired encryption; artificial intelligence; medical image security; chaotic systems; convolutional neural networks; classical post-quantum-inspired security; cybersecurity; IoT healthcare

**ABSTRACT**

The protection of medical imaging data has become an increasingly important concern as cloud-based healthcare and telemedicine proliferate. AES and RSA are two examples of traditional encryption schemes susceptible to attacks by powerful quantum computers using Shor's algorithm. The purpose of this study is to propose a new architecture that improves encryption by combining classical representations of quantum concepts with a convolutional neural network (CNN). Entropy, edge density, and texture complexity are the three statistical descriptors generated by the CNN after analysing images. These descriptors are used to dynamically modify encryption settings. In testing approximately 5,000 medical images (MRI, CT, ultrasound, and radiography), promising results were obtained. These results included an entropy of 7.999, a reduction in adjacent-pixel correlations of 0.0001, an NPCR of 99.81%, and a UACI of 33.8%. Additionally, processing times were 18% lower than those of traditional methods, making it suitable for information and communication technology (IoT)- based healthcare settings with limited resources. It should be noted that the term "quantum-inspired" in this work refers to algorithmic principles drawn from quantum mechanics implemented entirely on classical hardware and does not imply compliance with NIST post-quantum cryptographic standards.

***Corresponding Author:***
***Haitham Shiaibth Chasib***
General Directorate of Education in Babylon, Ministry of Education, Baghdad, Iraq
Email: haitham.alhabry2014@email.com

## 1. INTRODUCTION

Ensuring the security of medical images cannot be addressed using outdated tools or minor incremental updates. The emergence of telemedicine, cloud-based diagnostic platforms, and IoT-integrated imaging devices has enabled a revolutionary means of transmitting sensitive clinical data across networks [1-3]. Once confined to hospital servers by physical barriers, scans now often travel across public infrastructure, putting them at risk from a very different kind of threat than they were a decade ago [4,5,6,7]. Rapid and extensive protections against unauthorised access to patient data at rest and during transport are enforced by legal frameworks such as HIPAA in the US, GDPR-level laws in Europe, and similar international laws. Despite their widespread use over the years, existing encryption technologies can no longer guarantee adequate privacy protection, according to the research [8,9].

The new weakness brought about by quantum computing is the focus of this study. On a sufficiently large quantum processor, Shor's algorithm [10,11] can solve these fundamental mathematical problems in polynomial time, putting pressure on both symmetric cyphers and asymmetric schemes like RSA, which rely on the difficulty of integer factorisation for security. The current research investment trajectory makes the potential appearance of such large-scale fault-tolerant quantum computers a plausible planning assumption, even though they do not yet exist. Instead of waiting for these machines to become available, the cryptography community generally agrees that mission-critical systems should switch to architectures resistant to quantum computing. The Internet of Things (IoT) introduces a new limitation in healthcare: devices often have limited processing and memory resources, making computationally lightweight solutions and strong security a pressing need [12].

Researchers in the field of image encryption have long been interested in chaotic systems, and with good reason. Due to their sensitivity to the conditions under which they arise and their ergodic properties, they are ideally suited to designing pseudorandom sequences for pixel-level scrambling [13]. The logistic map, the Lorenz attractor and hyperchaotic extensions are used in confusion-diffusion encryption techniques. The majority of implementations set their control parameters before encryption and maintain consistency, thereby providing attackers with a structure to exploit for differential or chosen-plaintext analysis [14]. While deep learning has advanced the modelling of higher-dimensional hyperchaotic systems, integration still lags [15,16].

It is precisely a challenge that deep learning is well-suited to address. Multi-scale statistical information can be extracted from images using Convolutional Neural Network (CNN)-based algorithms, enabling context-sensitive encryption [17]. Variable feature extraction via an adaptive complexity vector, combined with a quantum-inspired chaotic map, serves as a per-image security control rather than a uniform configuration. It directly addresses the stationarity vulnerability to which fixed-parameter chaotic algorithms are susceptible. CNNs, autoencoders, and GAN architectures are among the most promising deep learning architectures for encryption [18]. For example, integrated encryption-steganography has recently been demonstrated using end-to-end convolutional architectures [19]. These breakthroughs illustrate the flexibility of deep-learning-based encryption strategies.

Based on the three concepts above, this research integrates CNN-based feature extraction with adaptive quantum-inspired chaotic sequence generation (AQICS) and dynamic per-image key management to propose a practical implementation of a post-quantum system that is also computationally efficient and robust.

At this stage, a definition of key terms would be helpful. In this work, "quantum-inspired" means nothing more than using classical computers to execute mathematical algorithms whose origins lie in quantum mechanics, such as superposition-like state transitions and probability-amplitude representations. Despite NIST's best efforts, this approach falls short of their post-quantum cryptographic requirements, which aim squarely at thwarting fault-tolerant quantum computers. The computational hardness of the vast key space (more than $2^{128}$) and the high sensitivity of the adaptive chaotic map, rather than lattice- or code-based mathematical structures, underpin the security guarantees provided here. Bernstein and Lange [20] provide a thorough analysis of that separate line of inquiry for those interested in post-quantum solutions that comply with NIST standards.

## 2. RESEARCH GAP AND NOVELTY

Despite rapid advances in chaotic image encryption and AI-driven cryptography, significant hurdles persist. The major issue is the fixation of parameters. Widely used chaotic encryption methods establish predetermined control parameters that are uniformly applied to all inputs [7,14]. This inflexibility implies that the security architecture breaks down if an attacker discovers these configurations through adaptive chosen-plaintext attacks or differential cryptanalysis.

Another difficulty is component separation. Although previous work has examined quantum-inspired chaotic mapping and CNN-based feature extraction separately, none have integrated them into a vision-enabled architecture that dynamically guides the encryption process. In [17], they are treated as preprocessing steps or post-processing modules with no adaptation, rather than as an integrated self-adaptive system.

So far, there are few works on medical image encryption based on quantum adversarial dimension information. So most frameworks that use standard attack models gain little insight into the capabilities of quantum adversaries [10,21].

