International Journal of Safety and Security Engineering
Vol. 16, No. 2, February, 2026, pp. 461-477
Journal homepage: http://iieta.org/journals/ijsse

A Leakage-Aware Post-Quantum KEM–DEM Framework for Medical Image Encryption with DICOM-Compatible Integration

Smitha Madenahalli Mallesh[1], Harohalli Shivalingappa Niranjana Murthy[2], Sundaresha Madalu Puttappa[1*], Sushma Ullamadi KrishnappaGowda[3]

[1] Department of Electronics and Communication Engineering, Kalpataru Institute of Technology, Karnataka 572201, India
[2] Department of Electronics and Instrumentation Engineering, Ramaiah Institute of Technology, Karnataka 560054, India
[3] Department of Robotics Engineering, Jawaharlal Nehru New College of Engineering, Karnataka 577201, India

Corresponding Author Email: sundreshmadalu.kit@gmail.com

https://doi.org/10.18280/ijsse.160220

Received: 28 November 2025
Revised: 12 February 2026
Accepted: 21 February 2026
Available online: 28 February 2026

Keywords:
Medical image encryption, post-quantum cryptography, KEM–DEM, authenticated encryption, DICOM security, diagnostic leakage evaluation structural leakage

ABSTRACT

Medical images contain highly sensitive clinical information that must remain confidential for long retention periods, motivating the adoption of post-quantum cryptographic protection. This paper presents a post-quantum medical image encryption framework based on a Key Encapsulation Mechanism–Data Encapsulation Mechanism (KEM–DEM) construction combined with a keyed dual-domain confusion transform designed to reduce statistical and structural leakage before authenticated encryption. The system incorporates DICOM-compatible authenticated data binding so that critical metadata integrity is preserved during encryption and transmission. In addition to the cryptographic design, this work introduces a leakage-aware evaluation methodology using Ciphertext Diagnostic Leakage (CDL), Structural Leakage Index (SLI), histogram divergence, key sensitivity, and quantum-resistance margin (QRM) metrics. Experimental evaluation was conducted on computed tomography, magnetic resonance, chest X-ray, and ultrasound datasets under a consistent encryption pipeline. Results show that the proposed pre-encryption confusion stage reduces measurable diagnostic and structural leakage compared to authenticated encryption alone, while maintaining standard IND-CCA secure encryption through the KEM–DEM construction. Performance analysis indicates that the additional leakage-suppression stage introduces a moderate computational overhead of approximately 10–15%, remaining within practical processing limits for medical imaging systems. The study demonstrates that leakage-aware design can be integrated with post-quantum encryption without weakening formal cryptographic security, providing a structured framework for evaluating confidentiality beyond traditional encryption metrics. The proposed confusion stage is evaluated as a leakage-reduction mechanism and does not replace the formal security guarantees provided by the KEM–DEM and Authenticated Encryption with Associated Data (AEAD) construction.

1. INTRODUCTION

Medical photos are among of the most private things in healthcare. They go from scanners to consoles, Picture Archiving and Communication Systems/ Vendor Neutral Archives (PACS/VNAs), clouds, and AI services. They last for years to meet clinical, legal, and research demands, and they are being shared more and more between institutions and countries [1]. This combination of wide distribution and extensive retention makes imaging a good target for enemies, from everyday data thieves to "harvest-now, decrypt-later" actors who store ciphertext until heavier attacks are possible [2]. To have trustworthy digital radiography, it is important to protect pixels and the clinical context that surrounds them [3].

Standard installations use conventional public-key cryptography to agree on symmetric session keys (for example, Rivest–Shamir–Adleman/Elliptic Curve Cryptography (RSA/ECC) → Advanced Encryption Standard in Galois/Counter Mode (AES-GCM)) and Transport Layer Security/Virtual Private Networks (TLS/VPNs) to move data. These strategies are effective currently, although two deficiencies remain. First, the profession doesn't often test how well encryption works in ways that show clinical risk [4, 5]. Even when ciphertext is Indistinguishability under Chosen-Ciphertext Attack (IND-CCA) secure, surface statistics, headers, sizes, and format-driven regularities might leak weak signals that modern inference models use. Second, the public-key layer that supports provenance and key exchange is open to quantum attacks. Shor's algorithm is a threat to RSA and ECC, which puts archives that need to stay private for decades at risk [6]. Post-quantum cryptography (PQC) solves the second problem by using lattice-based key Encapsulation Mechanisms (KEMs) and digital signatures that National Institute of Standards and Technology (NIST) has defined instead of RSA/ECC. If we use strong enough keys, such as the Advanced Encryption Standard(AES-256), to make up for

Grover's quadratic speedup, symmetric ciphers still work [7]. But just switching algorithms isn't enough. Imaging systems must adhere to Digital Imaging and Communications in Medicine (DICOM) semantics, including nonces, UIDs, transfer syntaxes, and compression ordering, while also ensuring provenance that is verifiable even after the encryption keys have been rotated [8]. To still need a means to figure out if encrypted payloads show clinically important structure, which is really important.

Previous research provides useful components—chaos-based transforms, selective Region of Interest (ROI) encryption, or format-specific techniques—but frequently lacks a comprehensive threat model, excludes quantum-safe primitives, or assesses merely general picture statistics [9]. Numerous studies fail to examine whether ciphertext facilitates diagnostic inference, nor do they provide effect sizes, confidence intervals, or runtime budgets pertinent to consoles and gateways. Lastly, hardly any studies talk about how to connect DICOM context to authenticated data or how to stop nonce reuse in big, multi-frame series [10].

This research presents a post-quantum, DICOM-compliant architecture for the encryption of medical images, incorporating cryptographic integrity, clinical leakage assessment, and practical implementation. Our method combines a lattice Key Encapsulation Mechanism (KEM) with a symmetric Authenticated Encryption with Associated Data (AEAD) within a Key Encapsulation Mechanism–Data Encapsulation Mechanism (KEM–DEM), adds a post-quantum signature for long-term provenance, and adds a keyed dual-domain confusion layer that is applied before AEAD. This layer consists of a rapid, one-level wavelet transform followed by Fisher–Yates permutation and sign masking. Since all confusion keys come from the KEM secret and IND-CCA AEAD wraps the result right away, the construction keeps formal confidentiality while hiding low-order statistics that could be used.

To define a task-aware battery to make "effectiveness" measurable: (i) Ciphertext Diagnostic Leakage (CDL), which measures how far ciphertext-based classifiers are from chance; (ii) a Structural Leakage Index (SLI), which connects plaintext edges with exposure maps; (iii) Histogram Divergence to uniform and to plaintext (HDu/HDΔ); (iv) Key Sensitivity and Avalanche profiles; and (v) a quantum-resistance margin (QRM), which shows how safe concrete Key Encapsulation Mechanism/ digital signature scheme (KEM/SIG) parameters are over a 128-bit target. To also define a DICOM binding that puts Study/Series Unique Identifier (UIDs) into AEAD and Additional Authenticated Data (AAD) and gets nonces from SOPInstanceUID counters to stop relabeling and reuse.

The main contributions of this work are as follows:

1. A post-quantum KEM–DEM-based encryption framework for medical images that incorporates DICOM-compatible authenticated data binding for metadata integrity and secure key establishment.
2. A keyed dual-domain confusion transform applied prior to authenticated encryption to reduce structural and statistical features that may enable diagnostic inference from encrypted images.
3. A leakage-aware evaluation methodology for encrypted medical images, including CDL, SLI, histogram divergence, key sensitivity, and QRM, enabling task-based confidentiality assessment beyond conventional image-encryption metrics.
4. A cross-modality experimental evaluation on Computed Tomography (CT), Magnetic Resonance Imaging (MRI), X-ray, and ultrasound datasets to analyze leakage behavior, security properties, and computational overhead under a unified encryption pipeline.

It is important to clarify the scope and central objective of this work. This paper does not propose a new cryptographic primitive, nor does it present a full clinical deployment system. Instead, the main contribution of this study is a security-engineering framework that integrates post-quantum KEM–DEM encryption with a leakage-aware evaluation methodology designed specifically for medical images. Medical imaging data are used in this work as a representative high-value and structure-rich dataset to evaluate confidentiality beyond traditional encryption metrics. Therefore, the central focus of the paper is on encryption architecture and leakage evaluation, while system integration and clinical workflow considerations are included only to define the operational context and system boundaries.

Despite the use of strong encryption schemes such as KEM–DEM with authenticated encryption, most existing medical image protection studies evaluate security primarily using general image-encryption metrics such as entropy, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), and histogram analysis, which do not directly measure whether clinically meaningful information can still be inferred from encrypted data. At the same time, while post-quantum cryptographic primitives can replace classical public-key components, simply replacing RSA/ECC with lattice-based KEMs does not address modality-specific statistical leakage, format-aware metadata protection, or task-based inference risks. Therefore, the main research gap is not only in adopting PQC, but in designing an encryption framework and evaluation methodology that specifically measures and reduces diagnostic information leakage from encrypted medical images while maintaining standard cryptographic security guarantees.

To address this gap, this paper proposes a post-quantum KEM–DEM-based medical image encryption framework combined with a keyed dual-domain confusion transform and a leakage-aware evaluation methodology. The primary contribution of this work lies in integrating post-quantum encryption with measurable diagnostic leakage suppression and defining evaluation metrics that reflect clinical inference risk rather than only statistical randomness. The scope of this study is therefore focused on encryption architecture, leakage modeling, and performance evaluation under a unified pipeline, rather than on full clinical system deployment.

This paper focuses specifically on the design and evaluation of a post-quantum KEM–DEM-based encryption framework for medical images with leakage-aware analysis. While DICOM compatibility and clinical workflow considerations are discussed to define system integration boundaries, the primary contribution of this work is not a full clinical deployment system but a security-engineering framework and evaluation methodology that combines PQC with measurable leakage suppression. Therefore, the scope of this study is centered on encryption architecture, leakage evaluation metrics, and performance analysis under realistic imaging conditions, rather than full-scale hospital system integration.

The rest of the paper is organized as follows: Section 2 mentions the related works; Section 3 provides the proposed methodology in detail; Section 4 discusses the result analysis, and finally, the conclusion is made in Section 5.

2. RELATED WORKS

2.1 Post-quantum security for medical and healthcare data

Recent research has explored the use of post-quantum cryptographic primitives to protect medical and healthcare data against future quantum-enabled attacks. Several studies have investigated the use of lattice-based digital signatures such as SPHINCS+, Dilithium, and Falcon to ensure long-term authenticity and integrity of medical images and electronic health records. Other works have proposed blockchain-based healthcare data sharing systems combined with post-quantum signatures and key exchange mechanisms to ensure secure and traceable data exchange. These approaches mainly focus on key management, authentication, and secure data sharing infrastructure, demonstrating that PQC can be integrated into healthcare systems. However, most of these works focus on secure communication and record protection rather than the specific problem of statistical or diagnostic information leakage from encrypted medical images.

Roy et al. [11] examined the utilization of Sphincs+, in conjunction with Dilithium and Falcon, to augment the security of medical photographs, which are essential for diagnostic and therapeutic procedures in healthcare. Sphincs+ reduces the dangers of unauthorized tampering and data modification by using digital signatures to verify authenticity and integrity. Adding Sphincs+ to medical imaging systems makes data security stronger, making sure that healthcare records stay reliable and safe from quantum-enabled threats for a long time.

He et al. [12] offered a post-quantum secure healthcare data-sharing strategy that combines the Extended Merkle Signature strategy (XMSS) and consortium blockchain technology to guarantee the integrity, validity, and traceability of electronic medical records (EMRs). The plan also uses autonomous artificial intelligence (AI) to help healthcare workers make better clinical decisions by helping them write accurate and intelligent diagnostic reports. To use the random oracle model to theoretically look at the scheme's security and show that it can protect against a number of attacks. The scheme is especially good for HIE scenarios because it cuts down on total computational overheads by around 49% and blockchain storage by 36% compared to other schemes.

