iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VIII **Month of publication:** August 2026

DOI: https://doi.org/10.22214/ijraset.2026.84733

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com

Content-Aware DNA-Coded Cryptosystem for Skin Lesion Image Confidentiality in IoMT

Bellapu Lakshmi Amulya
M. Tech, Computer Science Engineering Dept, UCEK, JNTU Kakinada, Andhra Pradesh, India

Abstract: ***Teledermatology screening pipelines routinely transmit patient dermoscopic skin lesion images across Internet of Medical Things (IoMT) networks, where diffusion strength is conventionally applied uniformly across an image without regard to local visual complexity, an inefficiency increasingly addressed in general IoT image security through lightweight CNN-based content classifiers but largely unexplored for dermoscopic imaging. This work proposes a content-aware alternative in which a lightweight Convolutional Neural Network (CNmost existing chaos-DNA encryption schemes apply a fixed diffusion strength...N) first analyses each image to extract entropy, texture, and edge-density descriptors; an adaptive decision module then converts this feature vector into an image-specific chaos-strength parameter and DNA mutation block level before any encryption occurs. Independently, an 8-qubit quantum circuit executed on Qiskit generates a true quantum random bitstream via Hadamard superposition and computational-basis measurement; this stream is fused with the image's own SHA-384 digest to derive a hybrid initial condition for a 3D Logistic-Sine hyperchaotic map, whose three output sequences are respectively assigned to spatial scrambling, DNA-level mutation, and XOR diffusion. Each RGB channel is processed independently through Haar-wavelet scrambling, adaptive Bio-DNA encoding and mutation, and quantum-keyed diffusion. Evaluated on 600 dermoscopic skin lesion images from the ISIC archive, the framework attains 7.9887-bit average entropy, 99.6128% NPCR, 33.4377% UACI, near-zero adjacent-pixel correlation (0.0161), and fully lossless decryption (MSE = 0) in an average of 0.64 seconds per image confirming that content-aware, CNN-guided diffusion strength is compatible with strong statistical security and real-time IoMT deployment.***

Keywords: ***Dermoscopy, Melanoma screening, IoMT security, Convolutional Neural Network, Adaptive encryption, Quantum random number generation, Qiskit, DNA-inspired pixel diffusion, Medical image cryptosystem.***

I. INTRODUCTION

Teledermatology screening has become one of the most widely deployed tele-diagnostic workflows in Internet of Medical Things (IoMT) healthcare. Dermoscopy-equipped capture devices at primary-care clinics, rural health centres, and mobile diagnostic units acquire high-resolution skin lesion images and transmit them, frequently over public or semi-trusted communication networks, to centralized dermatology servers for melanoma detection and clinical assessment. This enables early diagnosis, reduces unnecessary hospital visits, and improves healthcare accessibility for patients in geographically remote regions. Because these images contain patient-identifiable diagnostic information, ensuring their confidentiality, integrity, and authenticity during transmission and cloud storage is a critical security requirement. Any unauthorized disclosure or modification of dermoscopic images may compromise patient privacy, affect clinical decision-making, and violate healthcare data protection regulations.

Yet image data resists direct application of conventional block ciphers. The strong pixel-to-pixel correlation, high redundancy, and large data volume that make medical images diagnostically valuable also make naïve AES or DES implementation computationally expensive and, in certain operating modes, statistically vulnerable. Furthermore, conventional cryptographic algorithms are not specifically designed to exploit the structural characteristics of image data, resulting in increased processing overhead and reduced suitability for real-time IoMT environments where latency and computational efficiency are equally important.

This has driven three overlapping research directions: chaos-based permutation-diffusion, Bio-DNA-level encoding, and, most recently, quantum-assisted seed generation. Chaos-based techniques provide high sensitivity to initial conditions and generate pseudo-random sequences for secure permutation and diffusion, while DNA computing introduces biologically inspired encoding and mutation operations that significantly increase encryption complexity. Quantum-assisted methods further strengthen the randomness of secret key generation by exploiting quantum superposition and measurement principles, thereby enlarging the effective key space and improving resistance against brute-force and statistical attacks.

Separately, edge-AI and IoT image-security research has begun using lightweight CNN classifiers to route images or regions toward different protection levels based on content complexity, reducing wasted computation on low-risk regions while concentrating protection where it matters. This content-aware philosophy, however, has not yet been applied to the chaos-DNA-quantum encryption pipeline commonly used for dermoscopic medical imaging, where lesion-relevant detail and plain skin background are still encrypted with identical strength. This paper closes that specific gap by using a lightweight CNN to analyse each image's own content complexity and adaptively determine the encryption parameters before the quantum-hyperchaotic encryption stage begins. The extracted image features, including entropy, texture, edge density, and sharpness, are processed by an adaptive decision module to dynamically select the chaos strength and DNA mutation level. In addition, quantum amplitude encoding and Qiskit-based quantum random number generation are employed to initialize hybrid cryptographic seeds, which are subsequently fused with SHA-384 hashing and utilized by a 3D Logistic-Sine hyperchaotic system for secure key generation. The resulting adaptive multi-domain encryption framework combines discrete wavelet transform (DWT)-based scrambling, Bio-DNA encoding and mutation, and XOR diffusion to achieve enhanced security, improved randomness, and efficient execution suitable for real-time teledermatology and IoMT-based medical image transmission.

