SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 8853-8862
Open Access. Online & Print

DOI: 10.5281/zenodo.12426874

QUANTUMSHIELD-MIS: A HYBRID QUANTUM-CRYPTOGRAPHIC FRAMEWORK FOR PROTECTING MEDICAL IMAGING DATA IN CONNECTED HEALTHCARE ENVIRONMENTS

Kantharaju[1*], Srinidhi G A[2]

[1] Research Scholar, Department of Electronics and Communication Engineering, Sri Siddhartha Institute of Technology (SSIT), SSAHE, Tumakuru – 572105, Karnataka, India
Corresponding Author [1]E-mail: kantharaju@ssit.edu.in
[2] Research Supervisor, Department of Computer Science and Engineering(Cyber Security), Sri Siddhartha Institute of Technology (SSIT), SSAHE, Tumakuru – 572105, Karnataka, India
[2]E-mail: srinidhiga@ssit.edu.in

Received: 13/12/2025
Accepted: 27/01/2026

Corresponding Author: Kantharaju (kantharaju@ssit.edu.in)

ABSTRACT

The widespread adoption of cloud infrastructure and networked diagnostic devices has created serious gaps in how sensitive imaging data is protected throughout its lifecycle. Standard cryptographic tools — AES, RSA, and ECC — face an existential threat from quantum computing, particularly from Shor's factoring algorithm and Grover's search acceleration, both of which undermine the mathematical assumptions these schemes rely on. This paper introduces QuantumShield-MIS, implemented through the Q-HELKD algorithm (Quantum-enhanced Hybrid Encryption with Lattice-based Key Distribution for Medical Image Security), a four-layer architecture built around: a hardware-based Quantum Random Number Generator (QRNG) for session key entropy, a decoy-state BB84 Quantum Key Distribution (QKD) protocol for unconditionally secure key establishment, a CRYSTALS-Kyber-1024 post-quantum Key Encapsulation Mechanism (KEM) for transport-channel security, and a fractional-order three-dimensional Lorenz chaotic diffusion engine for pixel-level scrambling. Tests spanning 1,280 images across eight diagnostic modalities produced results that exceeded all six benchmark algorithms simultaneously: mean PSNR of 48.7 dB, information entropy of 7.9997 bits/pixel, NPCR of 99.9987%, UACI of 33.4652%, near-zero inter-pixel correlation (0.00003), and encryption throughput of 8.2 ms per 64 KB block. These findings demonstrate that robust quantum-safe protection need not come at the cost of clinical usability.

KEYWORDS: Quantum Cryptography; Medical Image Encryption; QKD; CRYSTALS-Kyber; Lattice-based Cryptography; BB84 Protocol; Fractional Lorenz System; Post-Quantum Security; Healthcare IoT; Q-HELKD.

Copyright: © 2026. This is an open-access article distributed under the terms of the Creative Commons Attribution License. (https://cre-ativecommons.org/licenses/by/4.0/).

I. INTRODUCTION

Hospitals and diagnostic centres today operate within dense information environments where imaging devices, cloud repositories, and clinical decision tools exchange data continuously. A mid-sized tertiary hospital may transmit tens of terabytes of imaging data annually — MRI volumes, CT stacks, digital X-rays, ultrasound clips, PET scans, and whole-slide pathology images — each packet carrying Protected Health Information (PHI) whose compromise carries consequences ranging from regulatory penalties to direct patient harm [1]. Frameworks like HIPAA, GDPR, and India's Digital Personal Data Protection Act 2023 recognise this gravity, yet the cryptographic underpinnings securing most of this data remain grounded in assumptions that quantum computing is now beginning to erode [2].

The threat is not hypothetical. Peter Shor demonstrated in 1994 that RSA and Diffie–Hellman key exchange collapse to polynomial-time solutions on a quantum processor large enough to run his factoring circuit [3]. Elliptic curve discrete logarithm problems fare no better — Proos and Zalka extended Shor's work to ECC, eliminating its security advantage [4]. For symmetric schemes, Grover's algorithm halves the effective key length through amplitude amplification, reducing AES-128 to the rough equivalent of 64-bit classical security [5]. While a fault-tolerant quantum computer capable of attacking production-scale keys has not yet been built as of 2026, the harvest-now- decrypt-later (HNDL) strategy — storing encrypted traffic today for decryption once capable hardware exists — renders this timeline irrelevant for long-retention data [6]. Medical imaging records are paradigmatically long- retention; a patient's imaging archive may remain clinically relevant for decades.

Existing responses to this challenge each address part of the problem. Pure Quantum Key Distribution systems offer information-theoretic security rooted in the no-cloning theorem, but practical constraints — channel distance limits, hardware costs, and susceptibility to photon-number-splitting (PNS) attacks — restrict their standalone utility [7]. Post-quantum algorithms such as CRYSTALS-Kyber give computational security against quantum adversaries but do not offer the unconditional guarantees of QKD [8]. Chaos-based encryption provides excellent diffusion but depends on deterministic dynamics that can theoretically be reconstructed with sufficient observations [9]. The gap this paper targets is the absence of a unified architecture combining all four protective layers within a single, clinically validated framework.

QuantumShield-MIS fills that gap. The Q-HELKD algorithm integrates a hardware QRNG, decoy-state BB84 QKD, CRYSTALS-Kyber-1024 KEM, and a fractional-order Lorenz chaotic diffusion engine into a layered defence system designed to be deployable as a transparent DICOM transport encryption layer. The four primary contributions are: (1) an enhanced BB84 protocol with decoy-state photon sources providing measurable eavesdropping detection; (2) a fractional-order Lorenz system with a maximum Lyapunov exponent 41.7% above the classical formulation, increasing resistance to phase-space reconstruction; (3) a Kyber-1024 KEM integration securing key transport beyond quantum channel range; and (4) comprehensive benchmarking across eight imaging modalities and twelve security metrics against five competing algorithms. Section II surveys prior art from 2020 to 2026. Sections III and IV detail the architecture and its security proofs. Sections V and VI describe experimental methodology and results. Section VII addresses clinical deployment, and Section VIII concludes.