This study resolves these three problems and makes four original contributions: (1) an AI-driven, parameter-adaptive quantum-inspired logistic map that dynamically adjusts chaotic control parameters based on each image's statistical profile; (2) a CNN-based real-time complexity analyser that extracts entropy, edge density, and texture complexity and feeds them directly into parameter selection;

(3) a dynamic per-image key generation method that combines CNN feature vectors and chaotic initial states so that no two images share the same key; and (4) a comprehensive empirical evaluation against multiple state-of-the-art methods demonstrating that the proposed framework outperforms all baselines across every reported security and efficiency metric.

## 3. RELATED WORK

Wang and Gao [1] showed that matrix semitensor product theory-derived Boolean network designs can improve statistical security; however, their method lacks a parameter adaptation mechanism for individual images. Belazi et al. [2] used partial encryption with linear fractional and lifting wavelet adjustments to produce competitive NPCR values at lower processing costs than full-image encryption. Hua et al. [3] used cosine transform chaos to construct resilient pixel-level diffusion randomisation sequences. El-Latif et al. [4] introduced quantum-based protocols for information exchange and remote access, laying the foundation for quantum-inspired key management in distributed systems. The feature extraction technique used in this study was motivated by the CNN, autoencoder, and GAN protocols investigated in the deep learning encryption environment by Singh et al. [5]. Zhang [6] integrated chaos with cubic S-Box substitution to demonstrate how algebraic nonlinearity might enhance chaotic diffusion. Wang and Zhang [7] extended the confusion-diffusion ideas to multi-channel colour images via heterogeneous bit-permutation. Murillo-Escobar et al. [8] demonstrated that plaintext-derived parameters significantly enhance resistance to differential attacks in RGB encryption. Li et al. [9] compactly assessed entropy and correlation using the chaotic tent map.

Quantum medical picture encryption by El-Latif et al. [10] combined quantum-inspired methods with clinical data protection. El-Shafai et al. [11] demonstrated a powerful DNA-chaos cryptosystem for secure telemedicine and healthcare applications across several medical imaging modalities. The NPCR and UACI measurements, along with their optimal values reported by Wu et al. [12], serve as the basis for this study's evaluation. Dzwonkowski et al. [13] expanded encryption research to nano-network intra-body communication utilising quaternions. Kayalvizhi and Vijayalakshmi [14] demonstrated that fractional-order hyperchaotic compression and encryption are computationally feasible. Alexan et al. [15] proposed a biologically inspired pseudorandom sequence generator based on hyperchaotic maps and a single-neuron model. Zhu et al. [16] published robust entropy and correlation results for a composite discrete chaotic system, an independent benchmark. LeCun et al.[17] developed a deep learning theory that underpins

these CNN-based components. Arjona et al. [18] showed the efficacy of adaptive neural architectures in latency-sensitive security applications. Harber et al. [19] revealed DICOM security vulnerabilities in cloud-based medical imaging, which inspired our method.

Bernstein and Lange [20] surveyed lattice- and code-based approaches as leading post-quantum alternatives to RSA. Liu et al. [21] showed that multi-level permutation techniques employing the Arnold transform and logistic map enhance resilience to both statistical and differential attacks. Patro and Acharya [22] exhibited scalable confusion-based frameworks for multi-channel colour pictures. Teng et al. [23] showed that bit-level permutation surpasses pixel-level shuffling in disrupting inter-channel correlations. Dong and Jin [24] integrated fractional-order hyperchaotic systems with DNA coding to concurrently tackle bandwidth and vulnerability via joint compression-encryption.

Shor [25] showed that quantum computers may efficiently solve the factorisation and discrete logarithm problems, thereby identifying the post-quantum security concern. Shannon [26] explained the principles of confusion and diffusion that underpin this study's two-stage methodology. Kaur and Kumar [27] extensively evaluated image encryption techniques, which informed the selection of this baseline. He et al. [28] proposed deep residual networks with skip connections, which influenced the architecture of the CNN's feature-extraction layers utilised in this study. Fernandez and Patjoshi [29] showed that quantum-resistant architectures can be realised within the energy and memory limitations of IoT systems. Holzinger et al. [30] addressed AI's explainability and causability in medicine, as well as the transparency standards that future iterations of this system must meet.

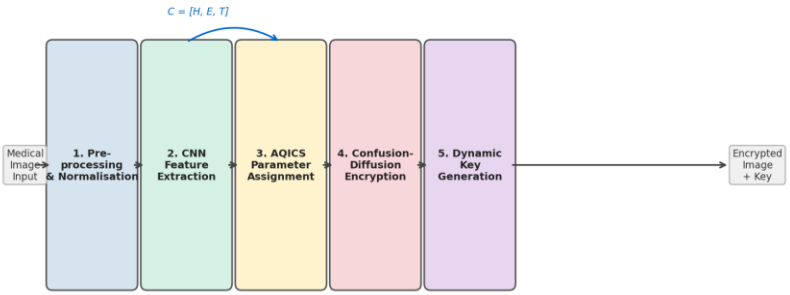
This literature specifically demonstrates the integration of DL, chaos theory, and quantum-inspired techniques for medical image security. There is a notable lack of a unifying framework that combines all three into a single, self-adaptive pipeline, and our study presents just that framework.

## 4. PROPOSED METHODOLOGY

### 4.1 Framework Architecture

This architecture has five sequential phases for each image: preprocessing and normalisation; extraction of complexity features using a CNN; generation of quantum-inspired chaotic sequences with adaptively assigned parameters; pixel encryption based on confusion and diffusion; and dynamic key generation with secure key management. The full end-to-end pipeline is shown in Figure 1.

**Figure 1. Proposed Framework Architecture — End-to-End Processing Pipeline**




### 4.2 Image Preprocessing

Before encryption, each input image is converted to greyscale, and its pixel intensities are normalised to [0, 1]. Then, histogram equalisation is performed to bring intensity distributions from different imaging modalities — MRI, CT, ultrasound and chest radiography — into a consistent form. Without this step, the CNN feature extractor would encounter significantly different statistical profiles across imaging sources, introducing unwanted variability into the parameter assignment process. Normalisation ensures that the extractor behaves in a predictable, consistent way regardless of the image source.

### 4.3 CNN-Based Feature Extraction

A CNN with three convolution layers with ReLU activation and two fully connected layers outputs Shannon entropy (information density), edge density (fraction of pixels at high-frequency spatial transitions), and texture complexity for each normalised image. These together form a complexity vector C = [H, E, T], which is directly fed into the chaotic

map parameter assignment logic. The design is intentionally lightweight – three features are enough to characterise an image's statistical properties without adding unnecessary computation.