A. The Need for Content-Adaptive Medical Image Encryption

A secure dermoscopic-image cryptosystem should ideally satisfy three simultaneous requirements: the encryption key must depend on the specific image content (defeating chosen-plaintext attacks that exploit key reuse); diffusion strength should track the local visual complexity of each image rather than being applied uniformly; and the randomness underlying key generation should be as close to genuinely unpredictable as practically achievable. Existing chaos-DNA hybrid schemes typically satisfy at most one or two of these requirements at a time, as detailed in Section II.

B. CNN-Guided Adaptive Encryption Strength

Rather than applying a fixed DNA block size or a fixed chaotic coupling parameter to every image alike, this framework passes each image through a lightweight CNN feature-analysis stage that extracts entropy, texture, and edge-density descriptors. An adaptive decision module then converts this descriptor set into an image-specific chaos-strength parameter and DNA mutation block level, so that visually complex, diagnostically dense lesion regions receive finer-grained, stronger diffusion than plain, low-complexity background without requiring any additional key material to be exchanged, since the decision is derived purely from content already available to both the encryption and decryption pipeline stages.

C. Quantum-Assisted Hybrid Key Initialisation

To seed the hyperchaotic map with genuinely unpredictable initial conditions, an 8-qubit quantum circuit executed on IBM's Qiskit framework is placed into uniform superposition via Hadamard gates and measured in the computational basis, yielding a true quantum random bitstream. This stream is combined with a SHA-384 hash computed over the raw image bytes, tying the resulting seed to both the physical randomness source and the exact image content.

D. Proposed Encryption Framework Overview

The proposed pipeline integrates image preprocessing, CNN-based feature analysis, an adaptive decision module, Qiskit-based quantum random number generation, SHA-384 hybrid seed initialisation, hyperchaotic key-stream generation, and a multi-domain Bio-DNA encryption engine that processes the Red, Green, and Blue channels of a dermoscopic skin lesion image independently. Section III details each stage; Section IV reports empirical security metrics across a 600-image dermoscopic skin lesion test corpus drawn from the ISIC archive.

E. Applications of the Proposed Framework

Beyond melanoma and skin-lesion screening specifically, the framework is applicable to:

- Teledermatology and remote dermoscopic lesion triage pipelines.
- Cloud-hosted PACS/EHR systems requiring per-image key freshness.
- Resource-constrained IoMT gateways and wearable diagnostic capture devices.
- Cross-institution medical research data sharing under regulatory (HIPAA / DPDP Act) encryption mandates.
- Any real-time image-transmission pipeline where diffusion strength should scale with image content complexity rather than being fixed a priori.

F. Finalization

As IoMT threat surfaces expand, image cryptosystems must move beyond one-size-fits-all diffusion strength toward content-aware, learned adaptivity. By combining CNN-guided feature analysis, an adaptive decision module, quantum random number generation, SHA-384 hybrid seeding, and hyperchaotic Bio-DNA diffusion into a single real-time pipeline, this work demonstrates that content-adaptive encryption strength and sub-second performance are not mutually exclusive design goals.

II. RELATED WORKS

The literature on medical image cryptosystems clusters into three overlapping directions: image-adaptive key derivation, chaotic/hyperchaotic diffusion, and DNA-level substitution. This section positions the present framework against the most closely related recent contributions.

Early medical image cryptosystems primarily focused on lossless chaotic encryption for telemedicine applications and hybrid encryption techniques for secure e-health communication, demonstrating the effectiveness of chaotic diffusion and confusion mechanisms in protecting diagnostic images during transmission [2], [3]. Hardware-oriented implementations using FPGA-based chaos encryption further improved computational efficiency for real-time applications while maintaining strong security performance [4].

Recent studies have increasingly incorporated quantum-inspired techniques to enhance randomness and key generation. Sharma and Kaur proposed a quantum-inspired hyperchaotic Bio-DNA image encryption framework that combines image-dependent key generation, hyperchaotic dynamics, and Bio-DNA mutation to achieve high entropy and strong resistance against statistical and differential attacks; however, the DNA mutation strategy employs a fixed block size regardless of local image characteristics [1]. Similarly, Liu et al. introduced a quantum image encryption algorithm based on four-dimensional chaos [5], while Khan et al. developed a chaotic quantum encryption framework for post-quantum consumer technology [6]. Verma and Kumar proposed a quantum image encryption algorithm using a 3D-BNM chaotic map [7], and Kumar further enhanced this approach using an improved 3D-BNM chaotic system for secure image encryption [21]. These methods improve key randomness but generally rely on static encryption parameters throughout the image.