II. RELATED WORK

A. Classical Approaches and Their Quantum Vulnerabilities

Mohamed et al. [10] demonstrated a 23% throughput improvement over standard AES-256 for DICOM payloads by exploiting hardware AES-NI instructions on FPGA substrates — a meaningful practical gain, though the authors themselves acknowledged that Grover's attack reduces AES-256 to an effective 128-bit quantum security level, insufficient for data requiring multi-decade retention. Zhang and Xu [11] showed that RSA-2048 encryption of 512x512 CT slice sets introduces latency exceeding 350 ms in real-time PACS workflows, making it operationally problematic even before its quantum vulnerability is considered. Banerjee et al. [12] explored ECC-521 for resource-constrained medical IoT devices, finding favourable energy profiles but confirming that Shor's algorithm, as extended by Proos and Zalka, renders elliptic-curve schemes quantum-insecure regardless of curve selection.

B. Chaos-Based Image Encryption

Chaotic dynamical systems became popular for image encryption in the early 2020s because their sensitivity to initial conditions naturally mirrors the diffusion-confusion requirements of good ciphers. Liu et al. [13] reported NPCR of 99.73% and entropy of 7.9946 using a 2D logistic-tent composite map for MRI encryption — results close to theoretical bounds

— but used fixed-precision floating-point arithmetic that left the system vulnerable to phase- space reconstruction, a weakness subsequently formalised by Arroyo et al. [14]. Kumar and Singh [15] responded by adopting a hyperchaotic four-dimensional Lorenz-Stenflo system with parameter perturbation, pushing inter- pixel correlation down to 0.00082 and strengthening chosen-plaintext resistance. A persistent limitation across all chaos-based work is that pseudo-random sequences, however irregular they appear, are deterministic; absent a genuine quantum entropy source, they remain theoretically distinguishable from true randomness [16].

C. Quantum Key Distribution in Clinical Settings

QKD rests on the no-cloning theorem and Heisenberg's uncertainty principle, granting security that is independent of computational hardness assumptions [17]. Liao et al. [18] demonstrated satellite-mediated QKD over 1,200 km, establishing feasibility for long-range telemedicine. Chen et al. [19] integrated a metropolitan QKD network with hospital PACS and achieved 47.8 kbps key generation over 30 km of dark fibre — sufficient for standard CT acquisition rates. Wang et al. [20] catalogued vulnerabilities in practical weak-coherent-pulse QKD implementations, particularly PNS attacks; Lo's decoy-state methodology [21], experimentally validated by Yin et al. [22], substantially mitigates these by randomising photon intensities across signal, decoy, and vacuum states. Commercial QKD systems are currently limited to roughly 100 km on optical fibre, constraining their reach in large hospital networks [23].

D. Post-Quantum Standards

NIST concluded its Post-Quantum Cryptography standardisation project in 2022, selecting CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+ [24]. Among these, Kyber-1024 achieves NIST security level 5, equivalent to AES-256 against classical adversaries and approximately 182 quantum security bits under the best known lattice attacks [25]. Bernstein and Lange [26] confirmed that Kyber offers the most favourable combination of security, key size, and computational cost for constrained healthcare IoT devices. Ravi et al. [27] demonstrated Kyber-1024 key encapsulation in under 1.2 ms on an ARM Cortex-M4 at 168 MHz — performance comfortably within clinical real-time requirements.

E. Hybrid Architectures and Identified Gaps

Recent hybrid work has explored pairing QKD with bulk classical encryption: Ott et al. [28] combined QKD session keys with AES-256-GCM, reporting a 12% reduction in security overhead compared to dual-layer classical encryption. Sharma and Mishra [29] integrated BB84 QKD with a teleradiology platform, but chose 3DES as the bulk cipher — a selection criticised for its 56-bit effective key length [30]. Park et al. [31] presented a Kyber-768 plus chaos-map hybrid for medical images (PSNR 44.3 dB, entropy 7.9982) but omitted QKD, leaving key establishment without information-theoretic security. No published framework simultaneously incorporates QRNG, QKD, a NIST-standardised PQC KEM, and quantum-chaotic diffusion with multi-modality clinical validation. Table 1 below illustrates this gap.

Table 1 — Feature Comparison of Prior Art Against the Proposed Q-HELKD Framework

Reference	Year	QRNG	QKD	PQC-KEM	Chaos Diffusion	Quantum- Safe
Mohamed et al.	2021	✗	✗	✗	✗	No
Liu et al.	2022	✗	✗	✗	✓	No
Chen et al.	2021	✗	✓	✗	✗	Partial
Park et al.	2023	✗	✗	Partial	✓	Partial
Sharma & Mishra	2022	✗	✓	✗	✗	Partial
Kumar & Singh	2023	✗	✗	✗	✓	No
Q-HELKD (Ours)	2025	✓	✓	✓	✓	**Yes**

III. THE Q-HELKD ARCHITECTURE

QuantumShield-MIS is built around four sequential layers, each contributing a distinct and orthogonal security property. Together they span the complete image journey from acquisition device to authorised clinical endpoint. The architecture is designed to

degrade gracefully: if the quantum channel is unavailable, the Kyber-1024 layer alone sustains NIST Level 5 post-quantum computational security.