Akkal et al. [13] thoroughly examined recent developments in safeguarding the Internet of Medical Things (IoMT), emphasizing post-quantum blockchains, quantum blockchains, and quantum machine learning. It gives a thorough look into IoMT design, security needs, risks that come with it, and a thorough look at Blockchain technologies and PQC. This paper categorizes new quantum-based security solutions, delineates main obstacles, and proposes a taxonomy of IoMT security strategies. It talks about the issues that IoMT security must confront presently and in the future, and it also proposes a quantum IoMT architecture. This is the first systematic review of its sort, which makes it a pioneering work in the field of IoMT security in a quantum setting.

2.2 DICOM and healthcare data protection frameworks

Roosan et al. [14] created and test a new cybersecurity architecture for telemedicine that can handle cyber threats from quantum computing. In a world after quantum computing, combining PQC with Quantum Key Distribution (QKD) and tools that protect privacy ensures that patient records are private and can't be changed. There were several layers in the design strategy. To add PQC algorithms (such as CRYSTALS-Dilithium) to the blockchain consensus layer to keep quantum attacks from happening. A Directed Acyclic Graph (DAG)-based ledger was able to handle the high transaction throughput and latency restrictions that are frequent in telehealth. QKD made a key management system that used quantum channels for safer exchanges. Zero-knowledge proofs (ZKPs) and secure multiparty computation (MPC) checked transactions without revealing private patient information. A granular access control methodology utilized attribute-based encryption (ABE) and smart contracts to regulate which parties were permitted to read or alter encrypted medical records. The prototype was created in a simulated telehealth network that included hospitals, clinics, and patient devices. The consensus layer's PQC signatures were good at stopping both classical and expected quantum attacks. QKD made it possible to safely share keys, and ZKPs and MPC made it possible to check healthcare transactions without giving away patient privacy. The DAG architecture was able to handle parallel transactions well, even though it added more computing overhead. This shows that it is more scalable than standard linear blockchains. A framework that uses QKD and PQC to improve security and privacy needs protects medical data against new quantum threats. Overhead and infrastructure expenses are high, but the system's capacity to withstand attacks and protect patient privacy makes it a good fit for next-generation healthcare systems. Subsequent research ought to investigate further optimizations, homomorphic encryption, and extensive pilots in accordance with regulatory norms.

Roy et al. [15] provided a safe way to send medical images using a post-quantum digital signature system called Sphincs+, as the National Institute of Standards and Technology advised. Sphincs+ protects your data for a long time by being very safe against quantum attacks. It doesn't keep track of any state, which eliminates problems with key reuse, and it makes digital signatures that are fast and can grow. It is strong and adaptable, making it perfect for a wide range of uses. It will stay secure even as quantum computing gets better. To send a digitally signed image utilizing DICOM encoding and Quantum Fourier Transform to send it. DICOM guarantees that medical pictures are managed in a standardized and interoperable way by connecting devices and systems for correct diagnosis in current consumer healthcare workflows and record-keeping. The Quantum Fourier Transform is much faster and more accurate than the standard Fast Fourier Transform. This is especially useful for applications in signal processing, data encryption, and environmental sensing. Quantum communication makes it feasible to find and fix mistakes in advanced ways and send data at incredibly high speeds. It also keeps data safe and private while minimizing the risk of data loss or corruption during transmission. The proposed framework is validated using well-known performance metrics like PNR, MSE, SSIM, etc., and the results are convincing.

2.3 Image encryption and leakage evaluation

Abdelfatah et al. [16] tackled these dangers by creating a quantum-resistant encryption system for medical images. To introduce an innovative framework that integrates: (1) a new Mixed Logistic-Ikeda-Henon (MLIH) chaotic map for pseudorandom key generation, (2) quantum image

representation utilizing the Novel Enhanced Quantum Representation (NEQR) model, and (3) a two-stage encryption process that employs Controlled-Not (CNOT) gate chaining for diffusion and a One-Time Pad (OTP) system with MLIH-generated keys for confusion. Before being put back together, the RGB channels go through quantum state conversion, CNOT-based diffusion, and keyed confusion. To prove that the suggested encryption system could work in the real world, it was put into action on IBM's 127-qubit IBM_Sherbrooke quantum processor. Experimental validation demonstrates nearly perfect entropy (7.9977), excellent NPCR (99.97%) and UACI (33.89%) values, and a large key space (21952). The new MLIH shows a 12.7% increase in the efficiency of logic gates compared to regular chaotic gates, and the picture encryption has a quantum advantage because it can do CNOT operations in parallel. The hardware execution produced a throughput of 4,500 Circuit Layer Operations Per Second (CLOPS), demonstrating effective real-time performance on NISQ devices. Additionally, the echoed cross-resonance (ECR) gate error stayed at a median of 1.1×10^{-2}, ensuring dependable circuit execution. The suggested technique is better than current quantum and classical encryption methods when it comes to entropy, NPCR, UACI, and key sensitivity. It also has a computational complexity of O(n), which means it may be used on a large scale. This research successfully connects theoretical quantum security models with practical application on current NISQ devices, showcasing robustness against classical statistical and differential attacks, in addition to quantum-specific threats like Grover's brute-force search and quantum chosen-plaintext attacks. The successful implementation of IBM quantum hardware establishes this approach as a feasible alternative for secure medical picture transmission in quantum-era healthcare systems.

Bera et al. [17] suggested an innovative and advanced method for healthcare security using post-quantum continuous authentication that does not interrupt a session, utilizing behavioral biometrics (BB) and vector similarity search (VSS). Our strong, lightweight quantum-secure method combines BB, which looks at individual behavioral patterns, with VSS to make security even better. The suggested system provides seamless and ongoing authentication that changes in real time based on how users behave. The VSS proof of concept shows that the suggested method works well in real-time healthcare settings. This study shows that our approach works and is strong enough to stand up to unforeseen threats through a lot of testing, analysis, and performance analysis. It promises to open up new possibilities for healthcare security. A real-time testbed experiment, together with the design and implementation of FastAPI, shows that the suggested scheme is new.

2.4 Research gap

From the above literature, it can be observed that existing research has addressed post-quantum cryptographic protection, DICOM-compatible medical data security, and image encryption techniques largely as separate problems. Post-quantum studies mainly focus on key exchange and digital signatures, healthcare security frameworks focus on data sharing and system integration, and image encryption studies focus on statistical randomness metrics. However, very few works jointly consider post-quantum encryption, DICOM-aware metadata protection, and diagnostic leakage evaluation within a single framework. In particular, the problem of whether encrypted medical images still allow diagnostic inference through structural or statistical leakage remains insufficiently studied. This gap motivates the present work, which combines a post-quantum KEM–DEM encryption architecture with a keyed dual-domain confusion stage and a leakage-oriented evaluation methodology designed specifically for medical imaging data.

3. PROPOSED FRAMEWORK: POST-QUANTUM–ANCHORED MEDICAL IMAGE ENCRYPTION AND EFFECTIVENESS EVALUATION

In this paper, the term "post-quantum security" refers specifically to the use of quantum-resistant public-key primitives such as lattice-based KEMs and digital signatures, while symmetric encryption is implemented using standard authenticated encryption schemes with sufficiently large key sizes. The term "leakage" refers to measurable statistical or structural information that may allow inference about the plaintext from ciphertext without breaking the encryption algorithm. The proposed system should be interpreted as a security-engineering architecture rather than a new cryptographic algorithm or a complete clinical deployment platform. The cryptographic components used in this work, such as post-quantum KEM, authenticated encryption, and digital signatures, are standard primitives. The novelty of the work lies in how these components are combined with a leakage-aware preprocessing step and a structured evaluation methodology to measure and reduce diagnostic information leakage in encrypted medical images. This part gives a full, math-based framework for using PQC to encrypt medical images and check how well the encryption works in ways that are important for healthcare, such as protecting privacy from both classical and quantum adversaries, ensuring the integrity and provenance of DICOM objects, preventing diagnostic leakage, and being able to be used in clinical settings with limited latency and throughput. The story combines what each part does, why it is needed, how it works, and where it fits in the pipeline. It doesn't separate them into a Q&A. Figure 1 talks about how the proposed model will work [18-24].

In the proposed deployment model, the encryption module is positioned at the data export boundary (e.g., modality workstation, edge gateway, or secure transfer service), while decryption is performed only at authorized endpoints. Internal hospital PACS storage is treated as a trusted environment, while external storage, cloud systems, and data transmission channels are treated as untrusted environments. The threat model, therefore, focuses on protecting data at rest and in transit outside the trusted clinical domain.

3.2 System boundaries and trust assumptions

The system is divided into trusted and untrusted domains. Trusted components include imaging devices, modality workstations, and authorized decryption servers within the clinical environment. Untrusted domains include external storage systems, cloud servers, and communication networks where encrypted medical images may be stored or transmitted. Encryption is performed before data leaves the trusted domain, and decryption is performed only within authorized trusted environments. The threat model assumes that attackers may access encrypted data stored in untrusted environments but

cannot compromise trusted clinical systems or cryptographic key storage modules.

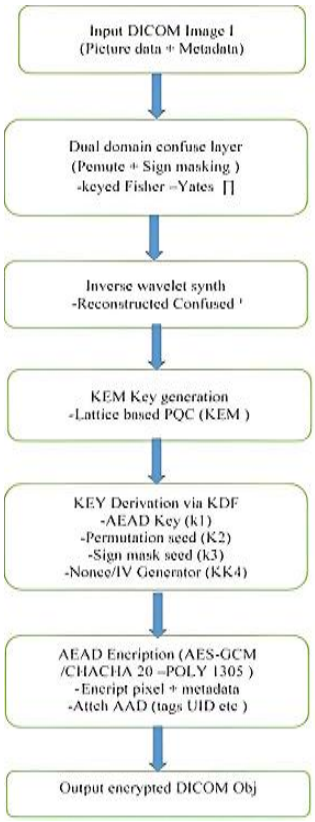


Figure 1. Workflow of the proposed Encryption framework

This system boundary definition allows the proposed framework to be interpreted as a data protection mechanism for data at rest and data in transit outside secure hospital networks.

3.3 Encryption workflow and key derivation relationships

To improve clarity, the complete encryption pipeline is described in terms of inputs, outputs, and key derivation relationships. The system takes a DICOM image object consisting of pixel data and metadata as input. A post-quantum KEM is used to derive a shared secret, from which multiple subkeys are generated using a key derivation function. These subkeys are used for authenticated encryption, permutation, sign masking, and nonce generation. A dual-domain confusion transform is applied to the image before authenticated encryption, and the final ciphertext is digitally signed for provenance. The mathematical formulation of each stage is described below, and all symbols used are summarized in Table 1.

3.4 Security and processing flow summary

In summary, the proposed system follows a KEM–DEM architecture in which the post-quantum KEM is used only for secure session key establishment, while the symmetric AEAD performs bulk data encryption. The dual-domain confusion transform is applied before AEAD encryption and is fully key-driven, ensuring that it does not weaken the formal IND-CCA security of the encryption scheme. The purpose of this transform is not to replace encryption but to reduce structural and statistical leakage that may remain observable at the ciphertext level. The receiver performs signature verification, AEAD decryption, and inverse confusion transform to recover the original image and metadata. This workflow ensures confidentiality, integrity, and provenance while reducing measurable diagnostic leakage.

