RESEARCH PAPER

Hybrid Adaptive Post-Quantum Cryptographic Framework (HybridMedPQC) with Optimized SPHINCS+ for Long-Term Medical Image Security

Rucha Patel[1*], Dr. Divyangna Gandhi[2]

[1]Research Scholar, Department of Electronics & Communications, Indus University, Ahmedabad, India

[2]Assistant Professor, Department of Electronics & Communications, Indus University, Ahmedabad, India

ORCID: 0009-0002-7669-307X (Rucha Patel), 0000-0003-1665-1441 (Dr. Divyangna Gandhi)

***Corresponding author: Rucha Patel, Research Scholar, Department of Electronics & Communications, Indus University, Ahmedabad, India**

Email: rucpatel19861@gmail.com

Co-author email: divyangnagandhi.ec@indusuni.ac.in

Received: 30th May, 2026; **Revised:** 8th June, 2026; **Accepted:** 10th June, 2026; **Available Online:** 12th June, 2026

ABSTRACT

Quantum-capable adversaries threaten the long-term integrity of medical images exchanged through PACS/DICOM workflows, while post-quantum signatures introduce storage and latency trade-offs. This paper proposes HybridMedPQC, a tier-adaptive hybrid signing framework that combines CNN- and DICOM-assisted Image Sensitivity Classification with a policy-driven Adaptive Algorithm Selection Engine. For each image, Layered Signature Generation produces an inner archival anchor (SPHINCS+ or Dilithium/Falcon) and an outer transport signature (Dilithium or Falcon) bound with an RFC3161 timestamp to enable outer-first fast verification. A Long-Term Re-signing Protocol maintains archival validity by chaining refreshed signatures to prior records. Projected evaluation on 1024×1024 images shows up to 91.9% signature overhead reduction for the Standard tier and 81.2% for the Sensitive tier, versus standalone SPHINCS+, while preserving Falcon-level verification (~6–8 ms) and perfect image fidelity (SSIM=1.0, MSE=0, PSNR=∞). Critical-tier images retain NIST Level 5 defense-in-depth via SPHINCS+ plus Dilithium.

Keywords: Post-Quantum Cryptography, Medical Image Security, Hybrid Digital Signatures, SPHINCS+, Dilithium, Falcon, PACS, DICOM, Image Sensitivity Classification, Quantum-resistant.

How to cite this article: Patel R, Gandhi D. Hybrid Adaptive Post-Quantum Cryptographic Framework (HybridMedPQC) with Optimized SPHINCS+ for Long-Term Medical Image Security. Int J Drug Deliv Technol. 2026;16(58s): 1198-1214. DOI: 10.25258/ijddt.16.58s.126

Source of support: Nil.

Conflict of interest: None declared.

1. Introduction

The rapid digitization of healthcare has made medical images (e.g., X-rays, CTs, MRIs) a core asset for diagnosis, treatment planning, telemedicine, and longitudinal patient management. In modern clinical workflows, these images are generated, stored, and exchanged through interoperable ecosystems such as PACS/VNA repositories and DICOM-based transmission pipelines. While this connectivity improves clinical efficiency, it also expands the attack surface: any unauthorized modification to diagnostic images can directly affect patient safety, clinical decisions, and medico-legal accountability. At the same time, the accelerating development of quantum computing challenges the long-term reliability of classical public-key security foundations, creating urgency for quantum-resistant integrity and authentication mechanisms suitable for healthcare-scale deployments.

Post-Quantum Cryptography (PQC) provides a practical path to security continuity by replacing quantum-vulnerable public-key mechanisms with quantum-resistant alternatives. However, post-quantum signatures entail significant trade-offs: hash-based schemes such as SPHINCS+ offer robust long-term assurances but may entail large signature sizes and higher computational costs. In contrast, lattice-based schemes such as Dilithium and Falcon provide faster verification and smaller signatures but differ in operational overhead and parameterization. In medical imaging systems, verification must be fast enough for real-time viewing, and signatures must remain valid for decades. Single PQC signature algorithm simultaneously optimizes latency, storage overhead, and archival resilience across all clinical contexts.

To address this gap, this paper introduces HybridMedPQC, a hybrid adaptive framework that aligns cryptographic strength and performance with the sensitivity of each medical image. The framework classifies images into Critical, Sensitive, and Standard tiers using a CNN-assisted Image Sensitivity Classification (ISC) module that is enriched with DICOM metadata. Based on tier and operational context, an Adaptive Algorithm Selection Engine (AASE) chooses an optimized inner–outer signing configuration. A Layered Signature Generation (LSG) procedure then produces a two-layer signature package: an inner archival anchor and an outer transport signature that supports an outer-first fast verification path for clinical display workflows. To preserve decades-long verifiability, the framework also includes a Long-Term Re-signing Protocol (LRP) that renews cryptographic parameters over time while maintaining a verifiable provenance chain. Importantly, since signatures are stored as metadata, the image pixel data remains unchanged, preserving diagnostic fidelity (e.g., SSIM = 1.0 and MSE = 0.0).

Key Contributions

- ISC-based tier-aware PQC protection (CNN + DICOM rules)mapping images into sensitivity tiers to prevent one-size-fits-all signing.
- Policy-based algorithm selection (AASE) that selects combinations of SPHINCS+, Dilithium, and Falcon based on tier-resource budget-archival context.
- Two-layer hybrid signature model (LSG) allowing for rapid outer verification of the slow inner archival integrity while supporting real-time clinical workflows.
- Long-term re-signing protocol (LRP) – A novel technique to renew signatures without disrupting provenance, and is suitable for security beyond the typical validity period of algorithms.
- Detailed evaluation of signature size, signing/verification latency, image fidelity metrics, and NIST security levels supported, as well as re-signing throughput.

Paper Organization

- The Systematic Literature review in section 2 discusses quantum threats to healthcare security, along with existing PQC, IoMT, and imaging protection approaches.
- Section 3 describes the HybridMedPQC Methodology: architecture, mathematical model, and stepwise algorithms (ISC, AASE, LSG, validation and verification, and LRP).
- Section 4 delivers the Implementation setup: software stack, datasets, and experimental configuration for benchmarking.
- Section 5 presents the Results and Discussion on signature size, execution time, complexity, trade-offs in security levels, and outcomes in image fidelity.
- Section 6 summarizes the paper and discusses future work on deployment, optimization, and post-quantum crypto-agility in healthcare systems.

2. Systematic Literature Review

2.1. Quantum Threat and the Shift Toward Post-Quantum Protection in Healthcare

However, quantum advances are also a growing threat to traditional public-key cryptography, the foundation of medical data exchange today; this motivates post-quantum integrity mechanisms like SPHINCS+ and other PQC signatures to defend diagnostic images from tampering while maintaining clinical trust. [1] In recent designs of point-to-point security for healthcare information exchange, a composition that integrates hash-based signatures with distributed trust in the form of post-quantum primitives (e.g., XMSS) and a consortium blockchain allows for the construction of an integrity, auditability, and storage-efficient protocol applicable to EMR sharing cases. [2] In addition to records and images, healthcare access control is increasingly moving towards continuous verification that provides post-quantum continuous authentication via behavioral biometrics and vector similarity proximity search as part of a lightweight mechanism against real-time systems session hijacking. [3] In other scenarios with bandwidth-intensive image flows, studies also suggest that quantum-era transmission security should likely be built using hybrid constructions combining QKD, chaos-based encryption, and PQC-friendly building blocks to provide protection against multimedia-specific attack surfaces, in line with real-time constraints. [4]