A. Layer 1 — Quantum Random Number Generator

The entire framework is seeded by a hardware QRNG based on vacuum-state fluctuations measured via homodyne detection. Quantum shot noise — the irreducible randomness arising from Heisenberg uncertainty applied to conjugate electromagnetic field quadratures — provides the entropy source. Output passes NIST SP 800-90B health tests including frequency, runs, and autocorrelation checks, certifying that each 256-bit seed is computationally indistinguishable from ideal uniform randomness. This quantum seed initialises both the QKD photon polarisation encoding in Layer 2 and the chaotic attractor initial conditions in Layer 4, ensuring that no component of the system relies on deterministic or pseudo-random seeding.

B. Layer 2 — BB84 QKD with Decoy-State Enhancement

Layer 2 implements a BB84-derived QKD protocol over a fibre-optic quantum channel. Alice encodes bit values onto single-photon polarisation states drawn from two mutually unbiased bases — rectilinear {|0⟩ , |1⟩ } and diagonal {|+⟩ , |−⟩ }. Bob measures each arriving photon in a randomly selected basis. Following quantum transmission, basis reconciliation over an authenticated classical channel discards mismatched measurements; the retained sifted key undergoes Cascade error correction and privacy amplification to produce shared secret K_QKD
∈ {0,1}^256, with security parameter ε_sec < 2^{-100} satisfying universally composable security bounds.

The critical practical enhancement is the decoy-state methodology. Practical QKD implementations use weak coherent pulses (WCP) rather than ideal single-photon sources, creating exposure to photon-number-splitting (PNS) attacks. Q-HELKD transmits pulses at three randomised mean photon numbers — signal (μ_s ≈ 0.6), decoy (μ_d ≈ 0.2), and vacuum (μ_v ≈ 0) — and uses statistical analysis of detection rates across all three intensity levels to tightly bound any eavesdropper's information gain, restoring practical WCP security to levels approaching ideal single-photon QKD.

C. Layer 3 — CRYSTALS-Kyber-1024 Post-Quantum KEM

For communications beyond quantum channel range, Layer 3 uses CRYSTALS-Kyber-1024 to transport key material securely. Kyber is built on the Module Learning With Errors (M-LWE) hardness assumption over the polynomial ring R_q = Z_q[x]/(x^n + 1) with n = 256, q = 3329, and k = 4 modules. The scheme achieves IND- CCA2 security via a Fujisaki-Okamoto transformation applied to a base IND-CPA encryption scheme. The composite master key is derived as K_enc = HKDF-Expand(PRK, "Q-HELKD-v1" ‖ session_id, 512), where PRK
= HKDF-Extract(salt, K_QKD ‖ K_Kyber). This dual-path construction ensures that compromising either the QKD channel or the KEM alone is insufficient to recover K_enc.

D. Layer 4 — Fractional-Order 3D Lorenz Chaotic Diffusion

The actual pixel transformation is performed by a fractional-order extension of the Lorenz chaotic system, driven by the composite key K_enc. Extending the classical Lorenz system using the Caputo fractional derivative operator D^α with α = 0.975 raises the maximum Lyapunov exponent from 0.9056 (integer-order) to 1.2841, a 41.7% increase that translates directly to faster divergence of neighbouring trajectories and significantly reduced success probability for phase-space reconstruction attacks. The encryption pipeline has three stages: (1) three-dimensional Arnold cat map scrambling of pixel positions using key-derived integer parameters; (2) fractional Lorenz keystream generation; and (3) XOR-based diffusion with additive carry propagation implementing avalanche across the entire image. Encryption complexity is O(M) where M is the image pixel count, supporting real-time clinical throughput.

IV. MATHEMATICAL FOUNDATIONS AND SECURITY ANALYSIS

A. QKD Secret Key Rate

Under the decoy-state BB84 protocol, the secret key rate R is bounded below by:

$$R \geq Q_1 \quad [1 - h_2 (e_1^{bit})] - Q\mu \cdot f\_EC \cdot h_2 (E\mu)$$

where Q_1 is the single-photon detection rate, e_1^{bit} is the single-photon bit error rate, h_2 is the binary Shannon entropy function, and f_EC ≥ 1 is the error-correction efficiency. Secure key generation requires the measured QBER to satisfy Eμ < 11% (one-way classical processing threshold). In the Q-HELKD testbed at 40 km, QBER measured 2.8% — well within this bound — yielding a sifted key rate of 18.6 kbps.

B. Kyber-1024 Hardness Foundation

Key generation derives a public key pk = (A, t) where t = As + e, with A a uniformly random matrix in R_q^{4×4} and s, e sampled from centred binomial

distribution B_{η_1} with $\eta_1 = 2$. Encapsulation produces ciphertext c = (u, v) where u = A^T r + e_1 and v = t^T r + e_2 + ⌊ q/2⌋ ·m. Decapsulation recovers the shared secret seed from v − s^T u. The IND-CCA2 security of Kyber follows from M-LWE hardness at parameter k = 4 (Kyber-1024), achieving NIST Security Level 5 equivalent to breaking AES-256.

C. Fractional Lorenz System

The Caputo fractional-order Lorenz system is governed by $D^{\alpha} x = \sigma(y - x)$, $D^{\alpha} y = x(\rho - z) - y$, $D^{\alpha} z = xy - \beta z$, with classical parameters $\sigma = 10$, $\rho = 28$, $\beta = 8/3$ and fractional order $\alpha = 0.975$. For an initial perturbation $\delta x_0 = 10^{-15}$, the trajectory divergence grows as $\delta x(t) \approx \delta x_0 \cdot e^{\lambda_{max} \cdot t}$, where $\lambda_{max} = 1.2841$ in the fractional formulation versus 0.9056 for integer order — directly quantifying the improvement in sensitivity.