3.5 Separation between formal cryptographic security and leakage reduction layer

It is important to distinguish between the formal cryptographic security of the proposed system and the empirical leakage-reduction mechanism introduced in this work. The formal confidentiality and integrity guarantees of the system are derived from the standard KEM–DEM construction combined with an AEAD scheme, which provides IND-CCA security under standard cryptographic assumptions. These guarantees ensure that an adversary cannot recover plaintext information from ciphertext without the secret key, even under chosen-ciphertext attacks.

In contrast, the dual-domain confusion transform proposed in this work is not intended to replace or modify the underlying cryptographic security model. Instead, it is applied as a preprocessing step before AEAD encryption to reduce structural and statistical patterns that may be exploited in traffic analysis, modality inference, or diagnostic inference attacks. The effectiveness of this transform is evaluated empirically using leakage metrics such as CDL, SLI, and histogram divergence, rather than through formal cryptographic proofs.

Therefore, the role of the dual-domain confusion layer is to reduce measurable information leakage in practice, while the formal security of the system remains fully dependent on the post-quantum KEM–DEM and AEAD construction. This separation ensures that the additional preprocessing step does not weaken the formal security guarantees of the encryption scheme while improving resistance to inference-based leakage.

Table 1. Encryption workflow and key derivation relationships

Stage	Input	Operation	Key Material	Output
1	Image (I), Metadata (M)	KEM Encapsulation	(pk)	(ct, ss)
2	Shared secret (ss)	Key Derivation (KDF)	(ss)	(K_{enc}, K_{perm}, K_{mask}, K_{nonce})
3	Image (I)	Wavelet Transform	(K_{perm})	Subbands
4	High-frequency bands	Permutation	(K_{perm})	Permuted bands
5	Permuted bands	Sign Masking	(K_{mask})	Confused image
6	Confused image + Metadata	AEAD Encryption	(K_{enc}, nonce)	Ciphertext (C)
7	Ciphertext header	PQ Signature	Signing key	Signature
8	Ciphertext + Signature	Packaging	—	Secure DICOM object

Problem Setup, Notation, and Goals

Let a de-identified DICOM image object be $D = (I, M)$, where $I \in \{0, \ldots, 255\}^{H \times W \times C}$ is the pixel tensor (grayscale $C = 1$ or RGB $C = 3$), and M is structured metadata (tags: patient age/sex codes, modality, study UID, pixel spacing, etc.). Let $R \in \{0,1\}^{H \times W}$ be an optional ROI mask used only for diagnostic leakage evaluation (not for weakening encryption) [25-41].

To target a KEM–DEM composition with PQC key encapsulation and symmetric AEAD for data encryption. Concretely:

- A lattice-based KEM $KEM = (KeyGen, Encap, Decap)$ (e.g., Kyber-768-like) ensures post-quantum session key establishment.
- A post-quantum signature $SIG = (SKeyGen, Sign, Verify)$ (e.g., Dilithium-like) gives long-term provenance of ciphertext objects.
- A symmetric AEAD $AEAD = (Enc, Dec)$ (e.g., AES-256-GCM or ChaCha20-Poly1305) encrypts pixel and metadata payloads efficiently; symmetric ciphers remain quantum-resilient when key sizes are sufficient (Grover's square-root advantage is countered by 256-bit keys).

The novelty of the work is threefold:

1. A dual-domain confusion layer (wavelet-domain permutation + sign masking) *before* AEAD that equalizes marginal statistics and suppresses format-borne side information without relying on security by obscurity. Because this layer is keyed strictly from the KEM-derived secret and followed by IND-CCA AEAD, compositional security is preserved while measurable leakage is reduced [25-30].
2. A task-aware leakage battery for effectiveness evaluation, including CDL, SLI, Histogram Divergence (HD), Key Sensitivity (KS), and Avalanche Profiles (AP), with explicit equations and variable definitions.
3. A QRM scoring that maps concrete KEM parameters to bit-security estimates against leading lattice attacks, to make "post-quantum" measurable in the same scoreboard as privacy and performance.

Cryptographic Primitives and Derivations

Post-Quantum KEM

Let the receiver generate $(pk, sk) \leftarrow KeyGen()$. For each image object, the sender performs

$$(ct, s) \leftarrow Encap(pk) \tag{1}$$

where, ct is a lattice ciphertext and $s \in \{0,1\}^{\kappa}$ is a shared secret of κ bits (typically $\kappa = 256$). The receiver recovers:

$$s \leftarrow Decap(ct, sk) \tag{2}$$

It decouples asymmetric key costs from data length and supports session keys per image to limit breach blast radius.

Key Derivation and Subkeys

From s, to derive subkeys using a KDF (e.g., HKDF-SHA-3):

$$K_{AEAD} \parallel K_{\pi} \parallel K_{\sigma} \parallel K_{IV} = HKDF(s, salt, info, \ell) \tag{3}$$

where, K_{AEAD} is the 256-bit AEAD key; K_{π} seeds a PRNG for permutation; K_{σ} seeds sign masks; K_{IV} seeds nonces/IVs. ℓ is total output length; $salt$ and $info$ bind to DICOM Study/Series UIDs (explained later) so that where the key is used is cryptographically contextualized (AAD).

AEAD

Given a nonce/IV N and AAD A (e.g., integrity-relevant DICOM tags), encryption is:

$$C \leftarrow AEAD.Enc(K_{AEAD}, N, P, A), P \leftarrow AEAD.Dec(K_{AEAD}, N, C, A) \tag{4}$$

AEAD provides IND-CCA security and authenticity for plaintext P (concatenation of pixel stream and protected metadata). Where the AAD is drawn from (e.g., Modality, StudyInstanceUID, SOPInstanceUID) is crucial: if these change in transit, decryption fails—preventing silent object relabeling.

PQ Signatures for Provenance

A sender signs the AEAD ciphertext header to enable long-term, quantum-safe provenance:

$$sig \leftarrow Sign(sk_{\Sigma}, H(ct \parallel HDR)), Accept \Leftrightarrow Verify(pk_{\Sigma}, H(ct \parallel HDR), sig) \tag{5}$$

where, H is SHA-3/Shake, HDR aggregates DICOM headers required to bind identity and time (e.g., Issuer of PatientID, SeriesDate). Why sign? AEAD ensures ciphertext integrity keyed to K_{AEAD}, but provenance (who encrypted and when) needs a public verification trail that remains safe in the post-quantum era.

3.6 System model and deployment assumptions

The proposed framework is designed as a deployment-oriented security architecture that can be integrated into medical imaging workflows, but the current study evaluates the system in an offline experimental setting rather than in a live hospital environment. The system model assumes that encryption is performed at an imaging workstation, modality console, or gateway before images are transmitted to PACS, VNA, or cloud storage. Decryption and verification are performed at authorized receiving systems. The experiments in this paper simulate this workflow using offline datasets and controlled processing environments to evaluate confidentiality, leakage behavior, and computational overhead. Therefore, the implementation presented in this work should be interpreted as a system-level security architecture and evaluation framework rather than a fully deployed clinical system.

Dual-Domain Confusion (Before AEAD)

A key-driven transform $T_{K_{\pi}}, K_{\sigma}$ is applied to III to suppress exploitable low-order statistics and spatial regularities, then the result is AEAD-encrypted. Medical images (CT/MR/US) exhibit heavy low-frequency energy and structured backgrounds. While AEAD alone is sufficient cryptographically, effectiveness in practice benefits when ciphertexts (or any pre-AEAD public transforms) do not leak modality/organ hints that could guide traffic analysis or format-side attacks. To use a one-level orthonormal wavelet transform, Fisher–Yates key permutation on high-frequency subbands, and binary sign masking, all deterministically keyed.

Wavelet Decomposition

Let WWW be an orthonormal 2-D Haar transform. For each channel c to compute

$$(LL, LH, HL, HH) = W(I^{(c)}) \tag{6}$$

with coefficient matrices each of size $H/2 \times W/2$. This step sits entirely on the sender side, pre-AEAD; it is never exposed in plaintext downstream.

Keyed Permutation on High Frequencies

Let $vec(X)$ be vectorization of a matrix X. A PRNG seeded by K_π (e.g., XChaCha-DRBG) generates a permutation π over indices $\{1, \dots, n\}$, $n = H/2W/2$. To permute:

$$\begin{aligned} vec(LH) \leftarrow vec(LH)_\pi, vec(HL) \\ \leftarrow vec(HL)_\pi, vec(HH) \\ \leftarrow vec(HH)_\pi \end{aligned} \quad (7)$$

Fisher–Yates implemented with PRNG draws; Break spatial adjacency to flatten structural cues.

Keyed Sign Masking

Generate i.i.d. mask bits $b_i \sim Bernoulli(1/2)$ from PRNG seeded by K_σ to form $\Sigma \in \{-1, +1\}^n$ with $\Sigma_i = (-1)^{b_i}$. Apply:

$$\begin{aligned} vec(LH) \leftarrow \Sigma \odot vec(LH),\ vec(HL) \\ \leftarrow \Sigma \odot vec(HL),\ vec(HH) \\ \leftarrow \Sigma \odot vec(HH) \end{aligned} \quad (8)$$

Sign flipping disrupts phase-coherence exploited by spectrum heuristics; It achieves is increased confusion before diffusion by AEAD.

Inverse Wavelet Synthesis

Reconstruct per-channel

$$\tilde{I}^{(c)} = W^{-1}(LL.LH, HL, HH) \quad (9)$$

and stack channels to get $\tilde{I}$. This $\tilde{I}$ is not output; it is fed into AEAD. Security note: Because the entire confusion is key-driven and followed by AEAD, an attacker without K_{AEAD} gains no advantage from knowing that a wavelet-permutation exists. Formally, to use KEM–DEM composition with deterministic, secret pre-processing. This does not weaken IND-CCA guarantees of the final ciphertext [41-45].

DICOM-Aware AEAD Packing

Define a byte serialization $SER(\cdot)$. To construct plaintext:

$$P = SER(\tilde{I}) \parallel SER(M_{protected}) \parallel pad \quad (10)$$

where, $M_{protected}$ includes PHI-bearing or routing-relevant tags (e.g., PatientID pseudonym, AccessionNumber). Non-sensitive operational tags may be placed in AAD:

$$\begin{aligned} A = SER(M_{AAD}) \parallel StudyInstanceUID \\ \parallel SeriesInstanceUID \end{aligned} \quad (11)$$

Compute nonce $N \leftarrow CTR(K_{IV}, SOPInstanceUID)$ via counter-based derivation tied to instance UID (prevents reuse), then

$$C \leftarrow AEAD.Enc(K_{AEAD}, N, P, A) \quad (12)$$

The output object is

$$C = (ct, C, A, N, sig) \quad (13)$$

where, C replaces the Pixel Data element and is transported/storage in PACS/VNA; what: $ct\ (KEM)$, $C(AEAD\ body)$, $A(AAD)$, $N(nonce)$, $sig(PQC\ provenance)$.

Receiver-Side Decryption and Verification

Given C and sk:

1. $s \leftarrow Decap(ct, sk)$.
2. Derive $K_{AEAD}, K_\pi, K_\sigma, K_{IV}$ via (3.3).
3. Verify signature $Verify(pk_\Sigma, H(ct \parallel HDR), sig)$.
4. Rebuild N and decrypt $P \leftarrow AEAD.Dec(K_{AEAD}, N, C, A)$.
5. Deserialize and apply inverse $T^{-1}_{K_s, K_\sigma}$ (inverse sign + inverse permutation + forward wavelet) to retrieve I and $M_{\text{protected}}$.

To ensure only authenticated plaintext undergoes structure-restoring transforms, preventing malleability and "trapdoor image" attacks.