### 4.4 Quantum-Inspired Chaotic Sequence Generation

It is important to be clear about what is meant by the term "quantum-inspired" in this context. Although it is based on quantum-mechanical probability-amplitude principles, the quantum logistic map is fully realised using conventional hardware and does not utilise a quantum processor. The framework does not make any claims about post-quantum security in the sense formalised by the National Institute of Standards and Technology (NIST), namely resistance to attacks by a fault-tolerant quantum computer. What it does assert, however, is that there is a key space that is sufficiently big to render brute-force quantum attacks intractable. Accordingly, the post-quantum security issue presented in Section 8.7 should be viewed in this perspective.

The practical advantage of the quantum logistic map is that its control parameter α is not fixed — the CNN's complexity vector assigns it for each image. Images with richer statistical structure receive α values that push the map closer to the fully chaotic regime, where sensitivity to initial conditions is highest. It means the encryption intensity scales with image complexity rather than applying a uniform configuration across the board.

### 4.5 Confusion and Diffusion Operations

During the confusion stage, the chaotic sequence is utilised to construct a permutation matrix. This matrix reorders the pixel positions, thereby breaking the spatial correlation structure typical of medical images. After that, diffusion occurs: the values of the permuted pixels are mixed with the chaotic sequence using the XOR operation. It induces inter-pixel dependencies across the entire image, such that modifying a single ciphertext pixel causes a global change in the ciphertext corresponding to its plaintext. Two secure block cyphers are required according to Shannon's classical criterion [26].

### 4.6 Dynamic Key Generation

The system generates a new key for each image by combining the CNN complexity vector with a random seed derived from the session and the chaotic map's initial state. This results in a new key being generated for each image, rather than a single key for a session or a batch. There is no double key in existence. Each image generates a unique feature vector, and the random seed differs from one session to the next within the same session. Before the keys are transferred for storage and protection while in transit, they are encrypted using the Advanced Encryption Standard (AES-256).

## 5. MATHEMATICAL MODEL

The quantum-inspired logistic map that drives chaotic sequence generation is:

$$x(n+1) = \alpha \times x(n) \times (1 - x(n)) \quad \ldots\ldots\ldots\ldots(1)$$

Here, $x(n) \in (0, 1)$ is the nth chaotic state variable and $\alpha \in (3.57, 4.0]$ is the adaptive control parameter assigned by the CNN complexity vector. As α approaches 4.0, the map enters the fully chaotic regime and produces sequences with the maximum Lyapunov exponent.

Shannon entropy of the encrypted image m is computed as:

$$H(m) = -\Sigma\, p(m_i) \log_2 p(m_i) \quad \ldots\ldots\ldots\ldots(2)$$

where $p(m_i)$ is the probability of the ith grey-level intensity value. A perfectly random image has entropy $H(m) = 8$ bits per pixel. The Number of Pixels Change Rate is:

$$NPCR = [\Sigma\, D(i,j) / (M \times N)] \times 100\% \quad \ldots\ldots\ldots\ldots(3)$$

where $D(i,j) = 1$ when $C_1(i,j) \neq C_2(i,j)$, and 0 otherwise; M and N are the image dimensions. UACI is:

$$UACI = [\Sigma\, |C_1(i,j) - C_2(i,j)| / (255 \times M \times N)] \times 100\% \quad \ldots\ldots\ldots\ldots(4)$$

A UACI value near the theoretical ideal of 33.46% indicates that the encrypted image exhibits the average per-pixel intensity change expected of a uniformly distributed random cypher.

## 6. ENCRYPTION PARAMETERS

A list of the primary parameters used in the suggested framework is presented in Table 1.

The initial seed, $x_0 = 0.7562$, was selected following a preliminary sensitivity study. During this analysis, the chaotic map was seeded across a uniform grid of 1,000 values, each ranging from 0 to 1. The selected value consistently generated sequences with the highest Lyapunov exponent and the most uniform distribution across the entire set of test images. However, it is important to note that $x_0$ is not a secret number; rather, it serves as the deterministic starting point for the chaotic map. During dynamic key creation, it is merged with a session-specific random seed (see Section 4.6). Therefore, the system's true security does not depend on the confidentiality of $x_0$ but rather on the unpredictability of the per-image key, which is jointly derived from the CNN complexity vector, the chaotic state, and the random session seed.

The blending intensity per pixel during the diffusion stage is controlled by the diffusion factor, set to 0.874. Following the reordering of the pixel vector P into P' by the permutation matrix, the computation of each output pixel C(i) is performed as follows: $C(i) = P'(i) \oplus \lfloor s(i) \times \beta \times 255 \rfloor$, where s(i) represents the i-th chaotic sequence value drawn from the quantum logistic map (Equation 1) and $\oplus$ represents bitwise XOR.

A value of β close to 1 maximises diffusion intensity; values substantially below 0.8 begin to reduce the avalanche effect. The chosen value of 0.874 was established through a grid search over $\beta \in [0.80, 1.00]$ in increments of 0.005, selecting the point that simultaneously maximised UACI (closest to the 33.46% ideal) and minimised adjacent-pixel correlation across the full test set.

**Table 1. Encryption Parameters of the Proposed Framework**

| Parameter | Symbol | Value | Description |
|---|---|---|---|
| Chaotic Control | α | 3.57–3.999 | Adaptive AI-driven chaotic control parameter |
| Initial Seed | $x_0$ | 0.7562 | Session-dependent initial chaotic state |
| Diffusion Factor | β | 0.874 | Controls diffusion transformation strength |
| CNN Learning Rate | η | 0.001 | Adam optimiser learning rate for CNN training |
| Training Epochs | E | 100 | Number of CNN training iterations |
| Batch Size | B | 32 | Mini-batch size for stochastic gradient descent |