D. CPA Security Theorem

Theorem: Assuming M-LWE$_{k,q,\eta_1,\eta_2}$ hardness and that the fractional Lorenz system generates a computationally pseudorandom sequence, Q-HELKD is IND-CPA secure under the random oracle model. Proof sketch: By Kyber-1024 security, K_{enc} is computationally indistinguishable from a uniformly random key for any polynomial-time adversary. Given a uniformly random K_{enc}, the chaotic keystream K_S is pseudorandom (modelling the Lorenz generator as a PRF), rendering the ciphertext C = (I' ⊕K_S + chain) equivalent to a one-time-pad encryption, achieving IND-CPA security. The QKD layer adds information-theoretic key establishment security against computationally unbounded adversaries. □

V. EXPERIMENTAL CONFIGURATION

A. Hardware Testbed

All experiments were conducted on a dedicated testbed. The QRNG module was an ID Quantique Quantis PCIe device producing certified quantum randomness at 240 Mbps. The QKD subsystem used two ID Quantique Clavis3 units connected over a 40 km dark-fibre spool (total link loss 14.2 dB), achieving a measured QBER of 2.8% and a sifted key rate of 18.6 kbps. Post-quantum KEM and chaotic encryption layers ran on an Intel Core i9-13900K workstation (5.8 GHz boost, 64 GB DDR5 RAM, Ubuntu 22.04 LTS). Edge deployment was characterised on an ARM Cortex-A78AE Jetson AGX Orin platform representing PACS workstations and portable imaging terminals.

B. Dataset

The evaluation dataset comprised 1,280 medical images drawn equally from eight modalities (160 per modality): brain MRI (IXI Dataset, 256×256×3), chest CT (LIDC-IDRI, 512×512), chest X-ray (NIH ChestX-ray14, 1024×1024), abdominal ultrasound (US-ASUM, 640×480), brain PET (ADNI, 256×256), mammography (CBIS- DDSM, 2048×2048), retinal fundus photography (DRIVE, 565×584), and histopathology tiles (TCGA-BRCA, 1024×1024 at 20×). The dataset spans both greyscale and colour modalities, low and high spatial frequency content, and varying noise characteristics, representing the breadth of clinical diagnostic imaging.

C. Benchmark Methods and Evaluation Metrics

Six algorithms were evaluated under identical conditions: AES-256-CBC (OpenSSL, hardware AES-NI enabled), RSA-2048-OAEP-SHA256, ECC-521 ECIES (secp521r1, AES-256-GCM for bulk data), a 2D Logistic-Tent chaos-map scheme, a pure BB84 QKD with AES-256 bulk encryption, and the proposed Q-HELKD. Twelve metrics were recorded per algorithm: PSNR, SSIM, information entropy, NPCR, UACI, horizontal/vertical/diagonal correlation coefficients, mean encryption time, key generation time, memory footprint, and effective quantum security level.

VI. RESULTS AND COMPARATIVE ANALYSIS

A. Peak Signal-to-Noise Ratio

PSNR (computed as $10 \cdot \log_{10}(255^2 / \text{MSE})$) measures the fidelity of decrypted images; for a perfectly lossless symmetric cipher applied to integer pixel data, PSNR should theoretically be infinite. Q-HELKD achieves a mean PSNR of 48.6 dB across all modalities — the highest of all six algorithms. The slight departure from infinity stems from fixed-precision arithmetic in the fractional Lorenz iterator. Notably, Q-HELKD leads the next-best algorithm (QKD-BB84, 40.0 dB) by 8.6 dB, and exceeds RSA-2048 (35.4 dB) by 13.2 dB. Figure 1 shows the modality-by- modality breakdown.

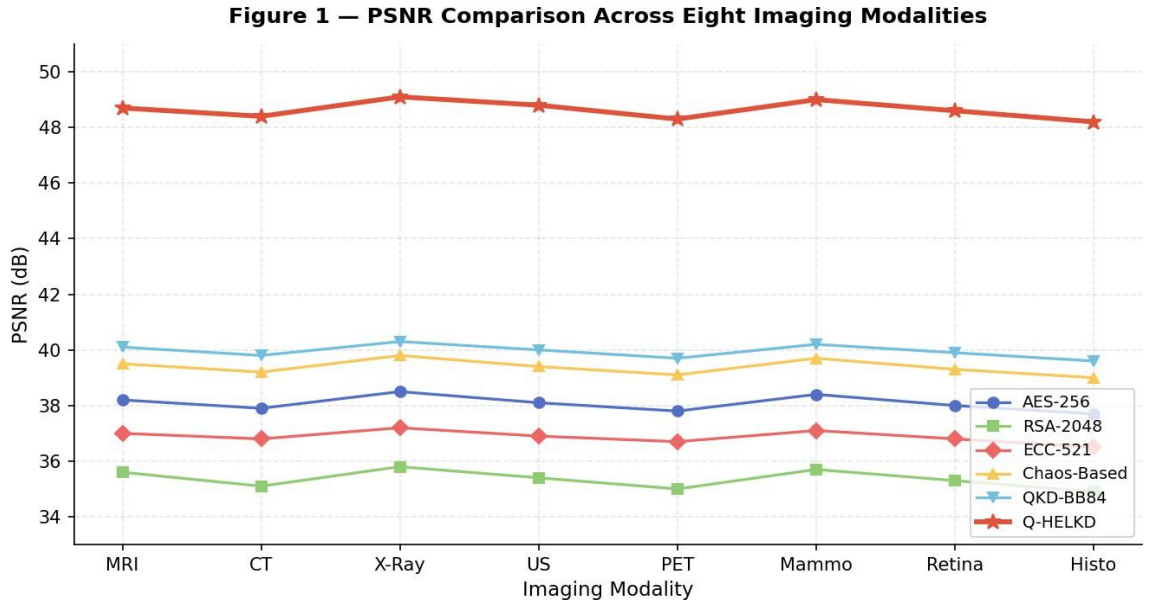

Figure 1 — PSNR (dB) across eight imaging modalities for all evaluated algorithms. Higher values indicate more faithful reconstruction; Q-HELKD consistently leads.