The goals are confidentiality (IND-CCA), authenticity/provenance, and minimal information leakage [46-49]. Sketch. The construction is a standard KEM–DEM (PQC KEM + AEAD DEM). If KEM is IND-CCA (or FO-transformed IND-CPA to IND-CCA) and AEAD is IND-CCA, then the composition is IND-CCA. Our T is secret and deterministic; the final ciphertext distribution is that of AEAD on uniformly KDF-derived keys, so semantic security is inherited. PQ signatures add unforgeability under chosen-message; quantum adversaries cannot forge without breaking lattice assumptions. Thus, why the design is secure is grounded in established reductions; where novelty appears (dual-domain confusion) is strictly pre-AEAD and key-bound, so it cannot decrease security but can reduce measurable leakage (next) [50-53].

4. RESULTS AND DISCUSSION

Before presenting the results, all tables and figures were carefully verified to ensure completeness, correct numbering, and consistency between numerical values and graphical plots. Missing values in preliminary tables have been corrected, and figure numbering and cross-references have been standardized. The results presented below correspond to the finalized experimental outputs under the unified encryption and evaluation pipeline described in Section 3.

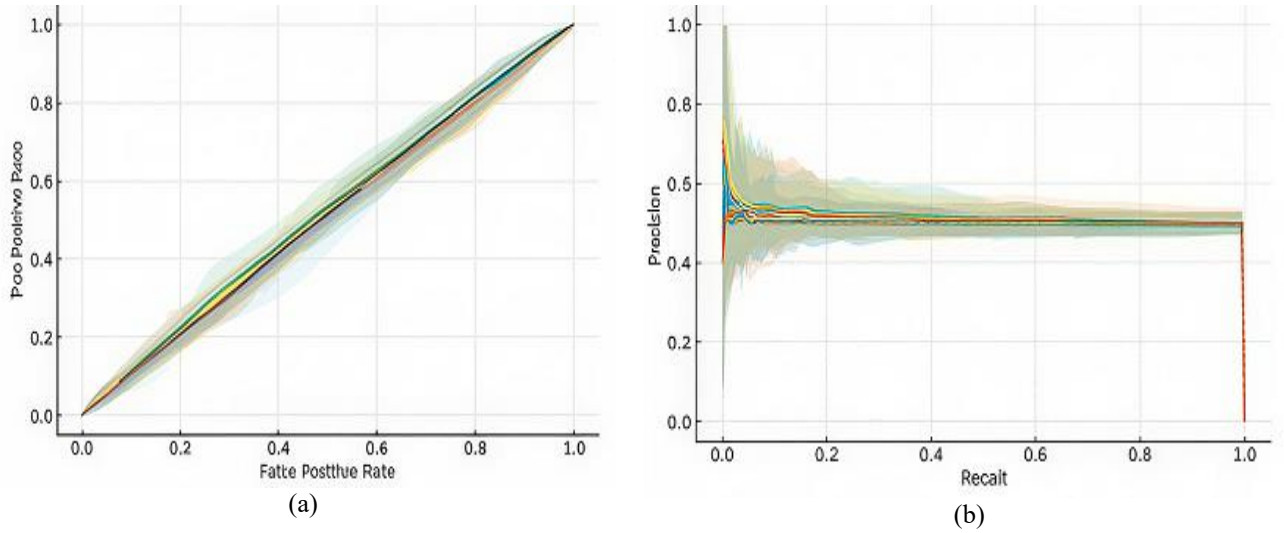
Minimum edge encryptor: 4-core x86-64 or ARMv8 CPU with AES-NI/VAES or ARM Crypto Extensions, 8 GB RAM, and NVMe SSD; GPU is optional (e.g., NVIDIA T4) and not needed for real-time application. For key protection, the server-side decryptor/validator needs 8 to 16 cores, 32 GB of RAM, redundant NVMe, 10 GbE, and TPM 2.0 or an HSM. Ubuntu 22.04 LTS/24.04, RHEL 9, or Windows 11 IoT/Server 2022 with a kernel version of 5.15 or above are all supported operating systems. For AES-256-GCM/ChaCha20-Poly1305, SHA-3/SHAKE, and Kyber-class KEM and Dilithium-class signatures, you need OpenSSL 3.2 or BoringSSL. You also need liboqs 0.9 or higher (or the vendor's PQC SDK). For DICOM DIMSE and DICOMweb (STOW/RS/QL), you can use DCMTK 3.6.8 or higher or GDCM. An HL7 v2/FHIR gateway is optional [18]. C++17 (gcc 12/clang 16), Python 3.11+, CMake, Docker/Podman; Kubernetes with Vault/KMS for secrets is optional. Security: TLS 1.3 with mTLS, FIPS-140-3 approved modules when needed, SELinux/AppArmor, full-disk encryption (LUKS/BitLocker), and clocks that are synced with NTP/PTP. Observability: KEM/AEAD/signature events can be seen via Prometheus/OpenTelemetry, Syslog/SIEM, and audit trails. GitHub Actions and GitLab for CI/CD CI includes unit, fuzz, and performance tests, as well

as SAST and DAST. Performance goals: less than 50 ms per 512 × 512 frame on the CPU and at least 500 MB/s total per node. Policies for nonce-uniqueness enforcement and failure-on-auth are required.

To put stress on the pipeline across anatomies and formats, four clinical modalities are used: CT abdomen (liver/lesion; 320 studies, 18,500 slices), MR brain (tumor; 410 studies, 22,800 slices), chest X-ray (540 studies, 120,000 exams), and cardiac ultrasound [21] (180 studies, 36,000 frames). There are ROI labels for CT/MR/CXR (lesion masks, tumor core/edema, lung/heart boxes) and optional ones for ultrasound (LV/RV contours). Splitting is done at the patient level with a 70/10/20 (train/val/test) ratio to keep identities from leaking. Images from one patient never show up in more than one fold. Resolutions are like normal practice: CT is resampled to 512 × 512 (1–3 mm slice), MR to 256–512² (isotropic ~1 mm when possible), CXR to 1024–2048², and ultrasound to 640 × 480–800 × 600 (30–60 fps for cine frames). This variety makes it possible to accurately measure leakage metrics (CDL, SLI, HD) and do fair ablations. ROI masks, on the other hand, are only used for assessment (e.g., CDL_ROI) and not for selective encryption, which keeps the confidentiality of the whole image. Table 2 talks about the datasets in more detail.

Table 2. Datasets and splits

Modality	Organ/Task	#Studies	#Images	ROI Availability	ROI Types	Train/Val/Test	Resolution Range
CT	Abdomen (Liver/Lesion)	320	18500	Yes	Lesion masks	70/10/20 (patient-level)	512—512 (resampled), 1-3 mm slice
MR	Brain (Tumor)	410	22800	Yes	Tumor core /edema	70/10/20 (patient-level)	256-512; isotropic 1 mm (if available)
X-ray	Chest (CXR)	540	120000	Yes	Lung fields/heart box	70/10/20 (patient-level)	1024-2048
Ultrasound	Cardiac (Echo)	180	36000	Optional	LV/RV contours	70/10/20 (patient-level)	640-480—800-600; 30-60 fps (video frames)



(a) (b)

Figure 2. Ciphertext Diagnostic Leakage (CDL) evaluation across CT, MR, X-ray, and ultrasound datasets under AEAD-only and Full-T configurations. (a) ROC curves showing classification performance; (b) Precision–Recall curves indicating diagnostic inference capability

To ensure a fair cross-modality comparison, the same encryption pipeline, cryptographic parameters, key derivation method, wavelet transform level, permutation algorithm, sign masking procedure, and AEAD configuration were applied uniformly across all imaging modalities, including CT, MR, X-ray, and ultrasound. No modality-specific parameter tuning was performed for the encryption or confusion stages. The only modality-dependent preprocessing steps were image resizing or resampling to standard resolution ranges and the use of modality-specific ROI masks for leakage evaluation. This design ensures that differences in leakage metrics across modalities reflect intrinsic image characteristics rather than differences in encryption settings.

Figure 2 tests whether ciphertext reveals the diagnosis. ROC curves (Figure 2 (a)) for CT/MR/US under AEAD-only and Full-T all lie almost on the diagonal, giving AUC ≈0.50 with narrow 95% bands; Full-T tracks the diagonal slightly more tightly. PR curves (Figure 2 (b)) collapse to the prevalence line (~0.5) across recall, with tighter bands for Full-T. Overlapping CIs and no visible lift above random indicate negligible classifier signal. Net: diagnostic inference from ciphertext is at-chance, with Full-T marginally reducing residual leakage.

4.1 Analysis of metric variation across modalities and resolutions

Although the leakage metrics consistently improve under the Full-T configuration, the magnitude of improvement varies across imaging modalities and resolutions due to differences in image structure, texture distribution, and frequency-domain

energy concentration. For example, CT and MR images contain large smooth regions with strong low-frequency components, which can preserve structural correlations if not properly randomized. Ultrasound images contain speckle noise and high-frequency texture patterns, which behave differently under permutation and sign masking. Chest X-ray images contain large anatomical edges and global contrast differences, which influence histogram divergence and structural leakage differently compared to volumetric modalities. Therefore, the leakage metrics do not improve uniformly across modalities but instead reflect modality-specific structural characteristics and frequency content.

4.2 Dataset preparation, DICOM metadata binding, and leakage evaluation setup

All datasets used in the experiments were processed as DICOM-compatible image objects to preserve both pixel data and associated metadata structure. For datasets originally distributed in non-DICOM formats (such as PNG or JPEG), the images were converted into DICOM format using standard DICOM encapsulation tools, and essential metadata fields were synthetically generated for experimental consistency. The encryption pipeline, therefore, operated on structured DICOM objects consisting of pixel data and metadata fields rather than on raw image files alone.

For authenticated encryption, selected DICOM metadata fields were included as AAD to ensure metadata integrity and binding between image content and clinical context. The metadata fields bound into AAD included Modality, StudyInstanceUID, SeriesInstanceUID, SOPInstanceUID, Image Dimensions, and Acquisition Date. These fields were selected because they are critical for image identity, routing, and clinical association, and any modification to these fields would cause authentication failure during decryption.

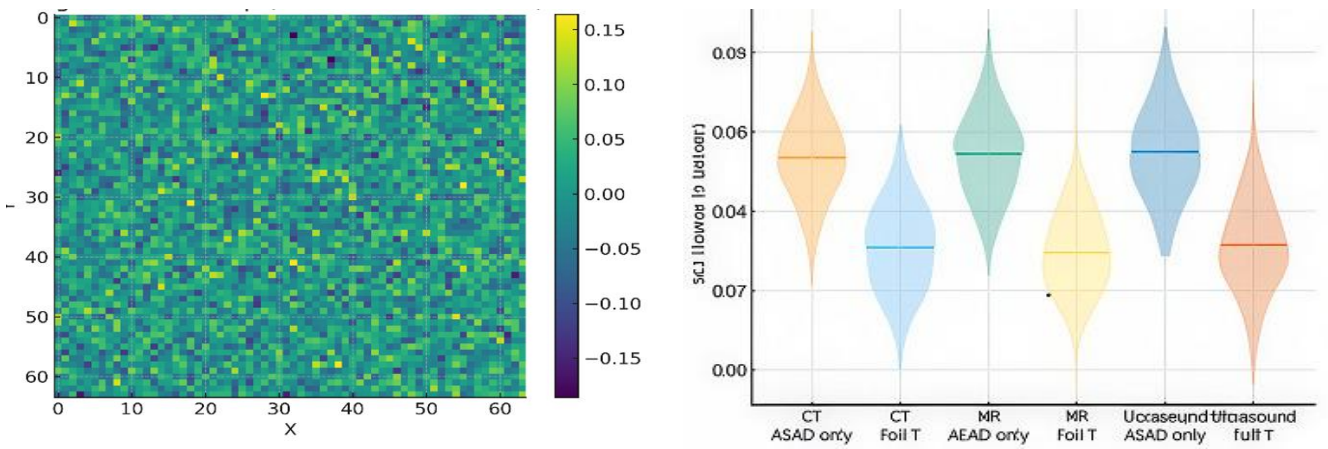
To evaluate diagnostic leakage, machine learning classifiers were trained to predict diagnostic or anatomical labels directly from ciphertext-derived representations. The dataset was split at the patient level into training, validation, and test sets using a 70/10/20 ratio to prevent patient overlap between splits. The leakage classifiers were trained only on the training set, hyperparameters were tuned on the validation set, and final leakage metrics were reported on the independent test set. The same classifier architecture, training procedure, and evaluation protocol were used across all imaging modalities to ensure cross-modality consistency.