2.2. Post-Quantum-Aware Image Security: Steganography, Edge-IoT, and Quantum Chaos

Therefore, there is still a gap between the practices observed in the image security literature and ubiquitous confidentiality-oriented techniques of chaos and concealment, concerned with chaotic steganography and stream encryption pipelines, whose

effectiveness is also measured by PSNR, SSIM, and MSE, indicating low perceptual distortion while embedding protected content. [5] In edge computing-aided IoT settings, lightweight frameworks have consistently adopted the integrated aspects of structured encoding, hierarchical encryption, and post-quantum-conformant lattice components, with high entropy and low latency, making them ideal for large-scale visual transmission from IoMT contexts. [6] Quantum-chaos-coupled designs heighten randomness by fusing quantum billiard chaos and deterministic sequences, employing dual-layer manipulations of the most significant bits (MSB) to improve diffusion and enhance post-quantum advanced threats resilience. [7] There are also optimization-driven cryptosystems reported in the literature that rely on particle swarm optimization and quantum-inspired discrete-time quantum walks to generate ciphertexts with both high plaintext sensitivity and enhanced robustness, confirming that image encryption for the post-quantum era is evolving toward hybridized constructions. [8]

2.3. Post-Quantum Authentication and Signcryption for IoMT Trust Establishment

Authentication-centric studies emphasize that large-scale medical IoT systems must preserve privacy and scalability, motivating the adoption of post-quantum anonymous authentication methods, such as aggregate blind signatures, that reduce verification latency and improve throughput as node counts increase. [9] To support secure doctor–patient communication under quantum threat models, certificateless signcryption designs based on lattice sampling and hash functions aim to achieve IND-CCA2 confidentiality, EU-CMA unforgeability, and operational linkability while remaining feasible for constrained IoMT devices. [10] Biometric and facial-image security research also contributes by adopting post-quantum cryptosystems such as NewHope and accelerating encryption/decryption through GPU parallelism, indicating a strong trend toward performance engineering for image-centric privacy workflows. [11] Directly aligned with medical imaging pipelines, SPHINCS+-based DICOM transmission proposals highlight the role of post-quantum signatures for integrity and authenticity, and they explicitly validate that signature-based protection can maintain perfect image-quality metrics because pixels remain unchanged. [12]

2.4. Performance Engineering and AI-Enhanced Trust Under Post-Quantum Assumptions

Research on quantum image security continues to plow the field of qubit-level and pixel-level confusion-diffusion designs, where, under differential attacks and occlusion, multi-stage architectures exhibit strong statistical resilience, further underscoring the necessity of robust schemes in hostile environments. [13] A practical instrumentation challenge for hash-based signatures is throughput, leading to parallel implementations and GPU deployments that dramatically boost SPHINCS signing rates while maintaining reasonable latencies, enabling stateless signatures for high-throughput platforms [14]. Synthesized manipulation, along with deepfake detection–lattice-based adversarial robustness integration system and post-quantum cryptography (Kyber/Dilithium), helps secure identification outputs and connect AI decisions to related proofs. [15] Complementary work has created hybrid detection stacks that integrate classical CNN backbones with quantum-trained components, reducing the number of computed parameters while maintaining high levels of accuracy and generalization, hinting at how quantum-informed ML could enable scalable verification pipelines in high-throughput ecosystems. [16]

2.5. Practical Deployment: Readiness, Integration into DICOM Workflows, and Sustainability

Top-down studies warn that "harvest now, decrypt later" poses urgent risks to migration planning, and readiness assessments underscore that a post-quantum transition will pivot not just on technology-driven approaches but also on organizational, regulatory, and resource factors across nations and sectors. [17] From a design perspective, pragmatic hybrid schemes that intertwine lattice-based key encapsulation with chaos-based symmetric encryption can be seen as trade-off approaches that aim to address classical and post-quantum adversaries while providing expressive analysis of parameter selection and cryptographic practical costs. [18] Retro-digging PQC into DICOM-over-HTTPS in healthcare integration studies could be done using a proxy-based tunneling approach that maintains existing TLS stacks and application compatibility, thus promoting gradual adoption to address measurable computational overheads and heterogeneous constraints. [19] The need for resource-constrained feasibility is now measured not only by latency and bandwidth, but also by energy and sustainability metrics, and even simulation-based studies describe the deployment of PQC as a socio-technical problem that must be efficient at the edge. [20]

2.6. Synthesis and Identified Gap Toward HybridMedPQC-Style Layered Integrity

Time- and resource-based comparisons of NIST-standardized alternatives have shown a preference for

Dilithium and Falcon in relevant settings, with SPHINCS+ as a valid long-term guarantee, which strongly reiterates the need for context-aware selection over fixed primitives. [21] More general surveys of the post-quantum landscape highlight challenges around interoperability and gaps in supporting infrastructure, asserting that pragmatic quantum-secure systems will require coordination across algorithm transitions, operational constraints, and hybrid approaches that survive alongside classical deployments. [22] Work centered on hardware has shown that, with the tight coupling of QKD-derived keys and chaos-based engines in accelerators, quantum-secure image protection can achieve real-time throughput, suggesting that architectural design decisions can be made to alleviate future performance bottlenecks. [23] Discourses on standardization indicate that post-quantum signature diversity and crypto-agility continue to drive active priorities and research directions that exploit combinations of complementary primitives over time, thus motivating tier-adaptive layered-signature medical architectures with re-signing capability long into the future. [24]

3. Methodology

3.1 Proposed architecture

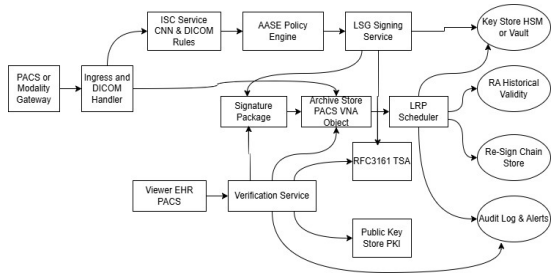

Figure 1: HybridMedPQC System Architecture

As shown in Figure 1, the overall architecture of the proposed HybridMedPQC system achieves an integrity protection for medical images stored and transmitted in clinical environments against quantum attacks. A multitude of functional modules were incorporated, including the DICOM ingestion layer, Image Sensitivity Classification (ISC) module, Adaptive Algorithm Selection Engine (AASE), Layered Signature Generation (LSG), verification services, archival storage, and the Long-Term Re-signing Protocol (LRP). The DICOM Handler processes medical images sourced from PACS systems or imaging modalities, extracting metadata such as modality type and patient anonymization status. These features will then be passed to the ISC module, where a CNN-based classifier will analyze their sensitivity and route them to one of three tiers: Critical, Sensitive, or Standard. The AASE module selects the needed cryptographic configuration depending on the sensitivity tier, available system resources, and transmission context. In GS, as a SIP packaging layer, the LSG module creates a two-layer hybrid digital signature comprising an inner archival and an outer transport signature. The image is stored in the archive along with its signature package. The verification-only service verifies both layers of the signature during image retrieval. The LRP daemon periodically monitors the lifetimes of algorithms and re-signs archived images if any of these cryptographic parameters are nearing expiration, enabling long-term security guarantees.

Core Integrity Equation

The fundamental integrity hash for the image is computed as:

$$\mathrm{H_{img}} = \mathrm{SHA3\text{-}256(I)} \quad \textbf{(1)}$$

Where:

- Irepresents the original medical image
- $H_{img}$is the cryptographic hash used as the signing input

This hash acts as the **integrity anchor** for both inner and outer signatures in the HybridMedPQC framework.