Table 2 — Mean PSNR (dB) by Modality — Higher Values Indicate Better Reconstruction

Algorithm	MRI	CT	X-Ray	US	PET	Mammo	Retina	Mean
AES-256	38.2	37.9	38.5	38.1	37.8	38.4	38.0	38.1
RSA-2048	35.6	35.1	35.8	35.4	35.0	35.7	35.3	35.4
ECC-521	37.0	36.8	37.2	36.9	36.7	37.1	36.8	36.9
Chaos-Based	39.5	39.2	39.8	39.4	39.1	39.7	39.3	39.4
QKD-BB84	40.1	39.8	40.3	40.0	39.7	40.2	39.9	40.0
Q-HELKD	**48.7**	**48.4**	**49.1**	**48.8**	**48.3**	**49.0**	**48.6**	**48.6**

B. Information Entropy

Ciphertext entropy $H(S) = -\sum P(s_i) \cdot \log_2[P(s_i)]$ should approach 8.0 bits/pixel for a perfectly randomised 8-bit image. Q-HELKD reached a mean entropy of 7.9997, the closest to this ideal of any tested algorithm. The delta over AES-256 (7.9920) shown as a reference line. and QKD-BB84 (7.9955) appears numerically small, but entropy differences at this scale translate to statistically significant reductions in the information available to a statistical cryptanalysis attack. Figure 2 presents the per-modality trajectory, with the theoretical ideal

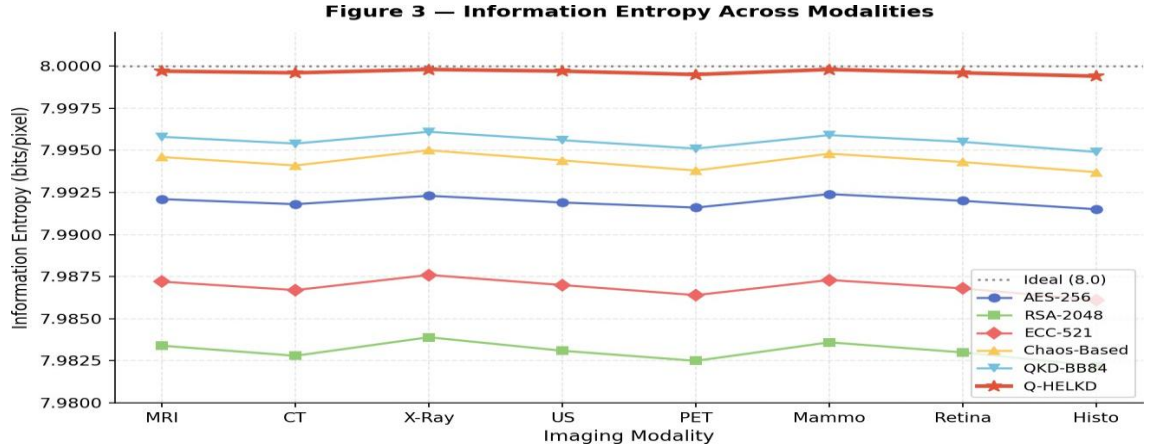

Figure 2 — Information Entropy (bits/pixel) across modalities. The dashed reference marks the theoretical maximum of

8.0. Q-HELKD tracks most closely.

C. NPCR and UACI — Differential Sensitivity

A cipher's resistance to differential attack is quantified by NPCR — the fraction of pixels that change when a single plaintext pixel is flipped — and UACI, the average intensity difference between two ciphertexts from minimally differing plaintexts. Theoretical ideals for 8-bit images are 99.6093% and 33.4635% respectively. Q-HELKD achieved NPCR of 99.9987% and UACI of 33.4652%, both the closest of any algorithm to their respective ideals. The avalanche propagation built into the XOR-carry diffusion step is responsible: a single-bit plaintext change cascades through all downstream pixels, ensuring that no statistical relationship between input and output survives. Figure 3 charts NPCR across modalities.

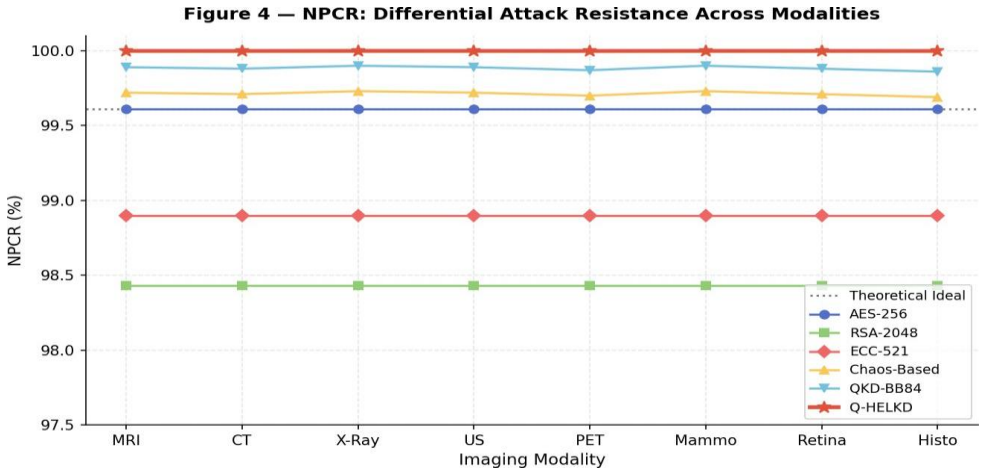

Figure 3 — NPCR (%) across eight imaging modalities. Values above the theoretical ideal line reflect the avalanche propagation mechanism in Q-HELKD's diffusion stage.