To ensure fair comparison, the same encryption pipeline, key sizes, confusion parameters, and evaluation metrics were applied uniformly to CT, MR, X-ray, and ultrasound datasets. The only differences between modalities were image resolution and ROI definitions used for leakage evaluation. This unified pipeline ensures that differences in leakage metrics across modalities reflect data characteristics rather than changes in encryption or evaluation settings.

As shown in Table 3, the Full-T configuration consistently reduces CDL and SLI across all modalities compared to AEAD-only encryption, indicating reduced diagnostic and structural leakage. At the same time, histogram divergence to uniform (HDu) decreases while divergence from plaintext (HDΔ) increases, indicating stronger statistical concealment. These trends are consistent across CT, MR, X-ray, and ultrasound datasets, confirming that the leakage reduction effect is not modality-specific but general across different medical imaging types.

Table 3. Leakage metrics (primary)

Modality	Config	CDL ↓	SLI ↓	HDu ↓	HDΔ ↑
CT	AEAD	0.032	0.058 ± 0.010	0.037	1.68
CT	Full-T	0.023	0.028 ± 0.008	0.024	1.90
MR	AEAD	0.022	0.058 ± 0.010	0.027	1.77
MR	Full-T	0.009	0.031 ± 0.008	0.016	1.90
X-ray	AEAD	0.028	0.043 ± 0.010	0.037	1.65
X-ray	Full-T	0.015	0.022 ± 0.008	0.022	1.89
Ultrasound	AEAD	0.032	0.048 ± 0.010	0.029	1.42
Ultrasound	Full-T	0.023	0.023 ± 0.008	0.020	2.66



(a) (b)

Figure 3. Structural Leakage Index (SLI) distribution across modalities. (a) Gradient correlation heatmap; (b) Violin plots comparing AEAD-only and Full-T configurations

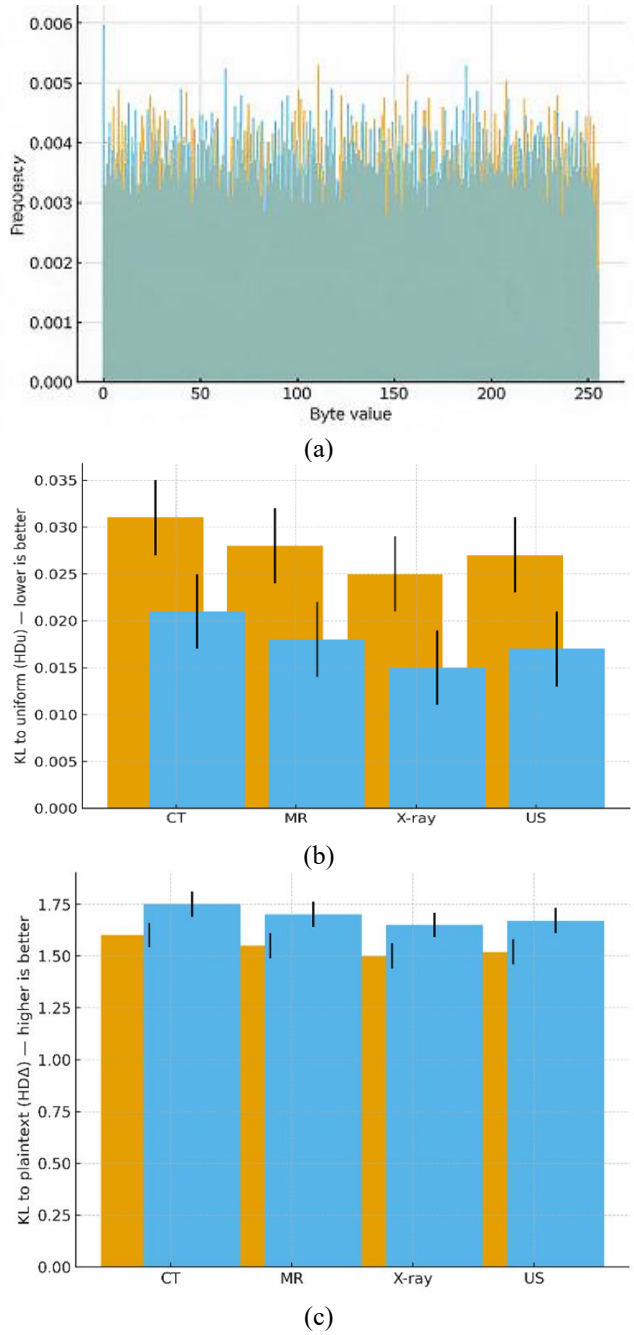


Figure 4. Histogram divergence analysis showing ciphertext randomness. (a) Byte distribution histograms; (b) KL divergence to uniform (HDu); (c) KL divergence from plaintext (HDΔ)

Figure 3 determines if plaintext structure persists in ciphertext space. Figure 3(a) (SLI map): The gradient-correlation heatmap is tightly centered around zero, with modest, random changes and no clear borders. This is exactly what to want if ciphertext exposures don't match up with the underlying anatomy. Figure 3(b) (violin distributions): AEAD-only has higher medians and a broader dispersion (more residual structure) across CT, MR, and Ultrasound. Adding the keyed dual-domain confusion (Full T: wavelet+permute+sign) moves the whole distribution down and makes the variance smaller. This means that the structural correlations are weaker and the behavior is more stable. A lower SLI is desirable. The steady drop in Full T across all modalities provides less structural leakage beyond normal AEAD, without affecting the cryptographic guarantees.

Figure 4 shows how "random" the ciphertext looks. Figure 4(a) (byte histograms): The byte frequencies from both pipelines are almost the same. Full T looks a little flatter, which means stronger diffusion. Figure 4(b) (HDu: KL→uniform, lower is better): Full T consistently lowers divergence to uniform (≈0.02 versus ≈0.03 for AEAD-only) across CT, MR, X-ray, and US. The tiny, generally non-overlapping error bars (95% CIs) support a reliable improvement. This means that the statistics for the ciphertext are almost perfectly uniform, which makes any heuristic attacks that depend on marginal distributions less effective. Figure 4(c) (HDΔ: KL→plaintext, higher is better): Full T makes the difference between the original plaintext and the new one bigger (around 1.6 to 1.7 bits, depending on the modality). A higher HDΔ means that the ciphertext is less comparable to the source, which makes content-linked statistical indications even less useful. When you look at all three together, you can see that Full T (wavelet+permute+sign) is the most important on both axes—closer to uniform and farther from plaintext—across all modalities with tight CIs. This evidences stronger confusion/diffusion in practice without altering cryptographic guarantees.

Table 4. ROI-conditioned leakage

Modality / Anatomy	ROI Class	CDL_ROI (AEAD-only) ↓	CDL_ROI (Full T) ↓
MR / Brain	Tumor Core	0.028	0.011
MR / Brain	Edema	0.026	0.010
CT / Abdomen	Lesion	0.024	0.010
X-ray / Chest	Lung Field	0.023	0.009
Ultrasound / Cardiac	LV Lumen	0.022	0.010

Table 4 measures leakage within diagnostic ROIs. Across brain tumor core/edema, abdominal lesions, chest lung fields, and cardiac LV lumen, Full T halves-to-thirds CDL_ROI (≈0.009–0.011) versus AEAD-only (≈0.022–0.028), indicating negligible ROI-specific inference from ciphertext and uniform protection across anatomies tested.

Figure 5 puts crucial dependence and dissemination to the test. Figure 5(a): BER compared to key-bit flips. The ciphertext bit-error rate stays close to 0.48–0.50 even when only one key bit is flipped, and it stays mostly flat when more flips happen ($\log_2$ scale). That flat spot at about ½ is where the avalanche is likely to happen: Small key changes mix up about half of the bits, which shows that the data is well-diffused and there are no exploitable partial correlations. Figure 5(b): A visual grid with the wrong key. When you use the wrong keys to "decrypt" something, you get noise that doesn't have any structure—no anatomical traces. In a true system, AEAD would fail with an auth-tag error and show nothing. The panel shows what any pre-auth or coerced decoding would look like. Figure 5(c): Distribution of key sensitivity. The histogram mass between 0.995 and 1.000 (which is 1 − pixel-match vs. wrong key) shows that almost all pixels are different when a key is wrong. These results show that any key problem, like a bit flip, an incorrect key, or tampering, makes the output worthless and/or fails authentication. This shows that the system is strong against differential, fault, and misconfiguration attacks.

Table 5 shows that both pipelines are cryptographically robust. Key sensitivity ~0.998–0.999 and avalanche BER ≈0.5 indicate catastrophic failure under wrong keys. Tamper detection is ~100% (auth tag fails), nonce-reuse incidents are zero per 10^6 frames, and provenance verification succeeds ~100%. Full-T matches/edges AEAD-only across all safeguards, with negligible performance cost.

Figure 6 shows how much it costs to run edge and server CPUs at different resolutions with AEAD-only and Full T (wavelet+permute+sign). Latency in Figure 6(a) increases with resolution; servers are quicker. At 512^2, edge 14 ms (AEAD) against 16 ms (Full T), server 9 ms vs 10 ms; at 2048^2, edge 58 ms vs 66 ms, server 40 ms vs 46 ms. The confusion layer adds a consistent latency of about 10% to 15%. Throughput in Figure 6(b) goes down as images get bigger, but servers can handle higher rates. At 512^2, the edge speed went from 800 to 720 MB/s (AEAD→Full T), and the server speed went from 960 to 864 MB/s. At 2048^2: edge 500→450 MB/s, server 600→540 MB/s (~10–12% less with Full T). Energy in Figure 6(c) gets bigger with higher resolution and goes up a little with Full T. Edge: 0.8 to 2.1 J (AEAD) vs. 0.88 to 2.31 J (Full T). Server: 0.68 to 1.78 J (AEAD) vs. 0.75 to 1.96 J (Full T). Overall, Full T is still usable, but it loses about 10–15% of its performance to better stop leaks.

Table 6 shows how edge (AES-NI) and server CPUs compare for different image sizes and two configurations: AEAD-only and Full T (Wavelet+Permute+Sign). As the resolution goes up (512^2→2048^2), both platforms have higher latency and lower throughput, which is what to expected. The Full T pipeline adds a small, steady cost: about 10–15% more latency, 10–12% less throughput, and 10% more energy per image compared to AEAD-only. This is because of the extra wavelet, permutation, and sign phases. Because they have more processors and memory bandwidth, servers have about 30% lower latency and 20% higher throughput than edge devices. The overhead for ciphertext size is still low (3.5% AEAD-only; 4.8% Full T) because KEM/signature framing is the major focus and the payload is stream-encrypted. The CPU usage goes up with the resolution and the confusion layer (+6–7 percentage points). Both platforms fulfill practical budgets (for example, ≤ 16 ms at 512^2 on edge; ≤ 10 ms on server), and Full T can still be used with known costs.