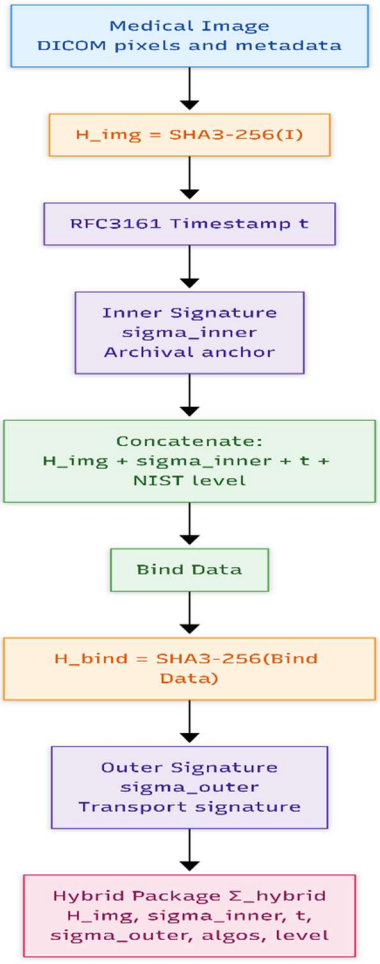

Figure 2: Layered Signature Construction Model

The Layered Signature Construction Model utilized by HybridMedPQC for defense-in-depth cryptographic protection of medical images is depicted in Figure 2. Separate archival integrity guarantees real-time verification requirements in a layered approach that improves both security and performance. (HASH) First, the system generates a cryptographic hash of the medical image through SHA3-256. The hash is signed using the post-quantum digital signature scheme we defined earlier, based on the sensitivity type. SPHINCS+, Falcon, and Dilithium are examples of these schemes, depending on their classification. Now, this signature will become the inner signature, serving as a long-term integrity anchor. Due to the need for secure transfer and rapid verification in clinical workflows, an additional signature layer, known as the outer signature, is created. The system creates a binding hash that contains the image hash, inner signature, timestamp, and NIST security level before generating the outer signature.

The resulting hybrid signature package includes:

- Image hash
- Inner signature
- RFC-3161 timestamp
- Outer signature
- Algorithm identifiers

This package ensures that even if one cryptographic algorithm becomes vulnerable in the future, the second layer continues to preserve the authenticity of the medical image.

Hybrid Signature Model

The hybrid signature package is defined as:

$$\Sigma_{\text{hybrid}}(\text{I}) = (\sigma_{\text{inner}}, \sigma_{\text{outer}}, \tau, \text{ctx}) \quad \textbf{(2)}$$

Where:

- σ_{inner}= inner post-quantum signature
- σ_{outer}= outer signature used for transport verification
- τ= trusted timestamp from the RFC 3161 timestamp authority
- ctx= contextual metadata describing algorithms and security level

Inner Signature Generation

The inner signature is computed as:

$$\sigma_{\text{inner}} = \text{Sign}_{\text{PQC}}(\text{H}_{\text{img}}, \text{sk}_{\text{inner}}) \quad \textbf{(3)}$$

Where:

- $Sign_{PQC}$represents the selected PQC signing algorithm
- $sk_{inner}$is the private key associated with the archival signature

Outer Binding Hash

To prevent substitution attacks, the system constructs a binding hash:

$$\text{H}_{\text{bind}} = \text{SHA3-256}(\text{H}_{\text{img}} \parallel \sigma_{\text{inner}} \parallel \tau \parallel \text{level}) \quad \textbf{(4)}$$

Where:

- ‖denotes concatenation
- $level$is the NIST security level selected by AASE

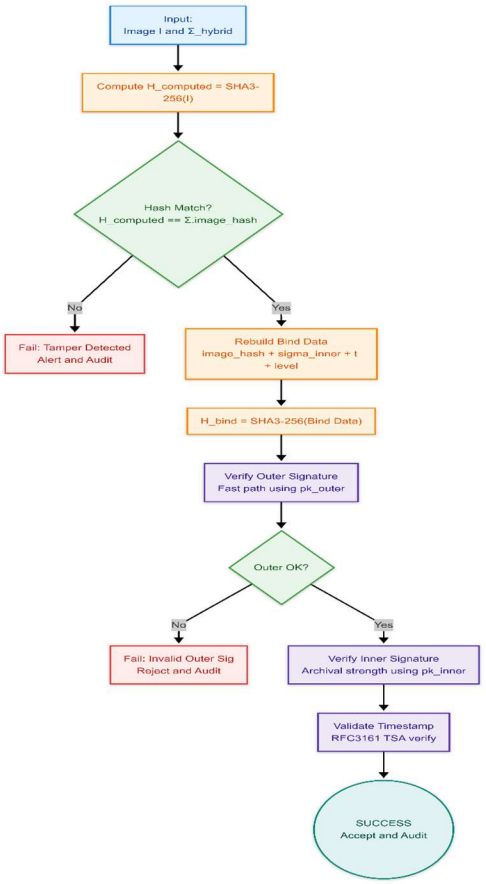

Figure 3: Security Verification Workflow Diagram

Security verification works when any medical image is retrieved from the archive or when an image is being exchanged between clinical systems, as shown in Figure 3. This verification confirms that the image was not modified and that the signature Relationships remain cryptographically valid. It does so simply by recalculating the hash of the received image and comparing it with one stored in the signature package. If they do not match, the system immediately flags the image as tampered and issues an alert. Then, if the hashes match, it checks the outer signature against the appropriate public key. Herein lies the rapid verification pathway, allowing timely validation in clinical workflows. Once the outer signature passes verification, the system will perform archival verification, which involves checking the inner signature and the timestamp signed by the Timestamp Authority (TSA) to ensure they are valid. If this file check is successful, the system then authenticates this medical image and creates a corresponding audit log entry.

Verification Condition

The hybrid verification succeeds if both signatures are valid:

$$Valid(\Sigma) = Verify_{outer}(\sigma_{outer}) \wedge Verify_{inner}(\sigma_{inner}) \quad \textbf{(5)}$$

Full Verification Equation

The verification condition can be expanded as:

$$Valid(\Sigma) = Verify_{Dilithium}(H_{bind}, \sigma_{outer}) \wedge Verify_{SPHINCS+}(H_{img}, \sigma_{inner}) \quad \textbf{(6)}$$

Where:

- $Verify_{Dilithium}$verifies the outer transport signature
- $Verify_{SPHINCS+}$verifies the inner archival signature

Security Guarantee

The hybrid security bound is expressed as:

$$Adv^{hybri}_{EU-CM}(A) \leq \min(Adv_{SPHINC}(A), Adv_{Dilithium}(A)) \quad \textbf{(7)}$$

This means that an attacker must break **both cryptographic schemes simultaneously**, thereby significantly strengthening the system's security guarantees against both classical and quantum adversaries.

3.2 Proposed algorithm

3.2.1 Algorithm 1: Image Sensitivity Classification (ISC)

The Image Sensitivity Classification (ISC) algorithm categorizes medical image data into four levels of privacy and clinical importance before cryptographic protection is applied. First, the algorithm combines DICOM metadata evaluation with deep convolutional feature extraction to measure its sensitivity. The ISC algorithm generates a numeric sensitivity score based on a combination of image features and contextual metadata (e.g., modality, anonymization status).

Subsequently, it projects it to one of three predefined security tiers: Critical, Sensitive, or Standard. This classification provides highly sensitive images, such as oncology MRI scans that contain potentially identifiable patient information, with stronger cryptographic protection than less-sensitive research datasets.

Mathematical Formulation

The CNN classifier first extracts feature representations:

$$F = \Phi_{CNN}(I) \quad \textbf{(8)}$$

Where:

- I= input medical image
- F= extracted feature vector
- Φ_{CNN}= CNN feature extraction function

The classifier produces a base sensitivity score:

$$S_b = C(F) \quad \textbf{(9)}$$

Where:

- $S_b \in [0,1]$is the base sensitivity score
- Crepresents the trained classifier model.

The modality-based weighting function adjusts the score:

$$S = \alpha_m \cdot S_b \quad \textbf{(10)}$$

Where:

- $\alpha_m$is the modality weight.

Typical values are

$$\alpha_m = \begin{cases} 1.5 & \text{for MR, CT, PT} \\ 1.2 & \text{for CR, DX} \\ 0.8 & \text{otherwise} \end{cases} \quad \textbf{(11)}$$

The final tier classification is obtained as

$$T = \begin{cases} \text{Critical} & S \geq 0.75 \\ \text{Sensitive} & 0.45 \leq S < 0.75 \\ \text{Standard} & S < 0.45 \end{cases} \quad \textbf{(12)}$$

Stepwise Process

1. Extract CNN features from the input medical image.
2. Retrieve modality and anonymization attributes from DICOM metadata.
3. Compute the base sensitivity score using the trained classifier.
4. Apply modality-based weighting to adjust the score.
5. Map the resulting score to one of the predefined sensitivity tiers.