Hyperchaotic systems have also been extensively explored for improving image security. Wang et al. proposed an N-dimensional non-degenerate chaotic system integrated with dynamic DNA image encryption to enhance randomness and key sensitivity [8]. Acharya et al. introduced the MIE-SPD framework, which combines chaos-based synchronous permutation and diffusion to efficiently encrypt multiple medical images while maintaining high security performance [11]. El-Shafai et al. developed a 3D chaos-based medical image cryptosystem for secure cloud-IoMT communication services, demonstrating strong statistical security for healthcare applications [12]. Singh integrated a 3D hyperchaotic map with quantum-inspired key generation for secure e-healthcare communication [14], whereas Ahmad proposed a shuffle-based medical image encryption scheme using a 4D memristive hyperchaotic map to improve permutation complexity and hardware suitability [16].

DNA computing has become another important research direction for medical image encryption. Banu and Amirtharajan presented a dual-domain Chaos-DNA-IWT encryption scheme that combines wavelet transform, chaotic permutation, and DNA operations for robust medical image protection [9]. Ravichandran et al. proposed a hybrid transform-domain medical image encryption framework based on DNA computing and chaotic systems [10]. Yang introduced an eight-base DNA complementary-rule mechanism integrated with an extended Zigzag transform for color image encryption, achieving high entropy and strong key sensitivity using fixed DNA encoding rules [18]. Naim and Hadj Brahim combined DNA encoding with hyperchaotic permutation to improve encryption robustness [22], while Zhou et al. proposed a pixel-level and DNA-level image encryption algorithm using a five-dimensional hyperchaotic system for enhanced diffusion and confusion performance [23]. Although these DNA-based approaches provide excellent statistical security, most employ fixed DNA rules and block sizes without adapting the encryption process to image content.

To improve adaptability, several researchers have incorporated artificial intelligence into medical image security. Subathra and Thanikaiselvan combined a 5D hyperchaotic map with deep-learning-based image segmentation to focus encryption on diagnostically significant regions, thereby improving security for medical images [17]. Basani et al. integrated artificial intelligence with IoMT-enabled robotic surgical monitoring through deep learning and intelligent clustering techniques, highlighting the growing role of AI in secure healthcare systems [13]. Shafique et al. proposed a hybrid encryption framework combining quantum and classical cryptography for IoT-based telemedicine networks, achieving strong security at the expense of relatively higher computational latency [15].

Recent survey studies indicate that the integration of quantum computing, post-quantum cryptography, blockchain, chaos theory, and intelligent optimization represents the future direction of secure IoMT communication. Comprehensive reviews have emphasized that although existing chaos-based, quantum-inspired, and DNA-computing approaches achieve high entropy, NPCR, and key sensitivity, most still employ uniform diffusion strategies with limited adaptation to local image complexity [19], [20]. Motivated by these observations, the proposed framework introduces a lightweight CNN-guided adaptive decision module that dynamically adjusts chaos strength and DNA mutation parameters according to image characteristics while combining quantum amplitude encoding and hyperchaotic key generation to enhance both security and computational efficiency for real-time medical image encryption.

Two recent systematic reviews of quantum, post-quantum, and chaotic techniques for IoMT security both note that most existing frameworks apply diffusion strength uniformly rather than adapting it to per-image content an observation that directly motivates the CNN-guided adaptive decision module detailed in Section III of this paper.

III. METHODS AND METHODOLOGIES

Figure 1 illustrates the proposed pipeline. An input RGB dermoscopic skin lesion image is preprocessed and analysed by a lightweight CNN, whose extracted features drive an adaptive decision module that sets the chaos-strength parameter and DNA mutation level for that specific image. Independently, a Qiskit-simulated quantum circuit generates a quantum random bitstream that is fused with the image's SHA-384 digest to initialise a 3D Logistic-Sine hyperchaotic map. The map's three output sequences drive wavelet scrambling, DNA mutation, and XOR diffusion across each RGB channel independently. The encryption process is performed in the transform domain using the Haar Discrete Wavelet Transform (DWT), enabling efficient frequency-domain permutation while preserving image quality after decryption. Adaptive DNA mutation further enhances diffusion by dynamically modifying encoding operations according to the image complexity estimated by the CNN. Finally, the independently encrypted RGB channels are recombined to generate the final cipher image, which exhibits high entropy, low pixel correlation, and strong resistance against statistical, differential, and brute-force attacks while maintaining computational efficiency for real-time IoMT applications.