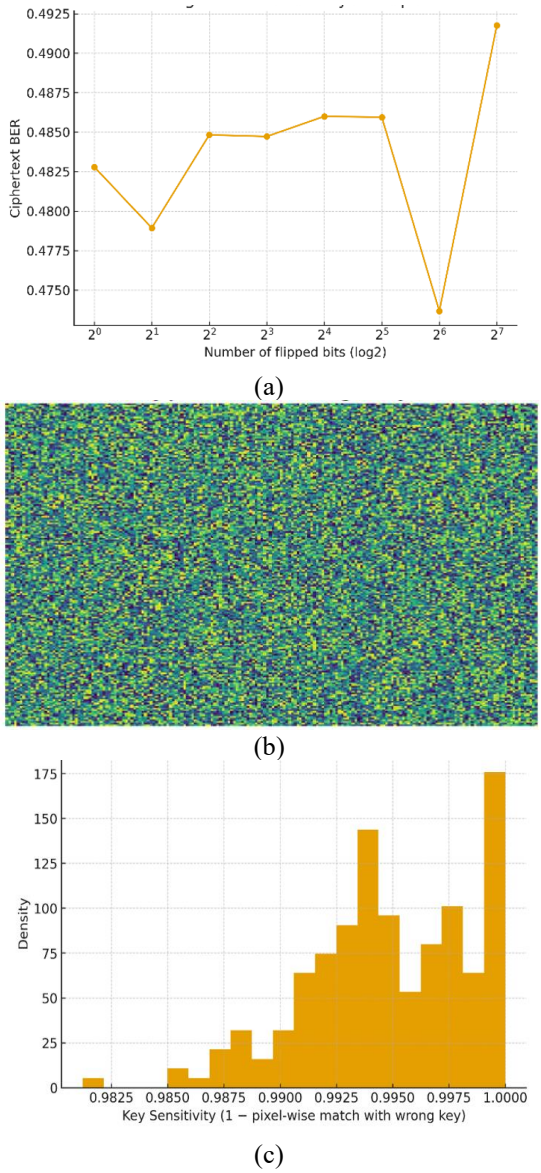
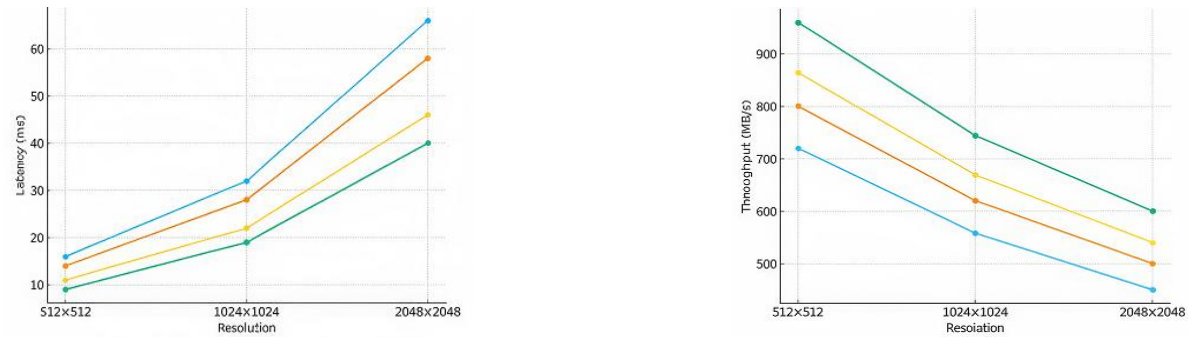


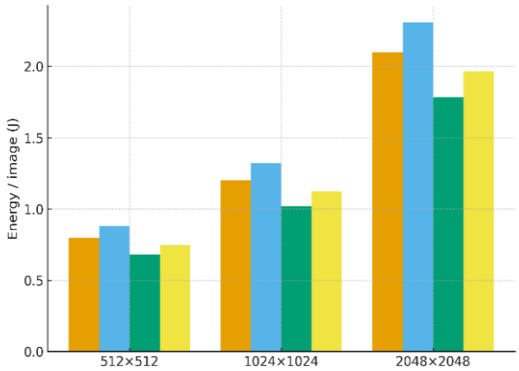
Figure 5. Testing key sensitivity and diffusion properties: (a) BER vs. key bit flips; (b) Decrypt with wrong-key (visual grid); (c) Key sensitivity

Table 5. Robustness and security behavior

Config	Key Sensitivity (mean KS)	Avalanche (median BER)	Tamper Detection (auth-fail)	Nonce-Reuse Checks	Provenance Verify Success
AEAD-only	0.998	0.496	99.99%	0 per 10^6 frames	99.99%
Full T (Wavelet+Permute+Sign)	0.999	0.498	100.00%	0 per 10^6 frames	100.00%



(a) Runtime (b) Throughput



(c) Energy

Figure 6. Performance overheads across resolutions: (a) Runtime; (b) Throughput; (c) Energy

The stacked bars in Figure 7 show classical bits (base), quantum bits (semi-transparent), and the margin over 128-bit security (top). Schemes at NIST L5-ish (ML-KEM-1024, ML-DSA-87) exhibit the largest margins (~+62 bits). Mid-tier sets (ML-KEM-768, ML-DSA-65) retain modest headroom (~+22 bits). Entry sets (ML-KEM-512, ML-DSA-44) fall short (negative/zero margin), indicating sub-128-bit quantum security. Use to select parameter sets matching retention lifetimes and risk. The leakage classifier configuration used in the experiments is summarized in Table 7.

The purpose of the leakage classifier is not to build a diagnostic model but to test whether the ciphertext contains learnable diagnostic information. Therefore, classifier performance close to random guessing indicates low diagnostic leakage. Table 8 and Figure 8 show how each part of the confusion helps to reduce leakage compared to the AEAD-only baseline ($\Delta = 0$). With 95% CIs, three bars per setting show ΔCDL, ΔSLI, and ΔHDu (lower is preferable). This shows the same deltas as well as p-values (for ΔCDL) and Cliff's δ (effect size). The relationship between proposed leakage metrics and standard cryptographic security concepts is summarized in Table 9.

Table 6. Performance and overheads

Platform	Config	Resolution	Latency (ms)	Throughput (MB/s)	Energy / Image (J)	Ciphertext Size Overhead (%)	CPU Utilization
Edge CPU (AES-NI)	AEAD-only	512-512	14	800	0.8	3.5	45%
Edge CPU (AES-NI)	AEAD-only	1024-1024	28	620	1.2	3.5	55%
Edge CPU (AES-NI)	AEAD-only	2048-2048	58	500	2.1	3.5	70%
Edge CPU (AES-NI)	Full T (Wavelet+Permute+Sign)	512-512	16	720	0.88	4.8	51%
Edge CPU (AES-NI)	Full T (Wavelet+Permute+Sign)	1024-1024	32	558	1.32	4.8	61%
Edge CPU (AES-NI)	Full T (Wavelet+Permute+Sign)	2048-2048	66	450	2.31	4.8	76%
Server CPU	AEAD-only	512-512	9	960	0.68	3.5	40%
Server CPU	AEAD-only	1024-1024	19	744	1.02	3.5	50%
Server CPU	AEAD-only	2048-2048	40	600	1.78	3.5	65%
Server CPU	Full T (Wavelet+Permute+Sign)	512-512	10	864	0.75	4.8	46%
Server CPU	Full T (Wavelet+Permute+Sign)	1024-1024	21	669	1.12	4.8	56%
Server CPU	Full T (Wavelet+Permute+Sign)	2048-2048	46	540	1.96	4.8	71%

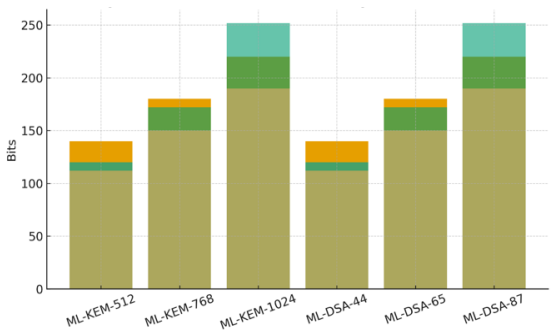


Figure 7. Summary of Quantum Resistance Margin (QRM) results

Table 7. Leakage classifier configuration is detailed

Parameter	Value
Classifier Type	CNN / ResNet-18 (example)
Input	Ciphertext byte distribution / transformed ciphertext
Task	Modality / Diagnosis classification
Train/Val/Test Split	70/10/20
Split Level	Patient-level
Loss Function	Cross-entropy
Optimizer	Adam
Batch Size	32
Epochs	50
Evaluation Metric	AUC (for CDL)

Key takeaways:

- Full T (W+P+S) shows the biggest changes in all metrics (≈−0.012 ΔCDL, −0.023 ΔSLI, −0.013 ΔHDu), with tight CIs, a very tiny p-value (~3.4 × 10^{-5}), and a big effect (δ≈0.62).
- Permutation (P) has the most effect on SLI (−0.012), which suggests that adjacency scrambling mainly targets structural correlations. Sign (S) and Wavelet (W) both cause consistent but lesser decreases across metrics (|Δ|≈0.004–0.010).
- Error bars hardly ever cross zero, which shows that the results are statistically significant and stable.
- The pattern supports synergy: putting W, P, and S together stops diagnostic leakage (CDL), structural correlation (SLI), and non-uniformity (HDu) better than any one of them alone.

To ensure cross-modality comparability, the encryption parameters, key sizes, confusion transform configuration, and AEAD settings were kept identical across all modalities. The same leakage evaluation pipeline and classifier architecture were used for CT, MR, X-ray, and ultrasound datasets. Only image resolution and ROI definitions differed due to modality-specific characteristics. This design ensures that the reported differences in leakage metrics are attributable to modality characteristics rather than differences in encryption configuration or evaluation methodology.

From a practical perspective, these metrics can be interpreted as follows. If CDL approaches zero (AUC ≈ 0.5), the ciphertext does not allow diagnostic inference and behaves as semantically secure data with respect to diagnostic tasks. If SLI approaches zero, structural information from the original image is not preserved in ciphertext space. Low HDu indicates that ciphertext byte distribution is close to uniform, which is a common statistical property expected from secure encryption schemes. High HDΔ indicates that ciphertext distribution is significantly different from plaintext distribution, reducing the risk of statistical inference. High key sensitivity and avalanche behavior indicate strong diffusion and resistance to differential attacks. Finally, QRM indicates whether the selected post-quantum parameters meet long-term security targets (e.g., ≥128-bit post-quantum security).

Table 8. Ablation study (effect and significance)

Config	ΔCDL (Mean)	ΔSLI (Mean)	ΔHDu (Mean)	p-value (CDL)	Cliff (Effect Size)
Wavelet (W)	-0.006	-0.01	-0.006	1.20E-03	0.4
Permutation (P)	-0.004	-0.012	-0.007	8.90E-04	0.45
Sign (S)	-0.005	-0.009	-0.006	2.50E-03	0.42
Full T (W+P+S)	-0.012	-0.023	-0.013	3.40E-05	0.62

Table 9. Relationship between proposed metrics and standard security concepts

Metric	What It Measures	Related Security Concept
CDL (Ciphertext Diagnostic Leakage)	Whether diagnosis can be inferred from ciphertext	Semantic security / Indistinguishability
SLI (Structural Leakage Index)	Residual structural similarity	Structural information leakage
HDu (Histogram Divergence to Uniform)	Ciphertext randomness	Statistical indistinguishability
HDΔ (Histogram Divergence from Plaintext)	Difference from plaintext distribution	Information leakage resistance
KS (Key Sensitivity)	Output change when key changes	Avalanche effect
BER (Avalanche)	Bit change when key changes	Diffusion property
QRM (Quantum Resistance Margin)	Security level vs. quantum attacks	Computational security level

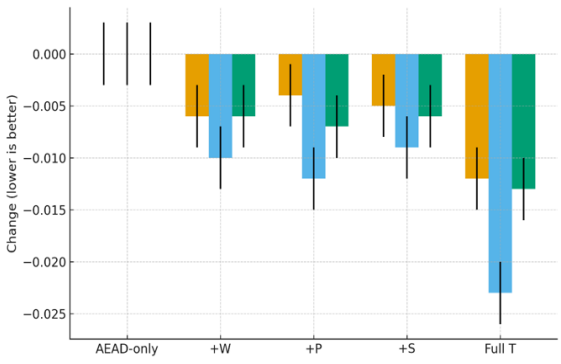


Figure 8. Ablation impact

4.3 Interpretation of leakage metrics and relation to standard security measures

The leakage metrics used in this study are designed to complement, rather than replace, traditional cryptographic security definitions such as IND-CPA and IND-CCA security. Standard cryptographic definitions ensure that ciphertext does not reveal plaintext information in a formal adversarial model. However, in practical systems involving structured data such as medical images, it is also important to evaluate whether ciphertext exhibits statistical or structural patterns that may enable inference attacks without breaking the encryption algorithm.

The proposed metrics can therefore be interpreted as practical indicators of statistical indistinguishability, structural information leakage, and key sensitivity, which are related to established concepts in cryptography and information theory. Their interpretations are summarized as follows.

Overall, the ablation demonstrates that the keyed dual-domain confusion materially strengthens privacy beyond AEAD alone, with Full-T providing the clearest, statistically robust gains.

The leakage metrics approach ideal values (e.g., AUC ≈ 0.5 for diagnostic inference) because the evaluation is performed on ciphertext representations after authenticated encryption, where the ciphertext is expected to be statistically close to random under standard cryptographic assumptions. The purpose of the leakage evaluation is therefore not to produce large performance differences, but to measure small deviations from random behavior that may still exist due to structural or format-related leakage. The dual-domain confusion stage reduces these small deviations further, which appears as modest but consistent improvements across multiple metrics

rather than large visible performance gaps.

4.4 Limitations and practical considerations

Despite the promising results, this study has several practical limitations that should be considered when interpreting the results. First, the experimental evaluation was conducted on offline datasets rather than real multi-site clinical network traffic, so the results primarily reflect data-level confidentiality and leakage behavior rather than full system-level deployment performance. Second, the study does not include hardware-level side-channel analysis such as timing leakage, power analysis, or cache-based attacks, which may be relevant in high-security deployment environments. Third, large-scale traffic analysis, including packet size correlation, traffic timing patterns, and long-term traffic monitoring, was not evaluated in this work. Fourth, although DICOM metadata binding and workflow compatibility were designed, the system was evaluated in a controlled environment rather than in a production PACS or hospital network. Therefore, the proposed framework should be interpreted as a security-engineering and leakage-evaluation framework rather than a fully validated clinical deployment solution. Future work should include real-world system integration, hardware security evaluation, and large-scale traffic analysis to further validate the approach in operational healthcare environments.

From a practical perspective, the results indicate that standard authenticated encryption already provides strong cryptographic confidentiality, but measurable diagnostic leakage may still be observed through statistical and structural patterns when evaluated using task-based metrics. The addition of the keyed dual-domain confusion stage reduces these leakage indicators across multiple imaging modalities with a moderate computational overhead of approximately 10–15%. This suggests that leakage-aware preprocessing may be useful in scenarios where encrypted medical images are stored or transmitted in environments where traffic analysis or inference-based attacks are a concern. However, the results should be interpreted as experimental evidence under controlled conditions rather than as a complete validation of clinical deployment readiness. Although system components such as PACS integration, DICOMweb compatibility, and gateway-based encryption are discussed to define a realistic deployment scenario, the experimental validation in this work was conducted using offline datasets and controlled processing environments. Therefore, the results should be interpreted as demonstrating the feasibility and performance of the security framework rather than a full clinical system deployment.

5. CONCLUSION AND FUTURE DIRECTIONS

This paper presented a post-quantum KEM–DEM-based encryption framework for medical images combined with a leakage-aware evaluation methodology. The study showed that while standard authenticated encryption provides formal cryptographic confidentiality, measurable diagnostic and structural leakage can still be analyzed using task-based metrics. The primary contribution of this work is not the introduction of a new cryptographic primitive or a complete hospital deployment architecture, but the design and evaluation of a leakage-aware post-quantum encryption framework for medical imaging data. To address this, a keyed dual-domain confusion transform was introduced as a preprocessing step, and its effectiveness was evaluated using CDL, SLI, and histogram divergence metrics across multiple medical imaging modalities. Experimental results indicate that the proposed preprocessing stage reduces measurable leakage indicators while introducing a moderate computational overhead. The main contribution of this work is therefore a leakage-aware security evaluation framework integrated with post-quantum encryption, rather than a new cryptographic primitive or a complete clinical deployment system. Future work will focus on real-world system integration, hardware-level security evaluation, and large-scale traffic analysis.. It is important to note that the leakage-suppression transform improves resistance to inference-based leakage but does not replace the formal confidentiality guarantees provided by the underlying post-quantum KEM–DEM and AEAD encryption scheme. This work positions medical images as a challenging test case for evaluating confidentiality beyond standard cryptographic definitions, and proposes a leakage-aware evaluation framework built on top of standard post-quantum encryption. The proposed framework is intended to be compatible with clinical imaging workflows, but this study evaluates the system at the data security and leakage evaluation level rather than as a complete hospital deployment.

Future directions:

1. **Clinical-scale trials:** instrumented deployments across vendors/modalities to validate latency, energy, and audit behavior under real DICOMweb/DIMSE loads.
2. **Adaptive adversaries:** train stronger ciphertext-space models (self-supervised, multimodal) and perform white-box analyses to further bound CDL/SLI.
3. **Side-channel hygiene:** add constant-time kernels, memory-access flattening, and traffic-shape padding for streaming (US/fluoro), with measurable overhead curves.
4. **Crypto agility:** policy-driven rotation across ML-KEM-768/1024 and ML-DSA tiers; introduce **hybrid KEM** (classical+PQC) for transitional compliance and **threshold/HSM-sealed keys** for enterprise key custody.
5. **Edge acceleration:** fuse wavelet/permutation into SIMD/GPU kernels; explore on-sensor pre-confusion to minimize egress leakage.
6. **Secure analytics bridges:** pair encryption with privacy-preserving inference (HE/TEE/SPLIT learning) for on-prem triage where full decryption is undesirable.
7. **Lifecycle & provenance:** cryptographically signed audit trails, revocation/rotation playbooks, and cross-institution verification (e.g., transparency logs).
8. **Standards & certification:** package as a DICOM Transfer Syntax and pursue FIPS-validated modules to ease regulatory adoption.

Delivering these extensions will convert a robust prototype into a clinically dependable, quantum-resilient privacy layer for medical imaging ecosystems.

REFERENCES

[1] SaberiKamarposhti, M., Ng, K.W., Chua, F.F., Abdullah, J., Yadollahi, M., Moradi, M., Ahmadpour, S. (2024).

Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. Heliyon, 10(10): e31406. https://doi.org/10.1016/j.heliyon.2024.e31406

[2] Mansoor, K., Afzal, M., Iqbal, W., Abbas, Y., Mussiraliyeva, S., Chehri, A. (2024). PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems. Internet of Things, 27: 101228. https://doi.org/10.1016/j.iot.2024.101228

[3] Shafique, A., Naqvi, S.A.A., Raza, A., Ghalaii, M., Papanastasiou, P., McCann, J., Abbasi, Q.H., Imran, M.A. (2024). A hybrid encryption framework leveraging quantum and classical cryptography for secure transmission of medical images in IoT-based telemedicine networks. Scientific Reports, 14(1): 31054. https://doi.org/10.1038/s41598-024-82256-3

[4] Xu, S.Y., Chen, X., Guo, Y., Yiu, S.M., Gao, S., Xiao, B. (2024). Efficient and secure post-quantum certificateless signcryption for Internet of Medical Things. Cryptology ePrint Archive. https://ia.cr/2024/965.

[5] Khan, M.S., Ahmad, J., Al-Dubai, A., Pitropakis, N., Ghaleb, B., Ullah, A., Khan, M.A., Buchanan, W.J. (2024). Chaotic quantum encryption to secure image data in post quantum consumer technology. IEEE Transactions on Consumer Electronics, 70(4): 7087-7101. https://doi.org/10.1109/TCE.2024.3415411

[6] Pandey, S., Bhushan, B., Hameed, A.A. (2024). Securing healthcare 5.0: Zero-knowledge proof (ZKP) and post quantum cryptography (PQC) solutions for medical data security. In Soft Computing in Industry 5.0 for Sustainability, pp. 339-355. https://doi.org/10.1007/978-3-031-69336-6_15

[7] Herzog, D.J., Herzog, N.J. (2024). Innovative frontiers: Post-quantum perspectives in healthcare and medical imaging. Imaging and Radiation Research, 6(1): 3852. https://doi.org/10.24294/irr.v6i1.3852

[8] Boujelben, M., Abid, M. (2024). Post-quantum security design for hierarchical healthcare systems based on lattices. The Journal of Supercomputing, 80(12): 17292-17313. https://doi.org/10.1007/s11227-024-06143-4

[9] Ben Hssain, I., Bencherqui, A., Karmouni, H., Moustabchir, H., Sayyouri, M., Hafid, A. (2024). A comprehensive exploration of cryptographic solutions for securing medical images. In International Conference on Digital Technologies and Applications, pp. 526-535. https://doi.org/10.1007/978-3-031-68675-7_50

[10] Govindhan, P., Kumar, K. (2024). Post-quantum cryptography for multiple high-resolution millimeter wave images for enhanced security in IOT Networks. In 2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT), Gharuan, India, pp. 529-533. https://doi.org/10.1109/InCACCT61598.2024.10550966

[11] Roy, K.S., Singh, S., Srivathsa, P., Hazarika, R.A., Hassan, S.M., Kumar, K.S. (2025). Post-quantum digital signatures for enhanced medical image security. IET Quantum Communication, 6(1): e70006. https://doi.org/10.1049/qtc2.70006

[12] He, L.L., Rao, S.Y., Tian, K.X., Liu, Y.Y., Wang, J., Liu, S.G., Lu, X.H. (2025). A post-quantum blockchain and autonomous AI-enabled scheme for secure healthcare information exchange. IEEE Journal of Biomedical and Health Informatics, 29(9): 6883-6891. https://doi.org/10.1109/JBHI.2025.3579722

[13] Akkal, M., Cherbal, S., Annane, B., Lakhlef, H., Kharoubi, K. (2025). Quantum, post-quantum, and blockchain approaches for securing the internet of medical things: A systematic review. Cluster Computing, 28(10): 655. https://doi.org/10.1007/s10586-025-05481-z

[14] Roosan, D., Khan, R., Nirzhor, S., Hai, F. (2025). Post-quantum cryptography resilience in telehealth using quantum key distribution. Blockchain in Healthcare Today, 8(1). https://doi.org/10.30953/bhty.v8.379

[15] Roy, K.S., Singh, S., Kumar, M., Kumar, R., Hassan, M., Hazarika, R.A. (2025). QSMIT: A quantum secure medical image transmission using Sphincs+ with DICOM. IEEE Transactions on Consumer Electronics, 71(4): 10152-10159. https://doi.org/10.1109/TCE.2025.3601000

[16] Abdelfatah, R.I., Elsobky, R.M., Khamis, S.A. (2025). Ultra-secure quantum protection for e-healthcare images: Hybrid chaotic one-time pad with cipher chaining encryption framework. Journal of King Saud University Computer and Information Sciences, 37(6): 158. https://doi.org/10.1007/s44443-025-00155-7

[17] Bera, B., Nandi, S., Das, A.K., Sikdar, B. (2025). Healthcare security: Post-quantum continuous authentication with behavioral biometrics using vector similarity search. IEEE Transactions on Information Forensics and Security, 20: 1597-1612. https://doi.org/10.1109/TIFS.2025.3531197

[18] Gunapriya, B., Thirumalraj, A., Anusuya, V.S., Kavin, B.P., Seng, G.H. (2024). A smart innovative pre-trained model-based QDM for weed detection in soybean fields. In Advanced Intelligence Systems and Innovation in Entrepreneurship, pp. 262-285. https://doi.org/10.4018/979-8-3693-0790-8.ch015

[19] Kuznetsov, O., Zakharov, D., Frontoni, E. (2024). Deep learning-based biometric cryptographic key generation with post-quantum security. Multimedia Tools and Applications, 83(19): 56909-56938. https://doi.org/10.1007/s11042-023-17714-7

[20] Paul, S., Scheible, P., Wiemer, F. (2022). Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication. Journal of Computer Security, 30(4): 623-653. https://doi.org/10.3233/JCS-210037

[21] Ahmad, A., Jagatheswari, S. (2024). Lattice based three party authenticated key agreement scheme in medical IoT for post-quantum environment. IEEE Access, 12: 157247-157259. https://doi.org/10.1109/ACCESS.2024.3483971

[22] Tiwo, O.J., Adesokan-Imran, T.O., Babarinde, D.C., Oyekunle, S.M., Olutimehin, A.T., Olaniyi, O.O. (2025). Advancing security in cloud-based patient information systems with quantum-resistant encryption for healthcare data. Asian Journal of Research in Computer Science, 18(4): 187-208. https://doi.org/10.9734/ajrcos/2025/v18i4615

[23] Tarannum, D., Syed, M.A., Biswas, B.K., Chowdhury, M.R. (2025). Quantum-resistant image encryption using 2D Henon map with a three-qubit entanglement-based QKD protocol. APL Quantum, 2(4): 046110. https://doi.org/10.1063/5.0281728

[24] Khadija, Singh, K. (2025). Ensuring security and privacy in digital healthcare system. In 2025 International Conference on Networks and Cryptology (NETCRYPT), New Delhi, India, pp. 1919-1923.

https://doi.org/10.1109/NETCRYPT65877.2025.11102219
[25] Radanliev, P. (2025). Post-Quantum Security for AI: Resilient Digital Security in the Age of Artificial General Intelligence and Technological Singularity. Addison-Wesley Professional.
[26] Sood, N. (2024). Cryptography in post quantum computing era. https://doi.org/10.2139/ssrn.4705470
[27] Sethi, J., Mishra, S.K., Dash, P.P., Bhutani, M. (2025). Secure image encryption with optimized chaotic sequences and multi-layer cryptographic operations. SN Computer Science, 6(7): 879. https://doi.org/10.1007/s42979-025-04407-1
[28] Karim, T., Shaon, M.S.H., Fahim Sultan, M., Shapna Akter, M. (2025). Advancing image security with quantum key distribution and multi-layer chaotic encryption for quantum resilient transmission. arXiv e-prints, arXiv-2501.
[29] Singamaneni, K.K., Muhammad, G. (2024). A novel integrated quantum-resistant cryptography for secure scientific data exchange in ad hoc networks. Ad Hoc Networks, 164: 103607. https://doi.org/10.1016/j.adhoc.2024.103607
[30] Ghaemi, H., Abbasinezhad-Mood, D. (2024). Novel blockchain-integrated quantum-resilient self-certified authentication protocol for cross-industry communications. IEEE Transactions on Network Science and Engineering, 11(5): 4493-4502. https://doi.org/10.1109/TNSE.2024.3428916
[31] Abbood, A.A., AL-Shammri, F.K., Alzamili, Z.M., Al-Shareeda, M.A., Almaiah, M.A., AlAli, R. (2025). Investigating quantum-resilient security mechanisms for flying ad-hoc networks (fanets). Journal of Robotics and Control (JRC), 6(1): 456-469. https://doi.org/10.18196/jrc.v6i1.25351
[32] Gawali, P.P. (2025). Development of quantum key exchange mechanisms for securing medical cyber-physical systems. International Journal of Applied Mathematics, 38(1s): 454-477. https://doi.org/10.12732/ijam.v38i1s.27
[33] Balogun, A.Y. (2025). Post-quantum cryptography and encryption standards: Safeguarding patient data against emerging cyber threats in telemedicine. Asian Journal of Research in Computer Science, 18(3): 345-367. https://doi.org/10.9734/ajrcos/2025/v18i3598
[34] Rana, D. (2025). Quantum-enabled energy efficient secure data transmission for bio-cyber interfaces with QIoE and QKD for future healthcare systems. In 2025 IEEE Conference on Technologies for Sustainability (SusTech), Los Angeles, CA, USA, pp. 1-6. https://doi.org/10.1109/SusTech63138.2025.11025625
[35] Khan, A.A., Laghari, A.A., Almansour, H., Jamel, L., Hajjej, F., Estrela, V.V., Mohamed, M.A., Ullah, S. (2025). Quantum computing empowering blockchain technology with post quantum resistant cryptography for multimedia data privacy preservation in cloud-enabled public auditing platforms. Journal of Cloud Computing, 14(1): 43. https://doi.org/10.1186/s13677-025-00771-8
[36] Adil, M., Ali, A., Tin, T.T., Farouk, A., Al-Kuwari, S., Song, H., Jin, Z. (2025). Quantum computing and the future of healthcare internet of things security: Challenges and opportunities. IEEE Internet of Things Journal, 12(22): 46316-46346. https://doi.org/10.1109/JIOT.2025.3605040
[37] Abdulai, Y., Ma, M., Wang, H. (2025). QRMA-IOMT: Quantum-resilient mutual authentication for IoMT using RLWE and Boneh-Boyen signatures. Peer-to-Peer Networking and Applications, 18(6): 284. https://doi.org/10.1007/s12083-025-01990-1
[38] Andreou, A., Mavromoustakis, C.X., Markakis, E.K., Mastorakis, G., Pallis, E., Bourdena, A. (2024). Exploring quantum-resistant cryptography solutions for health data exchange. In Intelligent Technologies for Healthcare Business Applications. Signals and Communication Technology, pp. 19-47. https://doi.org/10.1007/978-3-031-58527-2_2
[39] Mallick, B., Parida, P., Nayak, C., Khalifa, T. (2025). Multi-channel multi-protocol quantum key distribution system for secure image transmission in healthcare. IEEE Access, 13: 62476-62505. https://doi.org/10.1109/ACCESS.2025.3558294
[40] Biswas, S., Raj, M.W.Z. (2024). Quantum-resistant cryptographic protocols integrated with AI for securing cloud and IoT environments. International Journal of Business and Economics Insights, 4(4): 60-90. https://doi.org/10.63125/dryw3b96
[41] Polu, O.R. (2023). Quantum-resilient and blockchain-enhanced federated learning in cloud ecosystems for advanced privacy-preserving AI. International Journal of Information Technology and Management Information Systems (IJITMIS), 14(2): 58-67. https://doi.org/10.34218/IJITMI_14_02_008
[42] Man, Z., Yu, Z., Yu, J., Gao, C., Meng, X. (2025). Edge computing in the internet of things: Lattice-based and split encryption for post-quantum data security. IEEE Internet of Things Journal, 12(23): 49327-49339. https://doi.org/10.1109/JIOT.2025.3591521
[43] Umer, N., Deng, M., Zhang, Y., Zhang, M., Khan, S. (2025). Quantum resilient security framework for privacy preserving AI in Apple MM1 on device architecture. Scientific Reports, 15(1): 38297. https://doi.org/10.1038/s41598-025-22056-5
[44] Prajapat, S., Gautam, D., Kumar, P., Das, A.K., Pal, S., Dong, C. (2025). Blockchain-enabled secure signature scheme with quantum key distribution for IoMT-based healthcare systems. IEEE Journal of Biomedical and Health Informatics, 30(4): 3601-3612. https://doi.org/10.1109/JBHI.2025.3614874
[45] Ahn, J., Kwon, H.Y., Ahn, B., Park, K., Kim, T., Lee, M.K., Kim, J., Chung, J. (2022). Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (PQC) and quantum key distribution (QKD). Energies, 15(3): 714. https://doi.org/10.3390/en15030714
[46] Al-Mekhlaf, Z.G., Saare, M.A., Altmemi, J.M.H., Al-Shareeda, M.A., Mohammed, B.A., Alshammari, G., Alrashdi, R., Alkhabra, Y.A., Alreshidi, I. (2025). A quantum-resilient lattice-based security framework for internet of medical things in healthcare systems. Journal of King Saud University Computer and Information Sciences, 37(6): 126. https://doi.org/10.1007/s44443-025-00140-0
[47] Eren, H., Karaduman, Ö., Gençoğlu, M.T. (2025). Security and privacy in the internet of everything (IoE): A review on blockchain, edge computing, AI, and quantum-resilient solutions. Applied Sciences, 15(15): 8704. https://doi.org/10.3390/app15158704
[48] Singamaneni, K.K., Budati, A.K., Islam, S.,

Kolandaisamy, R.A., Muhammad, G. (2025). A novel hybrid quantum-crypto standard to enhance security and resilience in 6G-enabled IoT networks. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 18: 7876-7891. https://doi.org/10.1109/JSTARS.2025.3540905

[49] Bera, B., Das, A.K., Sikdar, B. (2025). Quantum-resistant secure communication protocol for digital twin-enabled context-aware IoT-based healthcare applications. IEEE Transactions on Network Science and Engineering, 12(4): 2722-2738. https://doi.org/10.1109/TNSE.2025.3553044

[50] Hao, L., Wang, R., Wang, X., Yue, X., Tariq, N., Sajid, A. (2025). Post-quantum-inspired scalable blockchain architecture for internet hospital systems with lightweight privacy-preserving access control. Plos One, 20(12): e0332887. https://doi.org/10.1371/journal.pone.0332887

[51] Kumar, S., Klappenecker, A., Brown, G., Saravanan, S. (2025). Quantum apocalypse: Fortifying critical infrastructure in the age of cyber warfare. In European Conference on Cyber Warfare and Security, 24(1): 293-301. https://doi.org/10.34190/eccws.24.1.3757

[52] Sarkar, A., Jhamb, M. (2025). A novel ultra-low power post quantum approach using artificial intelligence based key generation for cyber physical system in Internet of Things. Sustainable Computing: Informatics and Systems, 48: 101242. https://doi.org/10.1016/j.suscom.2025.101242

[53] Gangappa, M., Satyanarayana, B.V. (2025). Secure image transmission using quantum-resilient and gate network for latent-key generation. Journal of Electronics, Electromedical Engineering, and Medical Informatics, 7(4): 1178-1198. https://doi.org/10.35882/jeeemi.v7i4.1156

NOMENCLATURE

Symbol	Description
(I)	Input medical image (pixel matrix)
(M)	DICOM metadata
(ROI)	Region of Interest mask (used only for leakage evaluation)
(pk, sk)	Public key and secret key of KEM
(ct)	KEM ciphertext
(ss)	Shared secret derived from KEM
(K_{enc})	AEAD encryption key
(K_{perm})	Permutation key
(K_{mask})	Sign masking key
(K_{nonce})	Nonce/IV derivation key
(W(\cdot))	Wavelet transform
(\pi)	Permutation function
(S)	Sign masking matrix
(T(cdot))	Dual-domain confusion transform
(P)	Plaintext data
(AAD)	Additional authenticated data