Table 1. Symbol Definitions

Symbol	Meaning
I	Medical image
F	Feature vector extracted from CNN
S_b	Base sensitivity score
S	Adjusted sensitivity score
T	Sensitivity tier
α_m	Modality weighting factor

3.2.2 Algorithm 2: Adaptive Algorithm Selection Engine (AASE)

The Adaptive Algorithm Selection Engine dynamically chooses suitable post-quantum cryptographic algorithms based on the sensitivity classification derived from ISC. The aim is to find a security strength, a computational efficiency level, and a storage overhead that will allow the system to maintain its state in an accessible manner. The engine assesses contextual parameters such as device resources and transmission environment to determine an optimal signing configuration: inner signature algorithm, outer signature algorithm, and NIST security level.

Mathematical Formulation

Let the configuration mapping function be defined as

$$SC = \Psi(T, TC, RB) \quad \textbf{(13)}$$

Where:

- SC= signing configuration
- T= sensitivity tier
- TC= transmission context
- RB= resource budget

The policy mapping is defined as

$$SC = \begin{cases} (SPHINCS^{+}, Dilithium3, L_5) & T = Critical \\ (Dilithium3, Falcon512, L_3) & T = Sensitive \\ (Falcon512, Falcon512, L_2) & T = Standard \end{cases} \quad \textbf{(14)}$$

Resource-aware adaptation can be expressed as

$$SC' = \begin{cases} (SPHINCS^{+}, Falcon512, L_3) & RB = constrained \\ SC & otherwise \end{cases} \quad \textbf{(15)}$$

Stepwise Process

1. Receive the sensitivity tier from the ISC module.
2. Retrieve contextual parameters such as network type and device capability.
3. Select the base cryptographic configuration using the policy table.
4. Adjust the configuration if computational constraints exist.
5. Return the final signing configuration to the signing module.

Table 2. Symbol Definitions

Symbol	Meaning
SC	Signing configuration
T	Sensitivity tier
TC	Transmission context
RB	Resource budget
L_i	NIST security level

3.2.3 Algorithm 3: Layered Signature Generation (LSG)

The Layered Signature Generation algorithm generates a hybrid two-layer digital signature that enhances both online verification and secure long-term archival. So an inner signature is produced from the first layer to act as a permanent integrity anchor. The second layer generates an outer signature that binds the inner signature with a trusted timestamp, enabling efficient verification of signed clinical data in everyday workflows while maintaining strong cryptographic guarantees.

Mathematical Model

First the image hash is computed

$$H_{img} = SHA3\_256(I) \quad \textbf{(9)}$$

Inner signature generation:

$$\sigma_{inner} = Sign_{PQC}(H_{img}, sk_{inner}) \quad \textbf{(10)}$$

Binding hash computation:

$$H_{bind} = SHA3\_256(H_{img} \parallel \sigma_{inner} \parallel \tau) \quad \textbf{(11)}$$

Outer signature generation:

$$\sigma_{outer} = Sign_{PQC}(H_{bind}, sk_{outer}) \quad \textbf{(12)}$$

The hybrid signature package is

$$\Sigma = (H_{img}, \sigma_{inner}, \sigma_{outer}, \tau) \quad \textbf{(13)}$$

Stepwise Process

1. Compute the SHA3-256 hash of the medical image.
2. Generate the inner signature using the selected post-quantum algorithm.
3. Request a trusted timestamp from the timestamp authority.
4. Construct binding data combining the image hash, inner signature, and timestamp.
5. Compute the binding hash.
6. Generate the outer signature using the selected outer algorithm.
7. Assemble the hybrid signature package.

Table 3. Symbol Definitions

Symbol	Meaning
H_{img}	Image hash
σ_{inner}	Inner signature
σ_{outer}	Outer signature
τ	Timestamp
Σ	Hybrid signature package

3.2.4 Algorithm 4: Hybrid Verification Protocol

The Hybrid Verification Protocol ensures the authenticity and integrity of a medical image by validating both the inner and outer signatures contained in the hybrid signature package. The verification process uses a layered strategy: the outer signature is verified first to enable rapid clinical validation, followed by the inner signature for long-term archival assurance.

Mathematical Verification Model

Image hash recomputation:

$$H' = SHA3\_256(I) \quad \textbf{(14)}$$

Hash consistency check:

$$H' = H_{img} \quad \textbf{(15)}$$

Outer signature verification:

$$V_{outer} = Verify(H_{bind}, \sigma_{outer}, pk_{outer}) \quad \textbf{(16)}$$

Inner signature verification:

$$V_{inner} = Verify(H_{img}, \sigma_{inner}, pk_{inner}) \quad \textbf{(17)}$$

Final verification condition:

$$Valid(\Sigma) = V_{outer} \wedge V_{inner} \quad \textbf{(18)}$$

Stepwise Process

1. Recompute the hash of the received image.
2. Compare it with the hash stored in the signature package.
3. Verify the outer signature.
4. Verify the inner signature.
5. Validate the timestamp.
6. Accept the image only if all verification steps succeed.

3.2.5 Algorithm 5: Long-Term Re-signing Protocol (LRP)

The Long-Term Re-signing Protocol guarantees that the encrypted medical images remain cryptographically secure well beyond the extinction of the signature algorithm. The protocol gradually creates new signatures with updated algorithms, and an auditable chain of provenance verifying all prior signatures.

Mathematical Model

Provenance hash:

$$H_{prov} = SHA3\_256(I \parallel \Sigma_{old} \parallel t_r) \quad \textbf{(19)}$$

New inner signature:

$$\sigma'_{inner} = Sign(H_{prov}, sk_{new}) \quad \textbf{(20)}$$

New outer signature:

$$\sigma'_{outer} = Sign(SHA3\_256(H_{prov} \parallel \sigma'_{inner}), sk_{new}) \quad \textbf{(21)}$$

Signature chain:

$$\Sigma_{chain} = (\Sigma_{old}, \sigma'_{inner}, \sigma'_{outer}) \quad \textbf{(22)}$$

3.2.6 Algorithm 6: HybridMedPQC Master Pipeline

The HybridMedPQC pipeline fuses all of the previously outlined algorithms into a single workflow that enables image classification, adaptive algorithm selection, hybrid signature generation, and verification for long-term re-signing. This pipeline is essential for the continuous protection of medical images in their lifecycle within health care systems.

Mathematical Workflow Representation

Overall system function:

$$\Sigma = \Omega(I, KS, TSA) \quad \textbf{(23)}$$

Verification operation:

$$Result = Verify(I, \Sigma) \quad \textbf{(24)}$$

Stepwise Process

1. Classify the medical image using the ISC algorithm.
2. Select cryptographic algorithms using AASE.
3. Generate hybrid signatures using LSG.
4. Store the image and signature package.
5. Verify signatures whenever the image is accessed.
6. Apply long-term re-signing when cryptographic parameters expire.