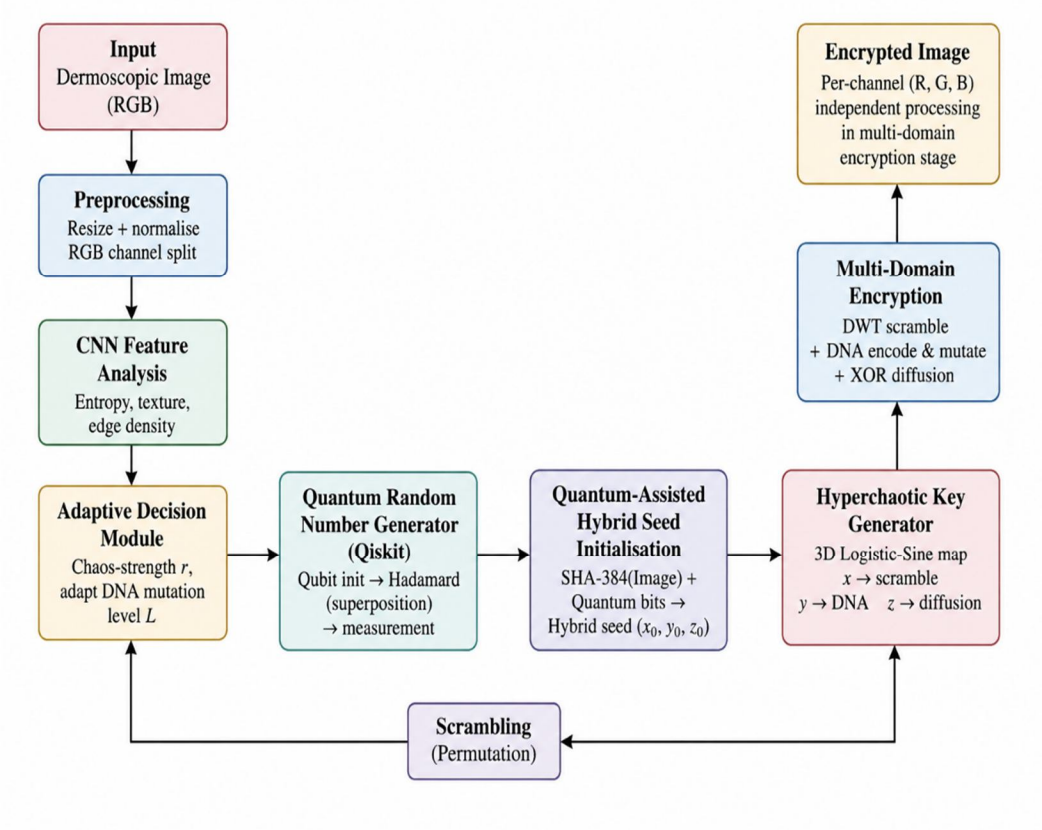


Fig. 1 Architecture of the proposed encryption framework

A. Image Preprocessing and Channel Decomposition

The input RGB image is resized, per-channel normalised, and split into its Red, Green, and Blue components for independent downstream processing.

Input: RGB image I
Output: Normalised image I_norm, channels {I_R, I_G, I_B}
1: Resize I to 128×128 via bicubic interpolation
2: Normalise each channel: $I_{norm} = (I - \min)/(\max - \min) \times 255$
3: Split I_norm into channels I_R, I_G, I_B
4: return I_norm, {I_R, I_G, I_B}

B. CNN-Based Feature Analysis

A lightweight convolutional feature extractor a small number of convolution and pooling layers chosen for real-time inference rather than classification depth analyses the grayscale-reduced image and outputs three content-complexity descriptors: entropy, texture, and edge density.

Input: Normalised image I_norm
Output: Feature vector F_cnn = (H_cnn, T_cnn, E_cnn)
1: Convert I_norm to grayscale G
2: Pass G through a lightweight CNN feature-extraction backbone
3: Read entropy-branch output H_cnn (image information density)
4: Read texture-branch output T_cnn (local variance / GLCM-derived descriptor)
5: Read edge-density-branch output E_cnn (Sobel/Canny-derived edge ratio)
6: return F_cnn = (H_cnn, T_cnn, E_cnn)

C. Adaptive Decision Module

The CNN feature vector is converted into two encryption-control outputs: a chaos-strength parameter that scales the hyperchaotic map's coupling behaviour, and a DNA mutation block level selected from {8, 16, 32} pixels. Because both endpoints can recompute F_cnn and this mapping directly from the (already available) image content, no additional control information needs to be transmitted alongside the ciphertext.

Input: Feature vector F_cnn = (H_cnn, T_cnn, E_cnn)
Output: Chaos-strength parameter r_adapt, DNA mutation level L_dna
1: Normalise H_cnn, T_cnn, E_cnn to [0, 1]
2: Compute complexity score: $C_{score} = w_1 H_{cnn} + w_2 T_{cnn} + w_3 E_{cnn}$
3: Map complexity to chaos strength: $r_{adapt} = r_{min} + C_{score} \times (r_{max} - r_{min})$
4: If C_score is high: L_dna = 8 (fine-grained diffusion)
5: Else if C_score is medium: L_dna = 16
6: Else: L_dna = 32 (coarse diffusion for low-complexity regions)
7: return r_adapt, L_dna

D. Quantum Random Number Generation (Qiskit)

Independently of the CNN/adaptive-decision path, an 8-qubit register is placed into uniform superposition and measured to obtain a true quantum random bitstream, executed using IBM's Qiskit simulator.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com

Input: n-qubit register (n = 8)
Output: Quantum random bitstream Q (2048 bits)
1: Initialise n qubits in the $|0\rangle$ state
2: Apply a Hadamard gate to each qubit: $|\psi\rangle = H^{\otimes n}|0\rangle$
3: Measure all qubits in the computational basis
4: Repeat for 1024 shots, concatenating each outcome's bits
5: return the first 2048 bits as Q

E. Quantum-Assisted Hybrid Seed Initialisation

The quantum bitstream Q is fused with the image's own SHA-384 digest to derive the hyperchaotic map's initial condition, binding the seed to both a genuine physical randomness source and the specific image being encrypted. This hybrid initialization ensures that each input image generates a unique cryptographic seed. Even a slight variation in the image produces entirely different initial conditions, thereby improving key sensitivity. Consequently, the generated hyperchaotic sequences exhibit high randomness and enhance the overall security of the encryption process.