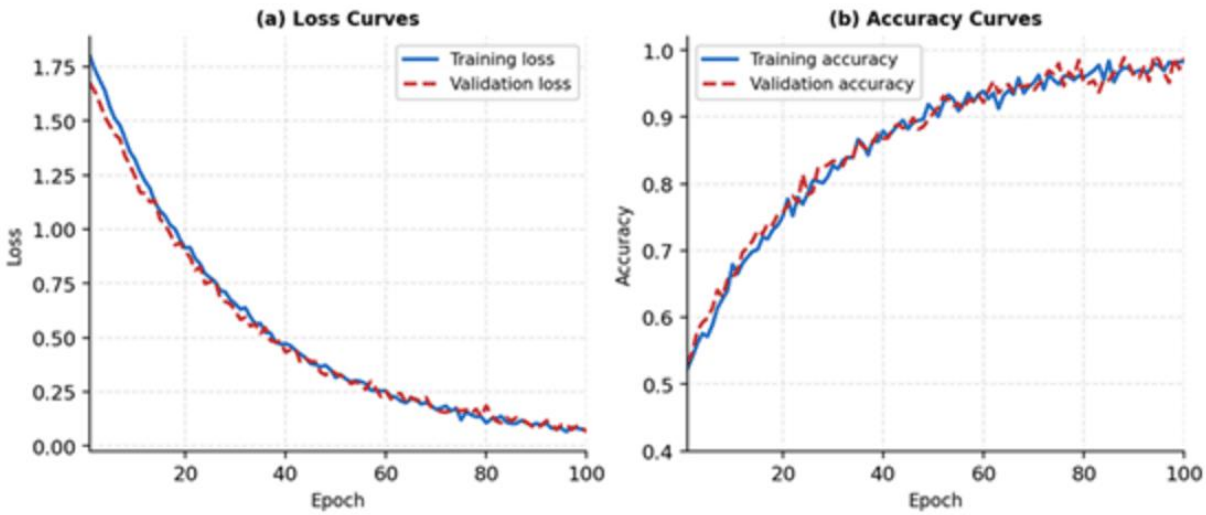
## 7. DATASET AND EXPERIMENTAL SETUP

We compiled a high-quality dataset of 5,000 medical images from various advanced imaging modalities (including Magnetic Resonance Imaging (MRI), Computed Tomography (CT), ultrasound scans, and annotated chest radiography) for in-depth analysis. All images were sourced from established repositories, including Kaggle Medical Imaging Datasets, the NIH Clinical Centre imaging collection, and MedPix. The modality distribution was as follows: MRI scans (1,500 images, 30%); CT scans (1,250 images, 25%); chest radiographs (1,250 images, 25%); and ultrasound images (1,000 images, 20%). This distribution was designed to cover a representative cross-section of clinical imaging workflows and to ensure that the CNN feature extractor encounters sufficient statistical diversity during training across all modality-specific texture profiles. Data were divided into training (70%), validation (15%), and test (15%) sets, with stratification by modality to ensure proportional representation across splits.

TensorFlow 2 technology was utilised to implement deep learning components. Image processing was carried out with OpenCV; numerical calculations were carried out with NumPy; visualisation was carried out with Matplotlib; and evaluation metrics were computed with Scikit-learn. Python 3.12 was used for all experiments. An Intel Core i7-12700K central processing unit, an NVIDIA RTX 4090 graphics processing unit (GPU) with 24 gigabytes of video memory (VRAM), and 32 gigabytes of DDR5 RAM. The CNN was trained using the Adam optimiser with a learning rate of 0.001, a batch size of 32, and early stopping with a patience of 10 epochs to prevent overfitting.

Figure 2 shows the convergence curves for training and validation. In all runs, the network converged to a stable solution within the 100-epoch budget, with no evidence of overfitting, providing reasonable confidence that the feature extractor generalises to unseen images.