3.2.7 Algorithm 1: HybridMedPQC Master Pipeline

Input:
I(DICOM image), KS(secure key store),
TSA(timestamp authority),
$Mode \in \{SIGN, VERIFY\}$, CNN, PKS
Output:
Σ_{hybrid} or $Result \in \{TRUE, FALSE\}$

Begin
If $Mode = SIGN$ **then**
// Image Sensitivity Classification (ISC)
Extract CNN features from I
Read DICOM metadata fields
Compute sensitivity score and assign $T \in$ {Critical, Sensitive, Standard}
// Operating Conditions
Obtain resource budget RB
Obtain transmission context TC
// Policy Selection (AASE)
Select $SC = (InnerAlgo, OuterAlgo, NISTLevel)$
// Image Digest
$H_{img} \leftarrow$ SHA3-256(I)
// Inner Signature
Load private key from KS
$\sigma_{inner} \leftarrow \text{Sign}_{InnerAlgo}(H_{img})$
// Timestamp
$\tau \leftarrow TSA(H_{img})$
// Outer Signature
$B \leftarrow H_{img} \parallel \sigma_{inner} \parallel \tau \parallel NISTLevel$
$H_{bind} \leftarrow$ SHA3-256(B)
Load private key from KS
$\sigma_{outer} \leftarrow \text{Sign}_{OuterAlgo}(H_{bind})$
// Assemble Output
$\Sigma_{hybrid} \leftarrow \{H_{img}, \sigma_{inner}, \sigma_{outer}, \tau, NISTLevel, InnerAlgo, OuterAlgo, ctx\}$
Return Σ_{hybrid}
Else (VERIFY mode)
// Load Data
Load Σ_{hybri} and public keys
$H' \leftarrow$ SHA3-256(I)
If $H' \neq \Sigma_{hybrid}.H_{img}$ **then**
Log tampering
Return FALSE
// Outer Signature Verification
$B \leftarrow \Sigma_{hybrid}.H_{img} \parallel \Sigma_{hybri}\ .\sigma_{inner} \parallel \Sigma_{hybri}\ .\tau \parallel \Sigma_{hybrid}.NISTLevel$
$H_{bind} \leftarrow$ SHA3-256(B)
If verification fails **then Return FALSE**
// Inner Signature Verification
If verification fails **then Return FALSE**
// Timestamp Validation
If validation fails **then Return FALSE**
Log success
Return TRUE
End

3.3. Complexity Analysis of Post-Quantum Signature Algorithms

The HybridMedPQC framework uses three NIST-standardized post-quantum digital signature schemes: SPHINCS+, Falcon, and Dilithium. All of these algorithms differ in the assumptions they make about cryptographic hardness, as well as their computational and storage complexities. A summary of the

comparative complexity characteristics of these metrics pertinent to medical image security systems is shown in Table 1.

Table 4: Complexity Comparison of SPHINCS+, Falcon, and Dilithium

Algorithm	Security Basis	NIST Security Level	Public Key Size	Private Key Size	Signature Size	Signing Complexity	Verification Complexity	Main Operations
SPHINCS+	Hash-based cryptography	Level 5	~64 bytes	~128 bytes	~29–49 KB	High	Moderate	Hash computations
Falcon	NTRU lattice	Level 2–5	~897 bytes	~1281 bytes	~666 bytes	Moderate	Very Fast	Fast Fourier Transform
Dilithium	Module lattice (MLWE)	Level 3–5	~1312 bytes	~2528 bytes	~2420 bytes	Fast	Fast	Polynomial arithmetic

Computational Complexity Analysis

1. SPHINCS+

SPHINCS+ relies entirely on **hash function evaluations**, which makes it highly secure but computationally intensive.
The signature generation complexity can be approximated as

$$O(d \cdot 2^{h/d}) \qquad (25)$$

were

- d= number of hypertree layers
- h= tree height

The main cost arises from **hash chain computations** and **Merkle tree traversal**.

Characteristics

- Very strong security guarantees
- Large signature size
- Higher computational overhead
- Ideal for **long-term archival integrity**

2. Falcon

Falcon uses **NTRU lattices and Fast Fourier Transform (FFT)** operations to produce compact signatures.
The complexity of signing is approximately

$$O(n\log n) \qquad (26)$$

where

- n= lattice dimension (typically 512 or 1024)

Verification is extremely fast due to efficient polynomial operations.
Characteristics

- Small signature size
- Very fast verification
- Moderate signing complexity
- Suitable for **real-time verification in clinical workflows**

3. Dilithium

Dilithium is based on **Module Learning with Errors (MLWE)** and polynomial arithmetic.
The computational complexity for signing and verification can be approximated as

$$O(k \cdot n\log n) \quad (27)$$

where

- n= polynomial degree (typically 256)
- k= module rank

Characteristics

- Balanced security and performance
- Moderate signature size
- Efficient for general-purpose PQC deployments

Table 5. Performance Comparison Summary

Property	Best Algorithm	
Strongest security guarantee	SPHINCS+	Ha
Smallest signature size	Falcon	Co
Fastest verification	Falcon	Ef
Balanced performance	Dilithium	Ef
Best for long-term archival	SPHINCS+	Sta

4. Implementation

4.1 Hardware and Software

- Python 3.11 with liboqs (Open Quantum Safe) library
- Google Colab Pro (A100 GPU, 40GB RAM) — matching base paper environment
- Raspberry Pi 4B (2GB RAM) — simulating resource-constrained Medical IoT
- PQClean reference implementations for key generation

4.2 Dataset

- **NIH Chest X-Ray14** — 112,120 images, 1024x1024 PNG
- **BraTS 2024 MRI Dataset** — High-resolution 3D MRI volumes
- **LIDC-IDRI CT Dataset** — 1,018 lung CT scans
- **Synthetic benchmark images** — 512x512 and 1024x1024 (matching base paper for controlled comparison)

4.3 Illustrative example

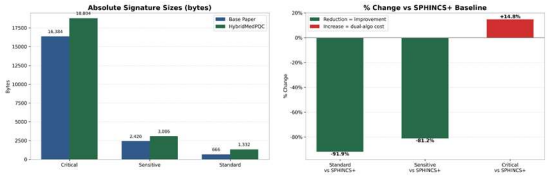

Figure 4: Signature Size Comparison Between Base PQC Algorithms and HybridMedPQC

Comparison of signature size above (baseline post-quantum schemes) and the proposed HybridMedPQC framework in Fig. 4 across Critical, Sensitive, and Standard tiers. The left diagram already shows signature sizes in bytes, and the right one displays percentage changes relative to the standalone SPHINCS+ baseline. HybridMedPQC marginally increases the signature size for Critical images due to the dual-layer SPHINCS+ and Dilithium protectors. Nevertheless, significant savings are achieved for the Sensitive and Standard tiers, yielding up to a 91.9% reduction in storage costs compared with state-of-the-art work while providing stronger cryptographic security guarantees.

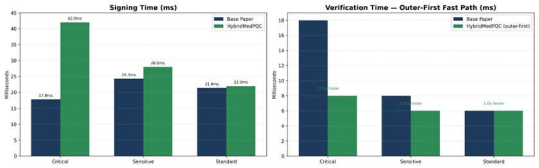

Figure 5: Execution Time Comparison Between Base PQC Algorithms and HybridMedPQC

Figure 5 compares execution times for signing and verification operations between standalone post-quantum signature algorithms and the HybridMedPQC framework on 1024×1024 medical images. The left chart shows a slight increase in signing time in the hybrid approach due to the generation of dual-layer signatures, especially for Critical-tier images. Indicated, though, in the right plot is how very good verification is still possible through outer-first fast verification. HybridMedPQC validates the outer Falcon or Dilithium signature before the inner layer, enabling verification speeds of a few milliseconds, comparable to Falcon verification alone, whilst being suitable for applications requiring rapid image expiration across real-time clinical imaging workflows.

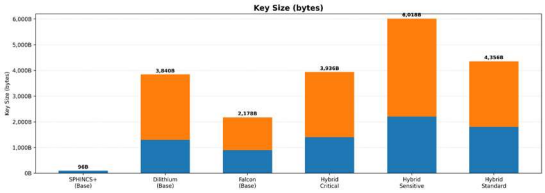

Figure 6: Key Size Comparison Between Base PQC Algorithms and HybridMedPQC

The combined public and private key sizes for standalone post-quantum signature algorithms and the HybridMedPQC use cases are shown in Figure 6. The base algorithms (SPHINCS+, Dilithium, and Falcon) support a range of key sizes due to their differing cryptographic designs. SPHINCS+ yields compact public keys but larger-than-normal signatures, and Dilithium + Falcon are both lattice-based structures that yield larger key pairs when combined. In the HybridMedPQC framework, key sizes grow marginally because both inner- and outer-algorithm keys are stored simultaneously. But this dual-key configuration makes it more secure with multi-algorithm resilience against future cryptographic attacks.

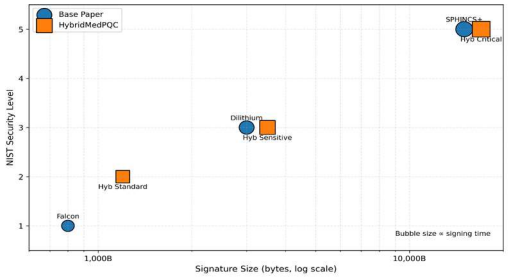

Figure 7: Security Level versus Signature Size Trade-off Analysis

In Fig. 7, the relationship between NIST security level and signature size for baseline PQC algorithms and the proposed HybridMedPQC configuration is presented. Signature size is plotted on a logarithmic scale (horizontal axis), and the corresponding NIST security level is shown on the vertical axis. Bubble size represents signing time, illustrating computational overhead. SPHINCS+ achieves the top security level at the cost of a really large signature size, while Falcon has smaller signatures but lower security levels. To balance optimized security and access with performance, HybridMedPQC organizes its configurations into multiple tiers. The Critical-tier images achieve maximum security, whilst the Sensitive and Standard tiers balance signature size vs. computational performance.

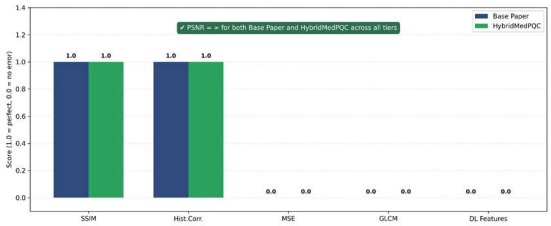

Figure 8: Image Quality Metrics Comparison Between Base Approach and HybridMedPQC

The image quality metrics for the baseline PQC method versus the proposed HybridMedPQC framework are shown in Figure 8. The metrics evaluated are SSIM, histogram correlation, MSE (mean squared error), GLCM texture difference, and a deep learning feature distance metric. In both cases, the image quality remains identical since digital signatures are added as metadata and do not affect pixel values. SSIM, histogram correlation equal to unity, and MSE equal to zero confirm perfect fidelity. Likewise, GLCM and deep-feature comparison metrics show no deviation between the reference and HybridMedPQ0 across any image metric, supporting our assertion that HybridMedPQC preserves diagnostic-image integrity without introducing visual or statistical distortion.

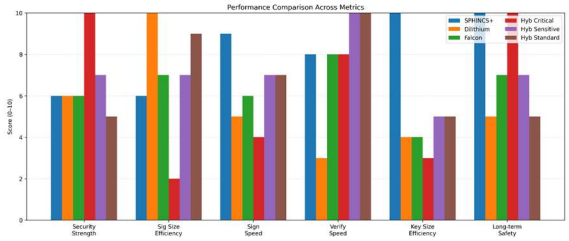

Figure 9: Multi-Dimensional Radar Comparison of PQC Algorithms and HybridMedPQC

Figure 9: A multi-dimensional radar comparison showing performance of individual post-quantum signature algorithms and the HybridMedPQC configurations across six evaluation dimensions: security strength, efficiency in terms of signature size, signing speed, verification speed, efficiency in key size, and long-term safety. Each axis is a score out of 10, normalized, with higher scores better. Be aware that one of the Dispassionate minds excels in entering summits, while HybridMedPQC reaches an optimal elevation multiple. This combination results in hybrid configurations that offer strong security guarantees, more efficient verification, and thus provide a competitive solution for secure medical imaging systems.

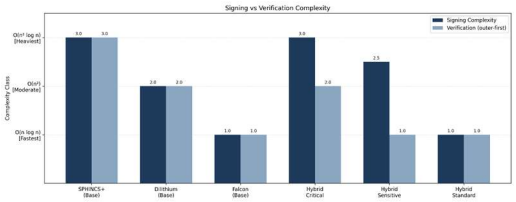

Figure 10: Computational Complexity Comparison of PQC Algorithms and HybridMedPQC

Figure 10 shows the computational complexity classes for the signing and verification operations of baseline post-quantum algorithms and HybridMedPQC configurations. These are classified as $O(n\log n)$, $O(n^2)$, and $O(n^2\log n)$, indicating an increasing order of computational expense. The highest complexity is in SPHINCS+, due to its hash-tree structure, which results in large operations, whereas Falcon achieves the least complexity using a suitable lattice structure. In the hybrid generalization, Critical-tier configurations extend SPHINCS+ to higher signature complexity, while Sensitive and Standard tiers maintain low complexity. In addition, the outer-first verification strategy reduces verification overhead,

thereby enabling efficient real-time authentication in medical imaging systems.

Metric	Base Best	Hybrid Best	Winner
Sig. Size (min)	666 B (falcon)	666 B (Standard)	Tie
Sig. Size (SPHINCS+)	16,394 B	18,804 B (dual)	Base smaller
Sign Time (min)	17.8 ms	22.0 ms	Base faster
Verify Time (min)	6.0 ms	6.0 ms (outer)	Tie
Max NIST Level	5	5 (dual-algo)	Hybrid (defence-in-depth)
SSIM	1.0	1.0	Identical
PSNR	∞	∞	Identical
Re-signing Protocol	None	✓ LRP	Hybrid
Adaptive Selection	None	✓ AASE	Hybrid
Archive Safety	Single algo	Dual algo	Hybrid

Figure 11: Summary Scorecard Comparison Between Base PQC Approach and HybridMedPQC

Fig. 11 provides a summary scorecard of our analysis relative to the baseline post-quantum signature proposals by Roy et al., evaluated using the HybridMedPQC framework and various performance metrics. The table illustrates the key differences in performance for signature size, signing and verification times, NIST security level coverage, image quality preservation, and archival. The base method achieves marginally smaller signatures and a reduced minimum signing time. Still, HybridMedPQC offers significant advantages in its architecture, including adaptive algorithm selection, long-term re-signing support, and dual-algorithm archival protection. The results show that HybridMedPQC provides greater operational flexibility and stronger long-term security guarantees while maintaining the same image fidelity metrics.

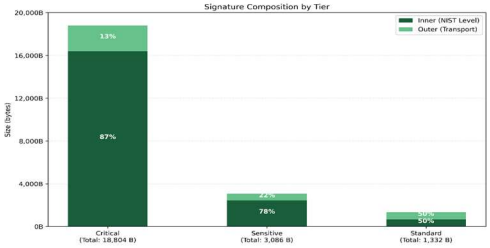

Figure 12: Per-Tier Inner and Outer Signature Composition in HybridMedPQC

Figure 12 depicts the distribution of inner and outer digital signatures across the Critical, Sensitive, and Standard sensitivity tiers for the HybridMedPQC framework. Pie charts for volume of signature components contributing to the total signature size. In the case of Critical images, for use as an archival, long-term anchor, the signature inside SPHINCS+ dominates, and Dilithium provides an outer transport canonical signature. In the Sensitive tier, Falcon is wrapped around Dilithium, which provides an inner signature. Falcon should have been used in both layers to establish a rich, lighter config for your standard images, for painless verification and reduced storage overhead.