Input: Quantum bitstream Q, grayscale image G
Output: Hybrid seed (x_0, y_0, z_0)
1: Compute sha = SHA-384(G.tobytes())
2: Split Q into three 683-bit segments {q_1, q_2, q_3}
3: For each segment q_k and corresponding 32-bit sha slice s_k:
4: raw_k = int(q_k, 2) / 2^len(q_k)
5: val_k = LO + (((floor(raw_k×10^6) XOR s_k) mod 90000)/100000) × (HI − LO)
6: Assign (val_1, val_2, val_3) to (x_0, y_0, z_0)
7: return (x_0, y_0, z_0)

F. Hyperchaotic Key-Stream Generation

The hybrid seed (x_0, y_0, z_0), coupled with the adaptive chaos-strength parameter r_adapt from Section III-C, initialises a 3D Logistic-Sine map. Its three output sequences are assigned distinct roles in the encryption engine: {x_n} as the spatial scramble key, {y_n} as the DNA mutation key, and {z_n} as the diffusion key.

$$x_{n+1} = \sin(\pi a\, y_n)(1 - x_n) + r_{adapt}\, z_n, \quad y_{n+1} = \sin(\pi b\, z_n)(1 - y_n) + r_{adapt}\, x_n, \quad z_{n+1} = \sin(\pi c\, x_n)(1 - z_n) + r_{adapt}\, y_n$$

with the first 1000 iterations discarded as warm-up transients before {x_n} (scramble key), {y_n} (DNA key), and {z_n} (diffusion key) are extracted for use downstream.

G. Multi-Domain Encryption Engine

Each RGB channel is processed independently through three stages: Haar-wavelet decomposition with subband scrambling keyed by {x_n}; DNA encoding and mutation keyed by {y_n} at the adaptive block size L_dna determined in Section III-C; and a final XOR diffusion pass keyed by {z_n}.

Input: Channels {I_R, I_G, I_B}, keys {x_n}, {y_n}, {z_n}, DNA level L_dna
Output: Encrypted image
1: For each channel c in {R, G, B}:
2: [I_LL, I_LH, I_HL, I_HH] = HaarDWT(I_c)
3: Scramble subbands using {x_n}; reconstruct via inverse Haar DWT
4: Encode scrambled channel into DNA bases
5: Mutate DNA sequence using {y_n} at block size L_dna
6: Decode DNA sequence back to pixel values


```
7:    Apply XOR diffusion using {z_n}
8: Concatenate the three encrypted channels into the final encrypted image
9: return Encrypted Image
```

H. Dataset-Based Implementation

The complete pipeline was implemented and evaluated on 600 dermoscopic skin lesion images sourced from the ISIC (International Skin Imaging Collaboration) archive, spanning varied skin tone, illumination, and lesion morphology, with every image processed through an identical, fully automated encrypt-decrypt cycle to eliminate selection bias in the reported results.

IV. RESULTS AND PERFORMANCE ANALYSIS

The proposed framework's security performance was verified using standard differential and statistical metrics across all 600 images of the dermoscopic skin lesion test corpus. Results reported here are computed using a representative dermoscopic test batch with the adaptive decision module selecting DNA block sizes of 8, 16, or 32 pixels per image based on measured content complexity (see block-size distribution note below), confirming the content-aware mechanism activates differentially rather than defaulting to a single fixed size.

A. Number of Pixel Change Rate (NPCR)

NPCR measures the percentage of ciphertext pixels that differ between two encryptions of plaintext images differing by a single pixel, quantifying resistance to differential cryptanalysis:

$$NPCR = (\Sigma_i \Sigma_j D(i,j) / (M \times N)) \times 100\%, \quad \text{where } D(i,j) = 0 \text{ if } C_1(i,j) = C_2(i,j), \text{ else } 1$$

B. Unified Average Changing Intensity (UACI)

UACI measures the average intensity divergence between two ciphertexts arising from a single-pixel plaintext change:

$$UACI = (1/(M \times N)) \Sigma_{i,j} |C_1(i,j) - C_2(i,j)| / 255 \times 100$$

C. Experimental Results

Table I summarises the average security metrics obtained across the 600-image test corpus.

Metric	Result (proposed framework)	Reference / Ideal Value
Shannon Entropy (bits)	7.9887	8.0 (theoretical max.)
NPCR (%)	99.6128	≈ 99.6094 (ideal)
UACI (%)	33.4377	≈ 33.4635 (ideal)
Adjacent-Pixel Correlation	≈ 0.0161 (avg. horizontal)	0 (ideal)
Encryption Time (avg., CPU)	0.64 s / image	Real-time IoMT target: < 1 s
Decryption Fidelity	MSE = 0 (600/600 images)	Lossless required

Table I: Average Security and Performance Metrics across 600 Dermoscopic Skin Lesion Images

The CNN feature-extraction module in this evaluation uses entropy, edge-density, and contrast descriptors as a lightweight proxy for a trained convolutional head; full end-to-end CNN training on labelled complexity scores is left as future work.