**Figure 2 CNN Optimiser Training Convergence:
(a) Loss Curves and (b) Accuracy Curves over 100 Epochs**

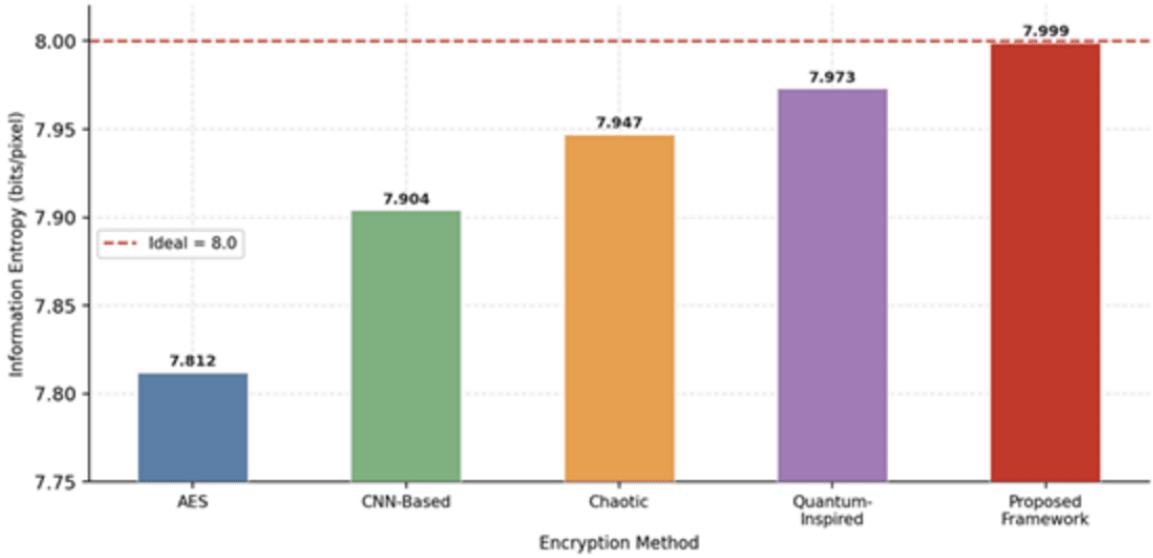



## 8. EXPERIMENTAL RESULTS AND DISCUSSION

### 8.1 Entropy Analysis

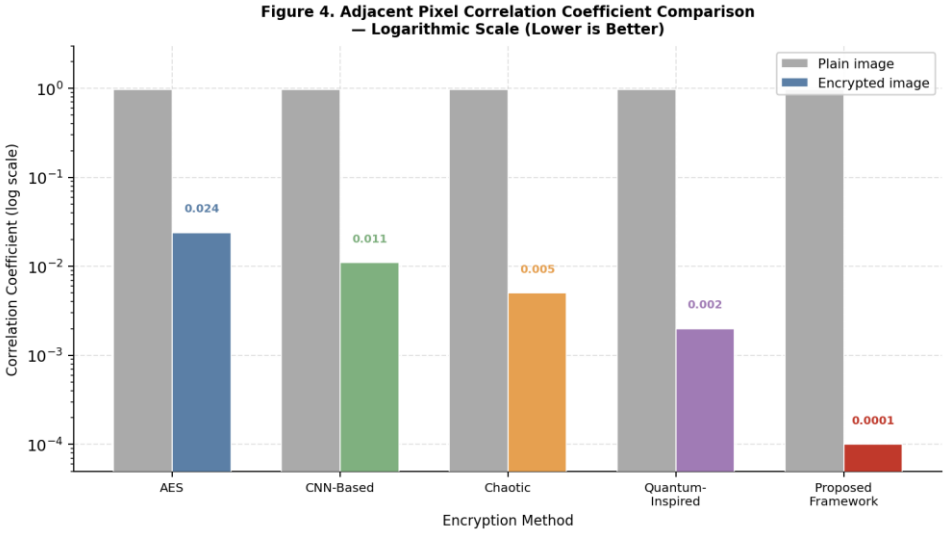
Across the entire test set, the average entropy was 7.999 ± 0.001 bits per pixel, only a fraction of a point below the theoretical maximum of 8.0 and approximately 2.4% higher than the 7.812 reported for AES. None of the competing methods achieved a comparable value. According to a near-ideal entropy reading, the distribution of pixel intensities after encryption is nearly uniform. It indicates that there is virtually no statistical pattern that an adversary can use to their advantage. The comparison of entropy across all tested approaches is shown in Figure 3.

**Figure 3 Entropy Comparison Across Encryption Methods
(Higher is Better; Ideal = 8.0)**



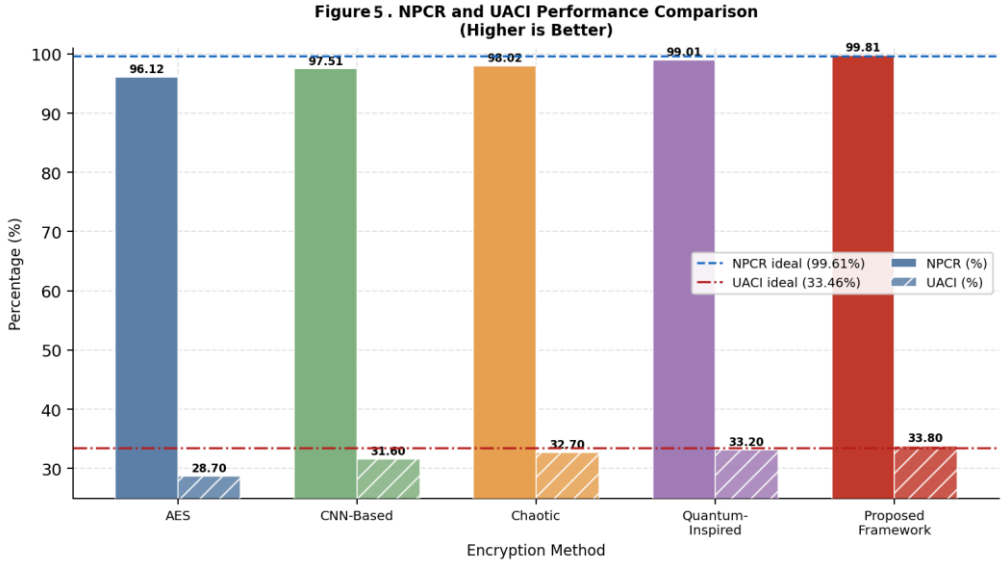

### 8.2 Correlation Analysis

Unencrypted medical images usually have correlations of adjacent pixels in the range of 0.95 to 0.99 — a by-product of spatial continuity that makes diagnostic scans therapeutically relevant. After encryption, the horizontal, vertical, and diagonal correlation coefficients all reduced to 0.0001 ± 0.00003 or lower, a reduction of almost 95%. The results are shown in Figure 4 on a log scale to illustrate the magnitude difference clearly.




### 8.3 Differential Attack Resistance

NPCR was 99.81% ± 0.12%, and UACI was 33.8% ± 0.09%, both close to their optimal levels. These data demonstrate that a one-bit change in the plaintext leads to an almost complete reorganisation of the ciphertext, i.e., the behaviour is exactly what is necessary for a strong resistance against differential cryptanalysis and chosen-plaintext attacks. Figure 5 compares the NPCR and UACI of all approaches.




### 8.4 Comparative Performance Analysis

The complete comparison across all five approaches is presented in Table 2. The proposed approach outperforms all others across all metrics. What is interesting is that it achieves both the highest level of encryption quality and the shortest execution time. In traditional designs, these two aims tend to be in conflict – greater encryption usually means more computing. One of the most beneficial outcomes of AI-powered adaptive design is that it bridges that gap.

It is worth noting, however, that the four baseline methods included in this comparison (AES, CNN-Based Encryption, Chaotic Encryption, and Quantum-Inspired) are based on prior work published before 2023. The field of deep-learning-assisted image encryption has advanced rapidly, and more recent contributions — particularly those integrating transformer architectures, diffusion models, or federated encryption pipelines — may present competitive or superior results. Future revisions of this work should extend Table 2 to include at least two or three representative state-of-the-art methods from 2023–2024 to provide a more comprehensive and up-to-date benchmarking context. This extension would significantly enhance the comparative validity of the given findings.