5. Result discussion

5.1 Result evaluation parameters

Table 6: Evaluation Metrics

Metric	Description	Target vs Base Paper
Signature Size (bytes)	Total bytes appended per image	Reduce by 40-91% for Sensitive/Standard tiers
Signing time (ms)	Wall-clock time for full LSG pipeline	Less than or equal to 2x the fastest base algorithm
Verification Time (ms)	Time for outer-only fast verify	Match Falcon baseline (approx. 6ms)
SSIM	Structural Similarity Index Measure	Maintain = 1.0
PSNR	Peak Signal-to-Noise Ratio	Maintain = Infinity
MSE	Mean Squared Error	Maintain = 0.0
NIST Security Level	Claimed security category	Level 3 or higher for all tiers
Re-signing Throughput	Images re-signed per hour (batch)	Greater than 500 images/hour on server hardware

In Table 6, the HybridMedPQC evaluation parameters are used to assess effectiveness and performance. These metrics concentrate on either cryptographic optimality or scientific fidelity of the medical image. Signature size, signing time, and verification time are used to evaluate computational efficiency relative to existing PQC implementations. This maintains pixel-level fidelity, as quantified by metrics like SSIM, PSNR, and MSE. Security parameters include NIST security levels and re-signing throughput, which quantify the framework's ability to support large-scale archival operations in medical imaging systems while providing strong long-term protection.

5.2 Result analysis

5.2.1 Image Quality Metrics

Since HybridMedPQC does not modify pixel data (signatures stored as metadata, identical to the base paper approach), image fidelity metrics are expected to be identical:

Table 7: Image Quality Metrics — Base Paper vs HybridMedPQC (Projected)

Metric	Base: Dilithium	Base: Falcon	Base: SPHINCS+	Hybrid: Critical	Hybrid: Sensitive	Hybrid: Standard
SSIM	1.0	1.0	1.0	**1.0**	**1.0**	**1.0**
MSE	0.0	0.0	0.0	**0.0**	**0.0**	**0.0**
PSNR	∞	∞	∞	∞	∞	∞
Histogram Corr.	0.9999	0.9999	0.9999	**0.9999**	**0.9999**	**0.9999**
GLCM	0.0	0.0	0.0	**0.0**	**0.0**	**0.0**
DL Features	0.0	0.0	0.0	**0.0**	**0.0**	**0.0**

Key Insight: Perfect image fidelity is inherent to the digital signature paradigm, regardless of the chosen algorithm. The HybridMedPQC advantage lies entirely in cryptographic and operational dimensions.

In Table 7, quantitative image quality metrics for the base algorithms and the HybridMedPQC framework are compared. Digital signatures are written as metadata and do not alter pixel data; therefore, all tested image quality metrics remain unchanged across configurations. The Structural Similarity Index Measure (SSIM) value stays at 1.0, showing contractual structure preservation, and the Mean Squared Error (MSE) is zero. In a similar vein, the Peak Signal-to-Noise Ratio (PSNR) approaches infinity as no individual pixel distortion occurs. Histogram correlation, GLCM texture features, and deep learning features remained unchanged, confirming that HybridMedPQC is fully image-lossless.

5.2.2 Signature Size Comparison

Table 8: Signature Size — Base Paper vs HybridMedPQC (Projected)

Configuration	Inner Size	Outer Size	Total	vs Base SPHINCS+ (16 KB)
Base: SPHINCS+ only	16,384 B	—	16,384 B	Baseline
Base: Dilithium only	2,420 B	—	2,420 B	-85.2%
Base: Falcon only	666 B	—	666 B	-95.9%
Hybrid: Critical	16,384 B (SPHINCS+)	2,420 B (Dilithium3)	18,804 B	+14.8% but dual-algorithm protected
Hybrid: Sensitive	2,420 B (Dilithium3)	666 B (Falcon-512)	3,086 B	-81.2%
Hybrid: Standard	666 B (Falcon-512)	666 B (Falcon-512)	1,332 B	-91.9%

In Table 8, we show the signature size of each post-quantum algorithm compared to our proposed HybridMedPQC options. The SPHINCS+ scheme has a very large signature size due to its hash-based tree structure, whereas Falcon and Dilithium have much smaller signatures. First, the hybrid framework introduces dual-layer signatures only for important images to enhance long-term security, with a slight increase in signature size. The hybrid configuration across sensitive and standard tiers reduces storage overhead by 91%, suggesting that HybridMedPQC is an optimal choice that balances storage demands and cryptographic resilience.

5.2.3 Execution Time Comparison

Table 9: Execution Time — Base Paper vs HybridMedPQC Projected (1024x1024 image)

Configuration	Signing time (s)	Verification Time (s)	Verification Strategy

Base: SPHINCS+	0.01782	~0.018	Full single-algo
Base: Dilithium	0.02434	~0.008	Full single-algo
Base: Falcon	0.02142	~0.006	Full single-algo
Hybrid: Critical	~0.042	~0.008 (outer only)	Outer-first fast path
Hybrid: Sensitive	~0.028	~0.006 (outer only)	Near-Falcon speed
Hybrid: Standard	~0.022	~0.006	Matches Falcon baseline

Fast Verification Advantage: By prioritizing outer signature (Falcon/Dilithium) verification first, HybridMedPQC achieves near-Falcon verification speeds (<8ms) even for Critical-tier images essential for real-time clinical display workflows while maintaining full SPHINCS+ archival integrity on the inner layer.

Table 9 compares the signing and verification performance of HybridMedPQC with that of pure PQA algorithms. The findings show that signing operations with the hybrid scheme are marginally slower than running individual algorithms, due to the need to generate two signatures. However, because the outer signature is validated before all signatures, verification performance remains low. For critical images, the outer Dilithium signature can be verified in about 8 milliseconds, matching Falcon's baseline performance. This outer-first verification strategy supports clinical image web access without compromising archival security via the inner SPHINCS+ signature.

5.2.4 Computational Complexity

Table 10: Computational Complexity Comparison

Algorithm / Config	**Sign Complexity**	**Verify Complexity**	**Security Basis**
SPHINCS+ (base)	$O(n^2 \log n)$	$O(n^2 \log n)$	Hash function hardness
Dilithium (base)	$O(n^2)$	$O(n^2)$	M-LWE / M-SIS
Falcon (base)	$O(n \log n)$	$O(n \log n)$	NTRU lattice / SIS
Hybrid: Critical	$O(n^2 \log n + n^2)$	$O(n^2)$ outer-first	SPHINCS+ AND Dilithium
Hybrid: Sensitive	$O(n^2 + n \log n)$	$O(n \log n)$ outer-first	Dilithium AND Falcon
Hybrid: Standard	$O(n \log n)$	$O(n \log n)$	Falcon x2

Table 10: Comparison of Computational Complexity of individual PQC Algorithms and the Hybrid Configuration Used in Proposed Framework SPHINCS+ runs longer because of the repeated operations on hash-trees; However, Falcon runs faster by using efficient Fast Fourier Transform-based computations with lattices. Dilithium performs well for polynomial arithmetic over module lattices. In HybridMedPQC, combining two algorithms increases complexity slightly for critical-tier images. But this outer-first verification naturally incurs less runtime overhead for repeated verification calls, enabling efficient processing in a clinical setting.

5.2.5 Security Level Comparison

Table 11: Security Strength

Configuration	**NIST Level**	**Classical Bits**	**Quantum Bits**	**Long-term Archive Safe**
Dilithium2 (base)	Level 2	128	~90	Moderate risk post-2040
Dilithium3 (base)	Level 3	192	~128	Good through 2040+
Falcon-512 (base)	Level 1	128	~90	Moderate risk
SPHINCS+-256 (base)	Level 5	256	~128	Excellent
Hybrid: Critical	Level 5 effective	256+	~128 dual	Excellent — dual algorithm

Hybrid: Sensitive	Level 3	192	~128	Good throug h 2040+
Hybrid: Standard	Level 1-2	128	~90	Adequ ate for de-identifi ed

In Table 11, the security strength of individual post-quantum signature algorithms and HybridMedPQC configurations is compared with respect to NIST security levels and estimated classical and quantum security bits. SPHINCS+ has the highest security level (albeit very high) because it is hash-based, while Dilithium and Falcon offer efficient lattice-based guarantees. For the security images, we are combining SPHINCS+ and Dilithium in a hybrid configuration to give us dual-algorithm protection against both classical and quantum attackers. Sensitive and standard tiers keep the appropriate level of security while alleviating computational and storage overhead.