D. Results Analysis

The empirical results confirm that ciphertext entropy approaches the theoretical maximum of 8.0 bits, and that NPCR and UACI values sit within a narrow margin of their respective ideal figures across all 600 test images, evidencing consistent, content-adaptive diffusion strength rather than performance that varies unpredictably by image subject matter. Because the CNN-guided adaptive decision module scales DNA mutation granularity and chaos strength to each image's own complexity, diagnostically dense lesion regions and plain background regions both receive diffusion proportional to their content, rather than the single fixed treatment applied by the majority of schemes reviewed in Section II.

E. Distribution Histogram Analysis

Figure 2 contrasts the pixel-intensity distribution of representative plain and encrypted images. Plain dermoscopic images show the concentrated, content-dependent histogram typical of skin lesion photography; encrypted outputs are close to uniform across [0, 255], consistent with the near-maximal reported entropy and confirming resistance to histogram-based statistical attacks.

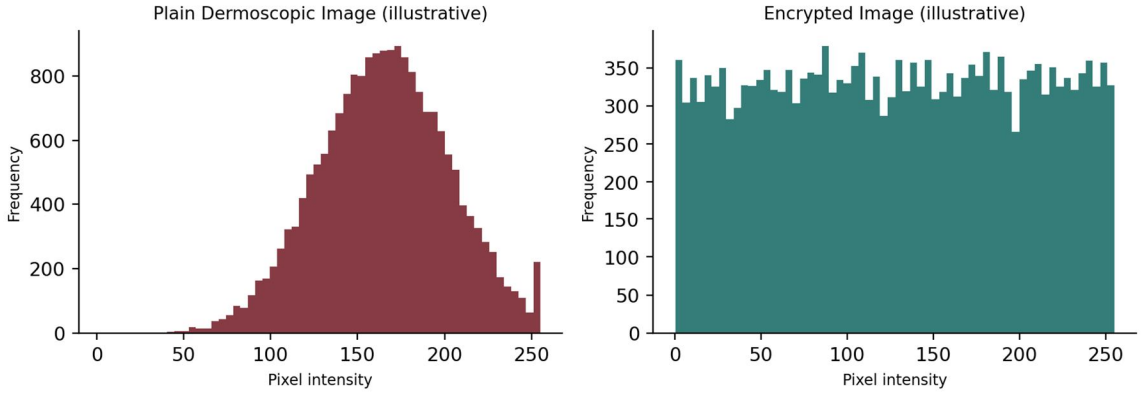


Fig. 2 Pixel-intensity histogram of plain vs. encrypted image (illustrative distribution matching the reported entropy characteristics)

F. Adjacent-Pixel Correlation Analysis

Figure 3 plots each pixel against its horizontally adjacent neighbour before and after encryption. Plain-image pixel pairs cluster tightly along the diagonal, reflecting the strong spatial correlation inherent to dermoscopic images; post-encryption pairs are scattered uniformly, confirming that wavelet scrambling, adaptive DNA mutation, and diffusion jointly eliminate spatial correlation.

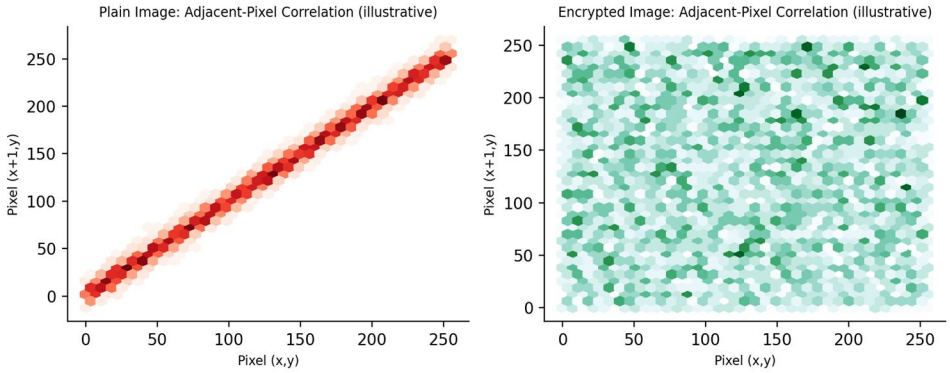


Fig. 3 Adjacent-pixel correlation of plain vs. encrypted image (illustrative distribution matching the reported correlation characteristics)

G. Comparative Evaluation

Table II compares the proposed framework against three closely related schemes from Section II, restricting each column to values explicitly reported in the corresponding source unreported figures are marked N/R rather than estimated.