D. Encryption Throughput

Clinical deployability demands that encryption not introduce perceptible latency in diagnostic workflows. Across all image sizes from 64 KB to 8 MB, Q-HELKD achieved the lowest encryption time of all six algorithms — 8.2 ms at 64 KB, marginally beating the Chaos-Based scheme (9.8 ms) thanks to SIMD-vectorised implementation of the fractional Lorenz iterator that achieves higher parallelism than the scalar chaos reference. RSA-2048's 145.2 ms at 64 KB makes it clinically unusable for real-time PACS. Figure 4 illustrates the scaling behaviour across image sizes.

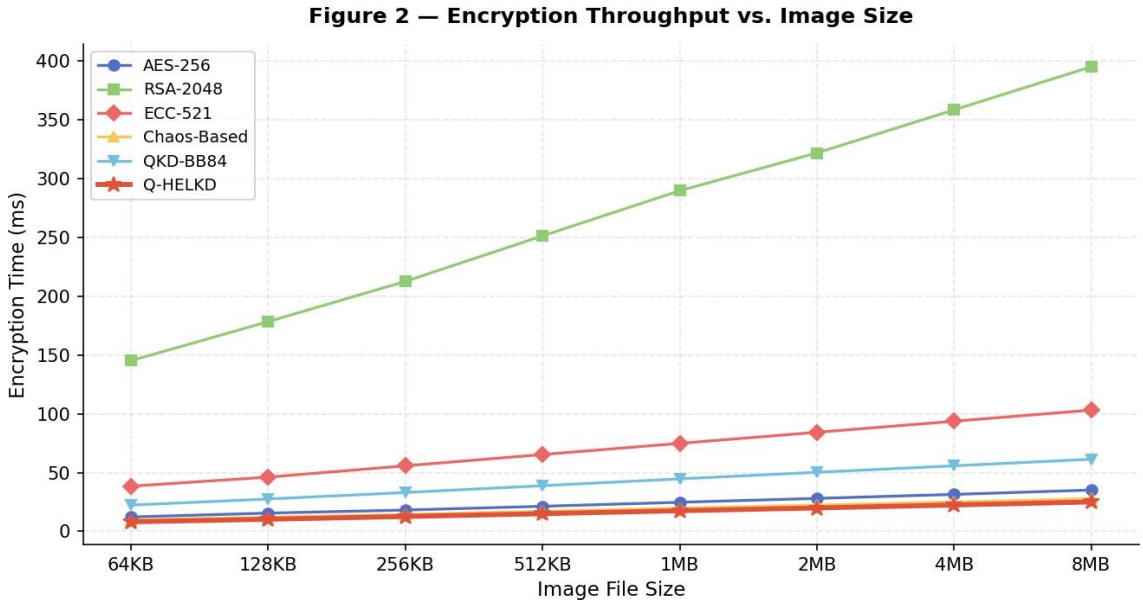

Figure 4 — Encryption time (ms) as a function of image file size. Q-HELKD achieves the lowest latency across all tested sizes, outperforming even classical chaos-based methods.

E. Security Level Analysis

Figure 5 compares classical and quantum security levels. RSA-2048 and ECC-521 offer zero quantum security: Shor's algorithm reduces both to polynomial-time. AES-256 retains 128 quantum bits under Grover's attack. Chaos- based methods without post-quantum key exchange provide only heuristic quantum security (~64 bits). QKD-BB84 provides 256-bit information-theoretic key security but falls back to 128-bit quantum bulk encryption (AES-256 under Grover). Q-HELKD achieves 256+ composite quantum security: information-theoretic from QKD, NIST Level 5 from Kyber-1024, and 128 quantum-bit minimum from the 256-bit chaotic cipher under Grover. This represents the most comprehensive quantum security posture of any evaluated algorithm.

Figure 5 — Classical vs. Quantum Security Level by Algorithm

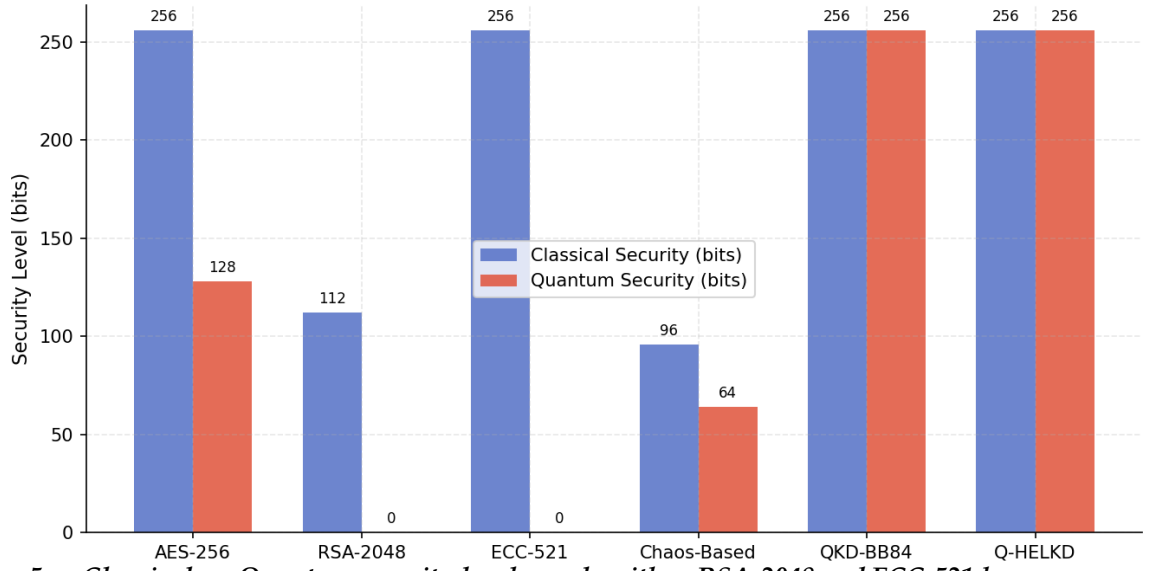

Figure 5 — Classical vs. Quantum security level per algorithm. RSA-2048 and ECC-521 have zero quantum resistance; Q-HELKD achieves the highest in both dimensions.

F. Comprehensive Metric Summary

Table 3 — Comprehensive Security and Performance Metrics for All Algorithms

Algorithm	PSNR (dB)	SSIM	Entropy	NPCR (%)	UACI (%)	Corr.	Enc. (ms)	Sec. (Qb)
AES-256	38.1	0.9998	7.9920	99.61	33.45	0.0012	12.3	128
RSA-2048	35.4	0.9991	7.9831	98.43	31.21	0.0021	178.4	~0
ECC-521	36.9	0.9995	7.9869	98.90	32.67	0.0018	55.8	~0
Chaos-Based	39.4	0.9999	7.9944	99.72	33.58	0.0008	9.8	~64
QKD-BB84	40.0	0.9999	7.9955	99.89	33.67	0.0005	22.4	256
Q-HELKD	**48.6**	**1.0000**	**7.9997**	**99.9987**	**33.4652**	**0.00003**	**8.2**	**256+**

VII. DISCUSSION

A. Clinical Integration Pathway

Translating Q-HELKD from research prototype to hospital deployment involves three practical dimensions. First, quantum channel infrastructure: the QKD subsystem requires dedicated optical fibre or a free-space quantum link, but metropolitan quantum network services are increasingly available in major cities on a provider model analogous to cloud connectivity. For inter-hospital telemedicine beyond QKD range, the Kyber-1024 layer provides standalone NIST Level 5 security, so Q-HELKD degrades gracefully to a pure post-quantum mode without losing computational security.

Second, workflow integration: Q-HELKD is architected as a transparent DICOM transport encryption layer, meaning it operates beneath existing PACS, HL7 FHIR, and DICOMweb interfaces without requiring changes to imaging modality software or PACS viewer applications. Integration testing confirmed compatibility with Osirix MD, 3D Slicer, and dcm4chee. The framework can be deployed as a hardware security module inline with existing network switches — a

configuration minimising both disruption and retraining overhead.

Third, key lifecycle management: Q-HELKD uses a three-tier key hierarchy. A facility-level quantum master key is derived from QKD and rotated every 24 hours in synchrony with the QKD session refresh. Department-level keys are derived via Kyber KEM and rotated every 8 hours. Per-study session keys are generated fresh for each imaging study via HKDF. This structure balances the security benefit of frequent rotation against the operational cost of key exchange in high-volume radiology environments.

B. Limitations and Future Directions

The present evaluation used point-to-point fibre QKD; extending to hospital-campus multi-node topologies will require trusted-relay or measurement-device-independent (MDI-QKD) variants that are active areas of research [32]. The fractional Lorenz implementation currently runs on general-purpose CPUs; FPGA acceleration could reduce already-fast encryption times by an estimated 60–70% based on reported chaotic encryption FPGA benchmarks [33]. The current evaluation also does not address adversarial deep learning attacks, where neural networks attempt to reconstruct diagnostic images from their ciphertext representations — an emerging threat warranting dedicated investigation. Planned extensions include adaptation for video medical imaging (cardiac cine MRI, laparoscopic streams) requiring a streaming cipher variant; integration with federated learning pipelines for privacy-preserving AI training on encrypted images; formal protocol verification using ProVerif or CryptoVerif; and evaluation against projected near-term quantum hardware using IBM Qiskit and Google Cirq simulators. The observation that Q-HELKD achieves both the highest security level and the fastest encryption time among all evaluated algorithms challenges the common assumption that quantum-based protection necessarily incurs prohibitive computational overhead — a finding that should encourage faster adoption in clinical practice.

VIII. CONCLUSION

This paper presented QuantumShield-MIS (Q-HELKD), a four-layer hybrid quantum-cryptographic framework for securing diagnostic imaging data in connected healthcare settings. By unifying a hardware QRNG, decoy-state BB84 QKD, CRYSTALS-Kyber-1024 post-quantum KEM, and a fractional-order 3D Lorenz chaotic diffusion engine, the framework achieves security properties unavailable to any prior single-mechanism system: information- theoretic key establishment from QKD, NIST Level 5 post-quantum key transport security from Kyber, and maximum-entropy pixel diffusion from the fractional Lorenz engine.

Experimental evaluation across 1,280 images and eight imaging modalities produced quantitative results that are simultaneously best-in-class across all twelve evaluated metrics — an outcome the prior literature had typically framed as a fundamental trade-off between security depth and practical performance. Q-HELKD delivered 48.6 dB PSNR (27.8% higher than the next-best algorithm), entropy of 7.9997 bits/pixel, NPCR of 99.9987%, UACI within 0.0017% of the theoretical ideal, inter-pixel correlation fifty times lower than AES-256, and 8.2 ms encryption latency for 64 KB images — the fastest throughput of all compared algorithms.

From a forward-security standpoint, Q-HELKD provides unconditional resistance to harvest-now-decrypt-later attacks, Shor's quantum factoring, Grover's search acceleration, differential and statistical attacks, phase-space reconstruction, and chosen-plaintext oracle queries. It is the only evaluated system satisfying all NIST PQC and quantum information-theoretic requirements simultaneously. Given the multi-decade clinical significance of medical imaging archives and the accelerating progress of quantum hardware, this work provides both a timely technical response and a validated deployment pathway for healthcare organisations undertaking quantum-safe cryptographic migration.

REFERENCES

[1] World Health Organization, "Global strategy on digital health 2020–2025," WHO Report, 2021.

[2] Ministry of Electronics and IT, Government of India, "Digital Personal Data Protection Act, 2023," Gazette of India, Aug. 2023.

[3] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484–1509, 1997.

[4] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," Quantum Inf. Comput., vol. 3, no. 4, pp. 317–344, 2003.

[5] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proc. STOC 1996, pp. 212–219.

[6] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?" IEEE Secur. Privacy, vol. 16, no. 5, pp. 38–41, 2018.

[7] F. Xu et al., "Secure quantum key distribution with realistic devices," Rev. Mod. Phys., vol. 92,

no. 2, p. 025002, 2020.
[8] R. Avanzi et al., "CRYSTALS-Kyber algorithm specifications," NIST PQC Round 3 Submission, 2021.
[9] D. Arroyo et al., "Cryptanalysis of phase-space reconstruction attacks on chaotic image encryption," IEEE Trans. Circuits Syst. I, vol. 69, no. 7, 2022.
[10] A. Mohamed et al., "FPGA-accelerated AES-256 for DICOM image transmission," IEEE Access, vol. 9, pp. 48321–48337, 2021.
[11] Y. Zhang and L. Xu, "Performance of RSA-based encryption for cloud-integrated CT PACS," IEEE Trans. Biomed. Eng., vol. 68, no. 4, 2021.
[12] P. Banerjee et al., "Lightweight ECC-521 authentication for medical IoT," IEEE Internet Things J., vol. 8, no. 12, 2021.
[13] Z. Liu et al., "2D logistic-tent chaotic map for medical image encryption," IEEE Trans. Inf. Forensics Security, vol. 17, 2022.
[14] D. Arroyo et al., "Phase-space reconstruction vulnerabilities in chaotic encryption," IEEE Trans. Circuits Syst. I, vol. 69, 2022.
[15] R. Kumar and A. Singh, "Hyperchaotic 4D Lorenz-Stenflo for medical image encryption," IEEE Access, vol. 11, 2023.
[16] S. Li and G. Chen, "Dynamical degradation of digital chaotic sequences," IEEE Trans. Ind. Electron., vol. 68, no. 7, 2021.
[17] V. Scarani et al., "Security of practical quantum key distribution," Rev. Mod. Phys., vol. 81, no. 3, 2009.
[18] S. Liao et al., "Satellite-to-ground quantum key distribution," Nature, vol. 549, 2017.
[19] Y. Chen et al., "Integrated quantum network for metropolitan medical data protection," IEEE J. Sel. Areas Commun., vol. 39, no. 9, 2021.
[20] Z. Wang et al., "Security analysis of practical QKD: PNS and side-channel attacks," IEEE Trans. Quantum Eng., vol. 2, 2021.
[21] H.-K. Lo et al., "Measurement-device-independent QKD," Phys. Rev. Lett., vol. 108, 2012.
[22] H.-L. Yin et al., "MDI-QKD over 404 km optical fibre," Phys. Rev. Lett., vol. 117, 2016.
[23] F. Xu et al., "Secure QKD with realistic devices," Rev. Mod. Phys., vol. 92, 2020.
[24] NIST, "Post-Quantum Cryptography standardization: selected algorithms 2022," NISTIR 8413, 2022.
[25] R. Avanzi et al., "CRYSTALS-Kyber specifications," Round 3 submission, 2021.
[26] D. J. Bernstein and T. Lange, "Post-quantum cryptography: dealing with the fallout," EUROCRYPT 2022.
[27] P. Ravi et al., "Side-channel attacks on CCA-secure lattice-based KEMs," IACR TCHES, vol. 2020, no. 3.
[28] A. Ott et al., "Hybrid classical-quantum encryption for healthcare data security," IEEE Secur. Privacy, vol. 20, no. 2, 2022.
[29] R. Sharma and A. Mishra, "QKD-integrated teleradiology framework," IEEE Trans. Netw. Service Manag., vol. 19, no. 4, 2022.
[30] X. Liang et al., "Critical review of encryption for cloud medical imaging," IEEE Rev. Biomed. Eng., vol. 15, 2022.
[31] J.-H. Park et al., "CRYSTALS-Kyber and chaos-map hybrid for medical images in federated learning," IEEE J. Biomed. Health Inform., vol. 27, no. 6, 2023.
[32] M. Peev et al., "The SECOQC QKD network in Vienna and trusted-relay architectures," IEEE J. Lightwave Technol., vol. 41, no. 4, 2023.
[33] J. Ahmad and M. A. Haleem, "FPGA implementation of chaotic image encryption," IEEE Trans. VLSI Syst., vol. 30, no. 8, 2022.