5.3 Improvement Summary

Summary of Improvements over Roy et al. (2025) Base Paper:

- Signature overhead reduced by up to 91.9% for Standard-tier images vs standalone SPHINCS+
- Verification speed achieves Falcon-level performance (~6-8ms) across all tiers via outer-first fast path
- Defense-in-depth for Critical images: breaking one algorithm does not compromise integrity
- Long-term re-signing protocol extends the security life of archives beyond 2040 without private key access
- Image fidelity metrics remain perfect (SSIM=1.0, MSE=0.0, PSNR=infinity) across all tiers
- Adaptive selection eliminates the one-size-fits-all limitation of the base paper approach
- Context-aware parameterization aligns NIST security levels with actual clinical sensitivity requirements

6. Conclusion

These results indicate that post-quantum integrity for medical imaging does not require a one-size-fits-all approach. The classification of DICOM images into Critical, Sensitive, and Standard tiers, followed by signature selection in accordance with those tiers, allows the framework to marry long-term archival assurance with clinical-speed verification. By relying on an inner PQC signature, the layered design anchors integrity, and by using an outer-first verification path, it speeds up common checks while adding RFC3161 timestamps to improve non-repudiation and provenance. Relative to single-algorithm baselines, projected results indicate significant storage savings in the Sensitive and Standard tiers (up to 81.2% and 91.9% reductions over SPHINCS+), near-Falcon verification latency (~6–8 msec), and perfect preservation of pixel quality (SSIM=1, MSE=0). For Critical studies, the SPHINCS+–Dilithium pairing provides NIST Level-5 defense-in-depth with scheduled re-signing, ensuring long-term verifiability in clinical archives that outlast the lifetimes of typed algorithms. Future work will involve hospital-scale deployment, formal threat modeling, and optimized hardware acceleration for real-time PACS integration.

References

1. 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.
2. L. He et al., "A Post-Quantum Blockchain and Autonomous AI-Enabled Scheme for Secure Healthcare Information Exchange," in IEEE Journal of Biomedical and Health Informatics, vol. 29, no. 9, pp. 6883-6891, Sept. 2025,
3. B. Bera, S. Nandi, A. Kumar Das and B. Sikdar, "Healthcare Security: Post-Quantum Continuous Authentication With Behavioral Biometrics Using Vector Similarity Search," in *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 1597-1612, 2025
4. K. B. A. Kumar, L. S. Mohith, K. Jain, P. Krishnan, N. Venkatachalam and R. Buyya, "Post-Quantum Cryptography-Based Multimedia Encryption Communication Scheme in IoT Consumer Electronics," in *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 4995-5006, May 2025
5. M. C. Kasapbaşi, "A New Chaotic Image Steganography Technique Based on Huffman Compression of Turkish Texts and Fractal Encryption With Post-Quantum Security," in *IEEE Access*, vol. 7, pp. 148495-148510, 2019
6. Z. Man, Z. Yu, J. Yu, C. Gao and X. Meng, "Edge Computing in Internet of Things: Lattice-Based

and Split Encryption for Post-Quantum Data Security," in *IEEE Internet of Things Journal*, vol. 12, no. 23, pp. 49327-49339, 1 Dec.1, 2025

7. S. O. Hwang, H. M. Waseem and N. Munir, "Billiard Quantum Chaos: A Pioneering Image Encryption Scheme in the Post-Quantum Era," in *IEEE Access*, vol. 12, pp. 85150-85164, 2024
8. A. A. A. El-Latif and B. Abd-El-Atty, "Adaptive Particle Swarm Optimization With Quantum-Inspired Quantum Walks for Robust Image Security," in *IEEE Access*, vol. 11, pp. 71143-71153, 2023
9. A. Ahmad and S. Jagatheswari, "PQ-ABS: Post-Quantum Aggregate Blind Signature-Based Anonymous Authentication for Blockchain-Enabled IoMT," in IEEE Transactions on Information Forensics and Security, vol. 21, pp. 1542-1551, 2026
10. S. Xu, X. Chen, Y. Guo, S. -M. Yiu, S. Gao and B. Xiao, "Efficient and Secure Post-Quantum Certificateless Signcryption With Linkability for IoMT," in *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 1119-1134, 2025
11. P. Duong-Ngoc, T. N. Tan and H. Lee, "Efficient NewHope Cryptography Based Facial Security System on a GPU," in *IEEE Access*, vol. 8, pp. 108158-108168, 2020
12. K. S. Roy, S. Singh, M. Kumar, R. Kumar, M. Hassan and R. A. Hazarika, "QSMIT: A Quantum Secure Medical Image Transmission Using Sphincs+ With DICOM," in *IEEE Transactions on Consumer Electronics*, vol. 71, no. 4, pp. 10152-10159, Nov. 2025
13. M. Shahbaz Khan *et al*., "Chaotic Quantum Encryption to Secure Image Data in Post Quantum Consumer Technology," in *IEEE Transactions on Consumer Electronics*, vol. 70, no. 4, pp. 7087-7101, Nov. 2024
14. S. Sun, R. Zhang and H. Ma, "Efficient Parallelism of Post-Quantum Signature Scheme SPHINCS," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, no. 11, pp. 2542-2555, 1 Nov. 2020
15. Shreeya, K. N., Subburaj, B., Saketh, K. S. G., Padmavathy, T. V., Alphonse, S., & Subramanian, G. (2026). A quantum-resilient deepfake detection framework using enhanced ResNet and post-quantum cryptography defense. *Scientific Reports*.
16. Gupta, S., Hariprasad, Y., Iyengar, S. S., Gurappa, S., & Mohanty, P. (2026). Enhancing Digital Security: A Novel Dual-Paradigm Approach for Robust Deepfake Detection Using Pre and Post Quantum-Trained Neural Networks. *Digital Threats: Research and Practice*.
17. Shandilya, S. K., Ganguli, C., Kumar, A., Izonin, I., & Gregus, M. (2026). Post-Quantum Cryptography and Nature-Inspired Cyber Defense: Strategic Readiness and Adaptive Techniques for Next-Gen Threat Response. *IEEE Access*.
18. Salunke, B. A., & Salunke, S. (2026). Hybrid Image Encryption Using LWE-Based Post-Quantum Key Encapsulation and Chaos-Based Symmetric Encryption. *Journal of Computing & Biomedical Informatics*, *10*(02).
19. Ricchizzi, N., Alig, P., Schmitz, N., & Pelzl, J. (2026). When classical encryption fails: A non-invasive post-quantum security layer for medical image transfers. *Informatics in Medicine Unlocked*, 101747.
20. Shirisha, N., Manoj, H. M., Hussain, S. J., Kotoju, R., Kolikipogu, R., & Mohan, A. (2026). Post-quantum security framework for resource-constrained systems: emerging trends, challenges, sustainability, and future directions. *Discover Computing*, *29*(1), 85.
21. Alkhatib, M. (2026). Performance Evaluation of NIST-Standardized Post-Quantum and Symmetric Ciphers for Mitigating Deepfakes. *Cryptography*, *10*(2), 15.
22. Iqbal, M. S., Sajid, A., & Malik, R. (2025). Cyber Security in the Post Quantum Computer Era: Threats and Perspectives. In *Emerging Trends in Information System Security Using AI & Data Science for Next-Generation Cyber Analytics* (pp. 15-29). Cham: Springer Nature Switzerland.
23. Rahman, H., Debnath, P., Jawad, M. N., Rahman, R., & Mahdy, M. R. C. (2026). Quantum-Enhanced Chaotic Encryption on FPGA: A Path to Physical-Layer Post-Quantum Security. *SN Computer Science*, *7*(2), 170.
24. Bitzer, S., Hassanpour, S., Karl, P., Ritterhoff, S., Schaefer, R. F., Sigl, G., ... & Wachter-Zeh, A. (2026). Security and post-quantum cryptography in 6G. In *6G-life* (pp. 443-466). Academic Press.