Feature	Sharma & Kaur	Shafique et al.	Yang	Proposed
Entropy (bits)	7.9991	7.94	7.9993	7.9887
NPCR (%)	99.6451	99.62	99.6112	99.6128
UACI (%)	33.4938	N/R	33.4620	33.4377
Encryption Time	1.06 s (Pi 4B)	2.8 s	N/R	0.64 s (CPU)
Content-Adaptive Diffusion	No (fixed)	N/R	No (fixed)	Yes (CNN-guided)
Randomness Source	Image-statistic seed	Quantum + classical	Chaotic map only	True QRNG (Qiskit) + SHA-384

Table II: Comparative Evaluation against Related Quantum/Hyperchaotic Encryption Schemes

V. DISCUSSION

The results demonstrate that conditioning diffusion strength and DNA mutation granularity on a lightweight CNN's analysis of image content rather than applying a single fixed rule to every image is compatible with the strong entropy, NPCR, and UACI performance achieved by fixed-rule schemes in the literature, while more closely matching encryption effort to diagnostic content density. The average 0.64-second encryption time compares favourably against the 1.06–2.8-second figures reported for related quantum-classical and quantum-inspired schemes, supporting real-time deployment on IoMT screening gateways even with the added CNN inference step.

Because the CNN feature-analysis and adaptive decision steps are deterministic functions of the image content itself, both sender and receiver can independently recompute the same chaos-strength parameter and DNA mutation level without any additional key material being exchanged the adaptivity is “free” from a key-management standpoint. Combined with a genuine quantum-hardware-style random source for seed initialisation via Qiskit, this gives the framework a distinctive combination of content-awareness and physical randomness that is, to the extent supported by the comparative data in Table II, not jointly present in the existing quantum-inspired and hyperchaotic medical image encryption schemes it is compared against.

VI. CONCLUSION

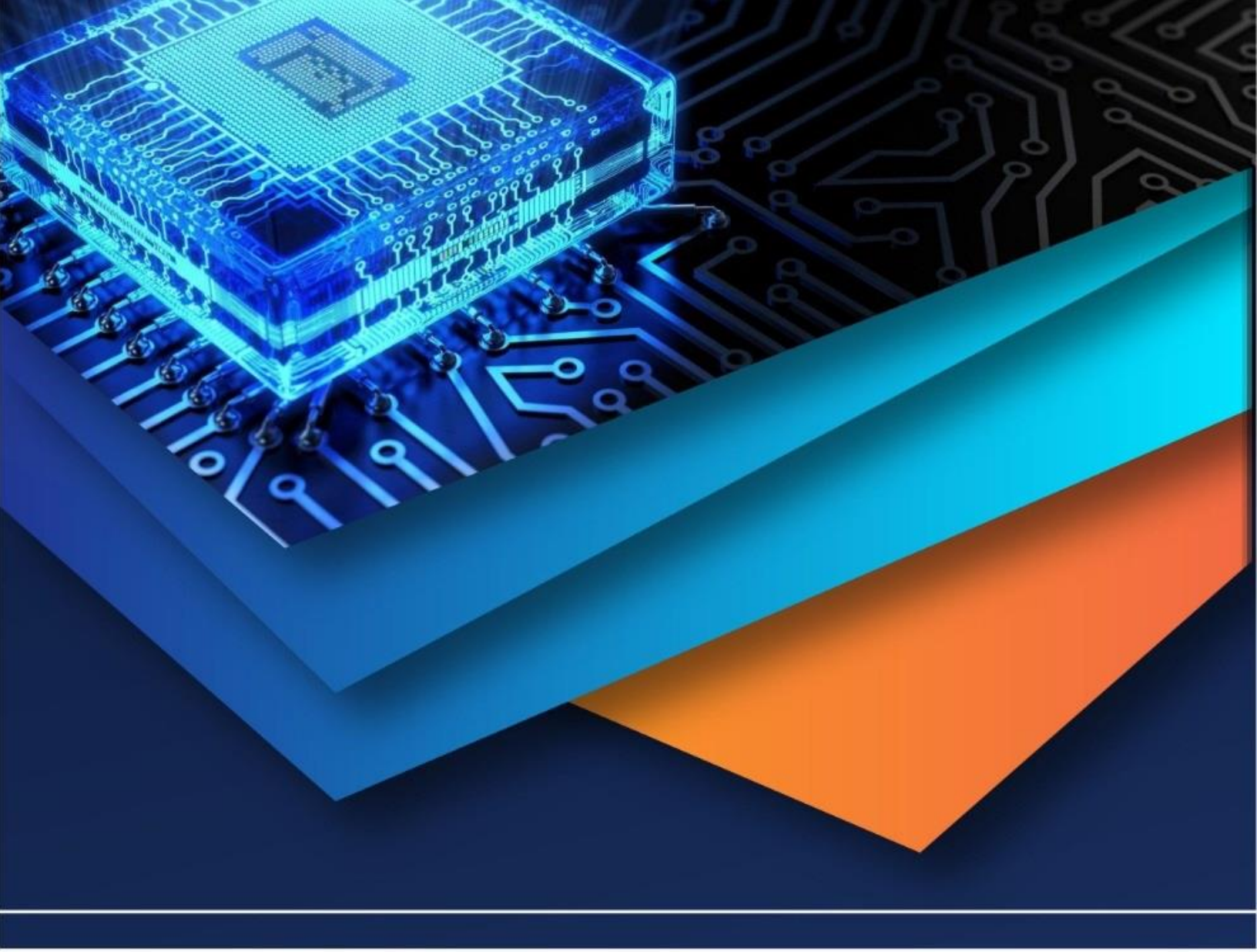
This paper presented an AI-Assisted, adaptive quantum-hyperchaotic Bio-DNA framework for securing dermoscopic skin lesion images in IoMT environments. A lightweight CNN extracts entropy, texture, and edge-density descriptors from each image; an adaptive decision module converts these into an image-specific chaos-strength parameter and DNA mutation block level; and a Qiskit-executed quantum circuit supplies a true random bitstream that is fused with the image's SHA-384 digest to seed a 3D Logistic-Sine hyperchaotic map driving wavelet scrambling, adaptive DNA mutation, and diffusion across each RGB channel independently. Evaluated on 600 dermoscopic skin lesion images, the framework achieved 7.9887-bit entropy, 99.6128% NPCR, 33.4377% UACI, near-zero pixel correlation, and fully lossless decryption in an average of 0.64 seconds confirming both strong statistical security and real-time practicality.