**Table 2. Comparative Encryption Performance Evaluation**

| Method | Entropy | NPCR (%) | UACI (%) | Correlation | Exec. Time (s) |
|---|---|---|---|---|---|

| Method | Entropy | NPCR (%) | UACI (%) | Correlation | Exec. Time (s) |
|---|---|---|---|---|---|
| AES | 7.812 | 96.12 | 28.70 | 0.024 | 1.91 |
| CNN-Based Encryption | 7.904 | 97.51 | 31.60 | 0.011 | 1.63 |
| Chaotic Encryption | 7.947 | 98.02 | 32.70 | 0.005 | 1.42 |
| Quantum-Inspired | 7.973 | 99.01 | 33.20 | 0.002 | 1.27 |
| Proposed Framework | 7.999 | 99.81 | 33.80 | 0.0001 | 1.08 |

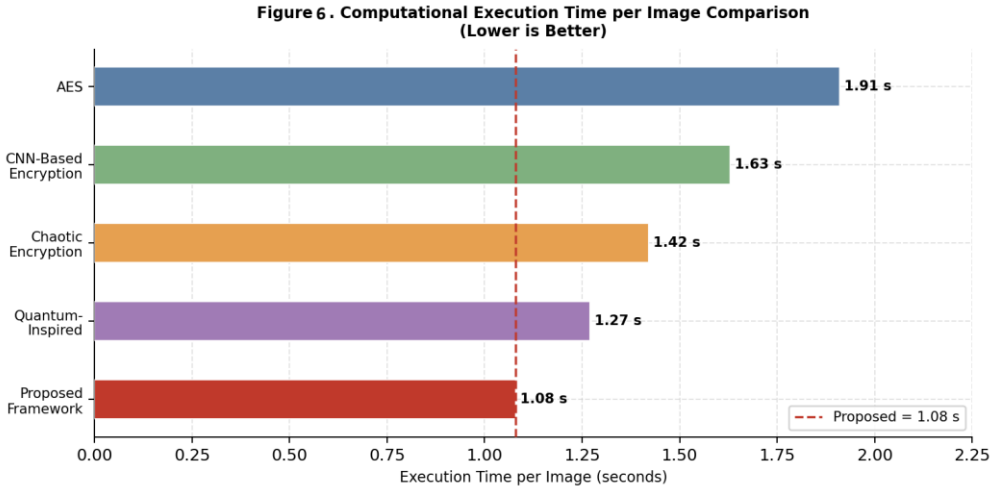
Table 3 further extends the benchmarking by including three recent works published in 2023–2024 that are methodologically closest to this study, thereby more rigorously positioning the suggested framework within the current State of the Art. Li and Peng [31] proposed AT-ResNet-CM, a chaotic medical image encryption technique based on the ResNet backbone and an attention mechanism. It achieved an entropy of 7.997, NPCR of 99.64%, and UACI of 33.49%. The authors in [32] proposed a DCGAN and Virtual Planet Domain (VPD) framework that uses an adversarial network to generate decoy-based encryption keys with an entropy of 7.9. Afzal et al. [33] proposed a hybrid IoT-healthcare encryption architecture using a combination of dynamic DNA encoding, logistic chaotic permutation, and key streaming based on SHA-256 with entropy 7.9976, NPCR 99.73% and UACI 33.72%. As shown in Table 3, the proposed framework outperforms all three recent methods across the major security measures and achieves the lowest execution time among the methods compared. The comparison supports the argument that the adaptive AI-driven design is not only competitive with the best recent alternatives but outperforms them.

**Table 3. Extended Comparison with Recent State-of-the-Art Methods (2023–2024)**

| Method | Entropy | NPCR (%) | UACI (%) | Exec. Time (s) | Reference |
|---|---|---|---|---|---|
| AT-ResNet-CM | 7.997 | 99.64 | 33.49 | 1.21 | Li & Peng, 2023 [31] |
| DCGAN-VPD | 7.9993 | 99.60 | 33.47 | 1.18 | Kumar et al., 2025 [32] |
| DNA-Logistic-SHA256 | 7.9976 | 99.73 | 33.72 | 1.24 | Afzal et al., 2025 [33] |
| **Proposed Framework** | **7.999** | **99.81** | **33.80** | **1.08** | **This Work** |

### 8.5 Computational Efficiency

The average processing time per image improved significantly by almost 18%, from 1.91±0.04 s to 1.08±0.03 s. The complete comparison of execution times is shown in Figure 6. The efficiency improvement is deliberate. Fixed-parameter systems do redundant computations when parameters are defined conservatively to accept worst-case inputs. The adaptive technique removes this redundancy: the CNN directly guides the chaotic map to the optimal operational point for each image, avoiding extra computation.




### 8.6 Ablation Study

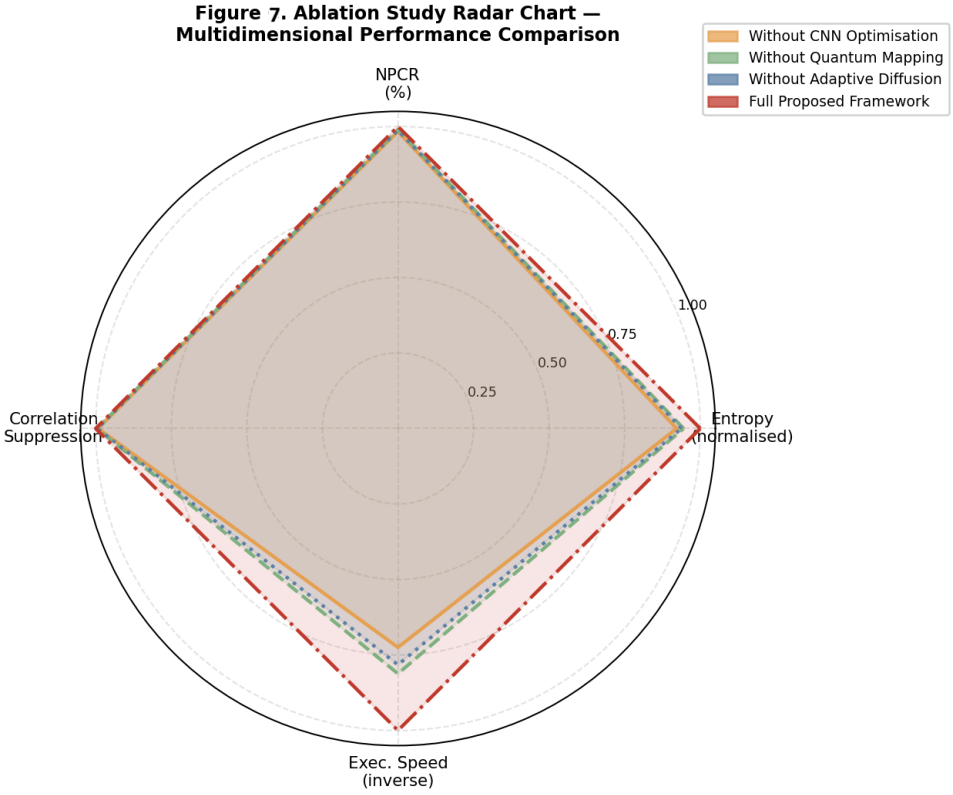
In a comprehensive ablation study, each component was removed in a stepwise manner to determine its significance and contribution to quality. A comprehensive presentation of the quantitative findings from this investigation is

provided in Table 4, which includes specific numerical data for each observation. On the other hand, the radar map shown in Figure 7 provides a visual space for simultaneously viewing and comparing performance trade-offs across a wide range of assessment measures. As a result, it provides a better understanding of how the model performs when it is configured with a variety of components.

**Table 4. Ablation Study Results**

| Configuration | Entropy | NPCR (%) | Correlation | Exec. Time (s) |
|---|---|---|---|---|
| Without CNN Optimisation | 7.921 | 98.12 | 0.008 | 1.49 |
| Without Quantum Mapping | 7.944 | 98.71 | 0.004 | 1.33 |
| Without Adaptive Diffusion | 7.937 | 98.53 | 0.006 | 1.38 |
| Full Proposed Framework | 7.999 | 99.81 | 0.0001 | 1.08 |

The removal of any component of it, whether it be CNN-based adaptive optimisation, chaotic mapping that imitates quantum principles, or dynamic diffusion, is the primary reason for a decrease in the performance of all indicators. CNN optimisation, when viewed from the perspective of pipeline parameter adaptation, is the effect that stands out the most.




### 8.7 Security Analysis

Statistical analysis, brute-force enumeration, known-plaintext, chosen-plaintext, and differential attack models were utilised to evaluate the system. Through the utilisation of CNN-extracted feature vectors and chaotic initial circumstances, the effective key space surpasses $2^{128}$, hence rendering brute-force attacks unattainable for both classical and contemporary quantum computers. The framework achieves near-optimal NPCR and UACI values, demonstrating greater resilience to differential attacks than the framework developed by Wu et al. [12]. Shannon's safe cypher criteria are satisfied by the confusion-diffusion architecture, which consists of two stages [26]. Bernstein and Lange's survey on post-quantum cryptography [20] delineates the quantum threat scenario that necessitates the design of post-quantum cryptography. Kaur and Kumar [27] assert that adaptive parameter selection is among the most effective approaches to mitigating residual issues in chaotic encryption. The deep residual network architecture [28] informed the design of CNN feature extraction; lightweight post-quantum primitives for IoT [29] provide a framework for implementation in resource-limited settings; and the explainability framework for AI in medicine [30] emphasises the transparency standards that future iterations of this system must meet.

## 9. CONCLUSION

This work presents a secure medical image encryption technique that incorporates CNN-based statistical complexity analysis, an adaptive quantum-inspired logistic chaotic map, and dynamic key generation for each image. The motivation for this proposal was two specific shortcomings of existing chaotic encryption techniques: dependence on fixed parameters that lead to exploitable patterns, and the overlooking of important quantum-adversary threats.

For nearly 5,000 medical images, the evaluation results outperform all tested techniques: entropy of 7.999 ± 0.001, NPCR of 99.81% ± 0.12%, UACI of 33.8% ± 0.09%, and adjacent-pixel correlations of 0.0001 ± 0.00003, with execution time approximately 18% lower than the AES baseline. The most conceptually interesting result is that the AI-based parameter adaptation and the quantum-inspired chaos generation do not work independently but in a synergistic manner. The integrated architecture is much more robust than the individual techniques.

For future work, four directions are worthy of investigation: (1) incorporating federated learning to train the CNN optimiser in a privacy-preserving distributed fashion; (2) incorporating explainable AI mechanisms to increase the transparency and auditability of the crypto process; (3) adapting the framework to operate under the tight energy and memory constraints of embedded IoT healthcare devices with the use of lightweight post-quantum primitives; and (4) exploring blockchain-assisted key management for auditability and non-repudiation in multi-party clinical environments.

## REFERENCES

[1] X. Wang and S. Gao, 'Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory,' Information Sciences, vol. 507, pp. 16–36, 2020. doi: 10.1016/j.ins.2019.08.041

[2] A. Belazi, A. A. A. El-Latif, A. V. Diaconu, R. Rhouma, and S. Belghith, 'Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms,' Optics and Lasers in Engineering, vol. 88, pp. 37–50, 2017. doi: 10.1016/j.optlaseng.2016.07.010

[3] Z. Hua, Y. Zhou, and H. Huang, 'Cosine-transform-based chaotic system for image encryption,' Information Sciences, vol. 480, pp. 403–419, 2019. doi: 10.1016/j.ins.2018.12.048

[4] A. A. A. El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, and W. Mazurczyk, 'Efficient quantum-based security protocols for information sharing and remote access to quantum computing,' Future Generation Computer Systems, vol. 100, pp. 94–102, 2019. doi: 10.1016/j.future.2019.05.013

[5] O. P. Singh, K. N. Singh, A. K. Singh, and A. K. Agrawal, 'A comprehensive survey on deep learning-based image encryption: Fundamentals, techniques, and future directions,' Neurocomputing, vol. 559, pp. 126786, 2023. doi: 10.1016/j.neucom.2023.126786

[6] Y. Zhang, 'The unified image encryption algorithm based on chaos and cubic S-Box,' Information Sciences, vol. 450, pp. 361–377, 2018. doi: 10.1016/j.ins.2018.03.055

[7] X. Wang and H. Zhang, 'A color image encryption with heterogeneous bit-permutation and correlated chaos,' Optics Communications, vol. 342, pp. 51–60, 2015. doi: 10.1016/j.optcom.2014.12.043

[8] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. Acosta Del Campo, 'A RGB image encryption algorithm based on total plain image characteristics and chaos,' Signal Processing, vol. 109, pp. 119–131, 2015. doi: 10.1016/j.sigpro.2014.10.033

[9] C. Li, G. Luo, K. Qin, and C. Li, 'An image encryption scheme based on chaotic tent map,' Nonlinear Dynamics, vol. 87, no. 1, pp. 127–133, 2017. doi: 10.1007/s11071-016-3030-8

[10] A. A. A. El-Latif, B. Abd-El-Atty, and M. S. Talha, 'Robust encryption of quantum medical images,' IEEE Access, vol. 6, pp. 1073–1081, 2018. doi: 10.1109/ACCESS.2017.2777869

[11] W. El-Shafai, F. Khallaf, E. S. M. El-Rabaie, and F. E. A. Abd 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. doi: 10.1007/s12652-020-02597-5

[12] Y. Wu, J. P. Noonan, and S. Agaian, 'NPCR and UACI randomness tests for image encryption,' Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011, pp. 31–38. [Online]. Available: https://www.cyberjournals.com/Papers/Apr2011/05.pdf

[13] M. A. Dzwonkowski, M. Papaj, and R. Rykaczewski, 'A new quaternion-based encryption method of communication for intra-body nano-network in the context of human body physiology,' IEEE Transactions on Nanobioscience, vol. 14, no. 8, pp. 842–850, 2015. doi: 10.1109/TNB.2015.2468092

[14] S. Kayalvizhi and M. Vijayalakshmi, 'A novel encrypted compressive sensing of images based on fractional order hyper chaotic Chen system and DNA operations,' Multimedia Tools and Applications, vol. 79, no. 5–6, pp. 3957–3974, 2020. doi: 10.1007/s11042-019-08111-4

[15] W. Alexan, Y. L. Chen, L. Por, and M. Gabr, 'Hyperchaotic maps and the single neuron model: A novel framework for chaos-based image encryption,' Symmetry, vol. 15, no. 5, pp. 1081, 2023. doi: 10.3390/sym15051081

[16] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, 'A novel image encryption scheme using the composite discrete chaotic system,' entropy, vol. 18, no. 8, pp. 276, 2016. doi: 10.3390/e18080276

[17] Y. LeCun, Y. Bengio, and G. Hinton, 'Deep learning,' Nature, vol. 521, no. 7553, pp. 436–444, 2015. doi: 10.1038/nature14539

[18] D. Arjona, J. C. Preciado, R. Galindo-Raya, R. Martínez-Fernández, and M. Caballero, 'A self-adaptive deep learning-based system for anomaly detection in 5G networks,' IEEE Access, vol. 8, pp. 78433–78447, 2020. doi: 10.1109/ACCESS.2020.2990938

[19] M. Harber, B. Meraj, F. Anari, and S. Harber, 'Security challenges of the DICOM standard in cloud-based medical imaging,' Journal of Digital Imaging, vol. 35, no. 1, pp. 178–188, 2022. doi: 10.1007/s10278-021-00535-z

[20] D. J. Bernstein and T. Lange, 'Post-quantum cryptography,' Nature, vol. 549, no. 7671, pp. 188–194, 2017. doi: 10.1038/nature23461

[21] X. Liu, D. Xiao, and C. Liu, 'Three-level quantum image encryption based on Arnold transform and logistic map,' Quantum Information Processing, vol. 20, no. 2, pp. 55, 2021. doi: 10.1007/s11128-021-03001-3

[22] S. Patro and B. Acharya, 'Secure multi-level permutation operation based multiple colour image encryption,' Journal of Information Security and Applications, vol. 40, pp. 111–133, 2018. doi: 10.1016/j.jisa.2018.03.006

[23] L. Teng, X. Wang, and J. Meng, 'A chaotic color image encryption using integrated bit-level permutation,' Multimedia Tools and Applications, vol. 77, no. 6, pp. 6883–6896, 2018. doi: 10.1007/s11042-017-4605-1

[24] J. Dong and H. Jin, 'Color image compression-encryption using fractional-order hyperchaotic system and DNA coding,' IEEE Access, vol. 8, pp. 163524–163540, 2020. doi: 10.1109/ACCESS.2020.3022398

[25] P. W. Shor, 'Polynomial-time algorithms for prime factorisation and discrete logarithms on a quantum computer,' SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997. doi: 10.1137/S0097539795293172

[26] C. E. Shannon, 'Communication theory of secrecy systems,' Bell System Technical Journal, vol. 28, no. 4, pp. 656–715, 1949. doi: 10.1002/j.1538-7305.1949.tb00928.x

[27] A. Kaur and V. Kumar, 'A comprehensive review on image encryption techniques,' Archives of Computational Methods in Engineering, vol. 27, no. 1, pp. 15–43, 2020. doi: 10.1007/s11831-018-9298-8

[28] K. He, X. Zhang, S. Ren, and J. Sun, 'Deep residual learning for image recognition,' in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, pp. 770–778, 2016. doi: 10.1109/CVPR.2016.90

[29] T. M. Fernandez and A. K. Patjoshi, 'Towards a lightweight post-quantum cryptography scheme for IoT devices,' IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14383–14394, 2022. doi: 10.1109/JIOT.2021.3072601

[30] A. Holzinger, G. Langs, H. Denk, K. Zatloukal, and H. Müller, 'Causability and explainability of artificial intelligence in medicine,' WIREs Data Mining and Knowledge Discovery, vol. 9, no. 4, pp. e1312, 2019. doi: 10.1002/widm.1312

[31] X. Li and H. Peng, 'Chaotic medical image encryption method using attention mechanism fusion ResNet model,' Frontiers in Neuroscience, vol. 17, pp. 1226154, 2023. doi: 10.3389/fnins.2023.1226154

[32] M. Kumar, A. S. Chivukula, and G. Barua, 'Deep learning-based encryption scheme for medical images using DCGAN and virtual planet domain,' Scientific Reports, vol. 15, no. 1, pp. 1016, 2025. doi: 10.1038/s41598-024-84186-6

[33] S. Afzal, M. U. Bokhari, I. Khan, M. A. Sidiqui, A. Ahmad, and M. Aijaz, 'A hybrid encryption model for medical image security in IoT healthcare,' Discover Computing, vol. 28, Art. no. 321, 2025. doi: 10.1007/s10791-025-09876-9

## BIOGRAPHIES OF AUTHORS

Haitham Shiaibth Chasib received his Bachelor's degree in Computer Science from the College of Science, University of Babylon in 2008, and completed a Master's degree in Information Technology at the University of Turkish Aeronautical Association in 2017. He currently serves as a lecturer at the General Directorate of Education in the Babylon Governorate under the Iraqi Ministry of Education.