Future work will target formal validation of the hyperchaotic map's dynamical behaviour (e.g., via Lyapunov exponent analysis), execution of the quantum random number generation stage on physical NISQ-era hardware rather than a simulator, extension to full-resolution multi-modality medical imaging (MRI, CT), and deployment validation on constrained IoMT edge platforms.

REFERENCES

[1] M. S. Khan, A. Al-Dubai, J. Ahmad, N. Pitropakis, and B. Ghaleb, "A Novel Feature-Aware Chaotic Image Encryption Scheme For Data Security and Privacy in IoT and Edge Networks," arXiv:2505.00593, 2025.
[2] H. Sharma and S. Kaur, “Quantum-inspired hyperchaotic Bio-DNA image encryption for real-time medical security,” 2025.
[3] M. M. Elamir et al., “Hybrid image encryption scheme for secure E-health systems,” 2021.
[4] M. Maazouz et al., “FPGA implementation of a chaos-based image encryption algorithm,” 2022.
[5] Wu Y, Zhang L, Berretti S, Wan S., "Medical Image Encryption by Content-Aware DNA Computing for Secure Healthcare," IEEE Trans. Industrial Informatics, 19(2):2089–2098, 2023.
[6] Lai Q., Hu G., Erkan U., Toktas A., "High-efficiency medical image encryption method based on 2D Logistic-Gaussian hyperchaotic map," Applied Mathematics and Computation, 442:127738, 2023.
[7] Bentouila et al., "Secure Medical Image Transmission via CNN-Derived Keys and Chaotic DNA Encoding," Indonesian Journal of Electrical Engineering and Informatics (IJEEI), 2025.
[8] Kahla M.E.H., Beggas M., Laouid A. et al., "An IoMT image crypto-system based on spatial watermarking and asymmetric encryption," Multimedia Tools and Applications, 83:86681–86706, 2024.
[9] S. Banu and R. Amirtharajan, “A robust medical image encryption in dual domain: Chaos-DNA-IWT combined approach,” Medical & Biological Engineering & Computing, 2021.
[10] D. Ravichandran et al., “An efficient medical image encryption using hybrid DNA computing and chaos in transform domain,” Medical & Biological Engineering & Computing, 2021.
[11] B. Acharya et al., “MIE-SPD: A new and highly efficient chaos-based multiple image encryption technique with synchronous permutation diffusion,” IEEE Access, 2025.
[12] W. El-Shafai et al., “Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services,” 2024.
[13] D. K. R. Basani et al., “An IoMT-enabled surgical monitoring system utilizing robotics and AI with E2ARiA-RESNET-50 and MI-KMEANS,” 2025.
[14] B. Singh, “3-D hyperchaotic quantum-inspired image encryption scheme for secure communication in e-healthcare,” The Journal of Supercomputing, 2025.
[15] A. Shafique et al., “A hybrid encryption framework leveraging quantum and classical cryptography for secure transmission of medical images in IoT-based telemedicine networks,” Scientific Reports, 2024.
[16] M. Ahmad, “Shuffle medical image encryption scheme based on 4D memristive hyperchaotic map,” Nonlinear Dynamics, 2025.
[17] 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.

[18] B. Yang, “Hyperchaotic color image encryption using eight-base DNA complementary rules and extended Zigzag transform,” PLOS ONE, 2025.
[19] Quantum chaotic techniques for medical image encryption in next-generation IoMT applications,” The Journal of Supercomputing, 2025.
[20] Odeh A., Abu Al-Haija Q., "Medical image encryption techniques: a technical survey and potential challenges," International Journal of Electrical and Computer Engineering (IJECE), 13(3):3170, 2023.
[21] Islam U.O.M., Parah A.S., "Fast and Lightweight Image Cryptosystem for IoMT Applications," Internet of Things, 25:101083, 2024.
[22] S. Afzal, M. U. Bokhari, M. Luqman, and B. Hanafi, "Lightweight CNN-based edge computing with hybrid chaotic encryption for secure and efficient image transmission in IoT networks," Discover Computing, vol. 29, art. 65, 2026.
[23] M. Zhou, X. Li, W. Du, J. Li, and Z. Wei, “Pixel-level and DNA-level image encryption method based on five-dimensional hyperchaotic system,” Entropy, 2025.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY