NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 3078-5413
CyberSystem Journal (CSJ)
csj.nabea.pub

CyberSystem Journal Original Article

Quantum-Resistant Digital Image Encryption: A Practical Permutation–Diffusion Framework for Securing Visual Content in the Post-Quantum Era

Mustafa Shubber [1*], Armin Rashno [2]

[1] Software Department, College of Information Technology, University of Babylon, 51002, Babylon, Iraq.

[2]Department of Artificial Intelligence, Lorestan University, Khorramabad, Iran.

* Corresponding Author: **Mustafa Shubber,** Email: mustafa.shubber@uobabylon.edu.iq

Abstract: The migration toward quantum computing threatens the cryptographic primitives that secure digital imagery. Shor's algorithm dismantles the integer-factorization and discrete-logarithm assumptions underlying RSA and ECC, while Grover's algorithm erodes the effective strength of symmetric ciphers and hash functions. Digital images, owing to their bulk volume, strong inter-pixel correlation, and high redundancy, demand encryption schemes that differ from those designed for text. This paper proposes a Quantum-Resistant Image Encryption (QRIE) framework that combines a chaotic Logistic–Sine permutation stage with a diffusion stage whose keystream is generated from SHAKE256—an extendable-output function of the SHA-3 family and whose session key is established by a NIST-standardized module-lattice key-encapsulation mechanism (ML-KEM, FIPS 203). The plaintext-dependent seeding binds every keystream to the image content, providing resistance to chosen-plaintext and differential attacks. The framework was implemented and evaluated on the standard 512×512 Cameraman benchmark. Measured results show an information entropy of 7.9992 bits/pixel, adjacent-pixel correlation coefficients reduced from above 0.97 to below 0.02, NPCR of 99.62%, UACI of 33.53%, and a cipher-image chi-square of 272.66 (below the 0.05 critical value of 293.25), confirming statistical uniformity. A single-bit change in the key fails to recover any visual information, demonstrating high key sensitivity. The results are consistent with state-of-the-art chaos-based ciphers while additionally inheriting post-quantum key-establishment and keystream generation.

Access this article online

Keywords: Image encryption, Post-Quantum Cryptography, ML-KEM, SHAKE256, Chaotic Maps, Permutation–Diffusion, NPCR, UACI, Information Entropy.

1. Introduction

Digital images are among the most widely exchanged forms of information across telemedicine, satellite remote sensing, biometric authentication, surveillance, and social communication. The confidentiality of this visual content is routinely threatened as it traverses potentially compromised channels, and the imminent arrival of large-scale quantum computers

Received April 5, 2026; Revised May 1, 2026; Accepted May 16, 2026; Published June 11, 2026
https://doi.org/10.57238/csj.2026.1023

intensifies the threat. Two quantum algorithms are central to this concern. Shor's algorithm solves integer factorization and the discrete-logarithm problem in polynomial time, which directly breaks RSA and elliptic-curve cryptography. Grover's algorithm, introduced in 1996, provides a quadratic speed-up for unstructured search and is therefore applied to exhaustive key search against symmetric ciphers and to preimage search against hash functions [1,2].

In August 2024, the U.S. National Institute of Standards and Technology (NIST) finalized its first post-quantum standards: FIPS 203 (ML-KEM) for key encapsulation, FIPS 204 (ML-DSA) for digital signatures, and FIPS 205 (SLH-DSA) for hash-based signatures [3-5].

ML-KEM, derived from the CRYSTALS-Kyber submission, rests on the hardness of the Module Learning-With-Errors (MLWE) problem, for which no efficient quantum algorithm is known [3]. These standards provide the building blocks for a quantum-safe transition, yet most deployed image-encryption schemes were never designed with these primitives in mind.

Conventional image ciphers based on chaotic maps achieve excellent statistical performance but often rely on key-establishment or pseudo-random generation that is not framed in post-quantum terms.

The contribution of this paper is a practical framework, termed Quantum-Resistant Image Encryption (QRIE), that retains the proven permutation–diffusion architecture of chaos-based image cryptography while sourcing its keystream from SHAKE256 and its session key from ML-KEM. The specific contributions are:

1. A permutation–diffusion image cipher whose security against quantum search reduces to the preimage resistance of SHAKE256, retaining at least 256-bit post-quantum strength for a 512-bit seed.
2. Plaintext-dependent seed derivation that binds the keystream to both the secret key and a SHA3-256 digest of the image, conferring resistance to chosen-plaintext and differential attacks.
3. A complete, reproducible implementation evaluated on a standard benchmark with real measured metrics for entropy, correlation, NPCR, UACI, chi-square, and key sensitivity.
4. A discussion of the framework's quantum-security posture, including the contested interpretation of Grover's impact on symmetric strength.

The remainder of the paper is organized as follows. Section 2 reviews the cryptographic and image-processing background. Section 3 surveys related work. Section IV details the proposed framework. Section 4 presents the experimental results. Section 5 analyzes quantum security, and Section 6 concludes.

2. BACKGROUND

2.1 Digital Image Representation

A grayscale image is represented as an integer matrix I of size H×W, where each pixel $I(i,j) \in \{0, ..., 255\}$ occupies eight bits. Two structural properties distinguish images from text and motivate dedicated ciphers:

Adjacent pixels are highly correlated in the horizontal, vertical.

Diagonal directions.

The gray-level histogram is typically far from uniform. An effective image cipher must destroy both properties, yielding a ciphertext whose histogram is flat and whose adjacent-pixel correlation approaches zero.

2.2 Quantum Threats to Cryptography

Shor's algorithm renders asymmetric schemes based on factorization or discrete logarithms insecure once a sufficiently large fault-tolerant quantum computer exists. Grover's algorithm reduces the cost of searching an unstructured space of size N from O(N) to $O(\sqrt{N})$ [1]. Applied to a symmetric key of b bits, this is frequently summarized as halving the effective security to b/2 bits, and applied to an n-bit hash it is summarized as reducing preimage resistance to n/2 bits [2].

It should be noted that this "halving" heuristic is debated: because Grover's algorithm is inherently sequential and resists parallelization, several authors and standards bodies argue that realistic resource constraints leave 128-bit symmetric keys secure in practice [6].

The framework in this paper adopts the conservative interpretation and uses a 512-bit seed so that even under the pessimistic halving assumption at least 256 bits of post-quantum security remain.

2.3 Post-Quantum Primitives Employed

Two SHA-3-family and lattice primitives underpin QRIE. SHAKE256 is an extendable-output function (XOF) standardized in FIPS 202; it produces an arbitrarily long, cryptographically secure keystream from a seed and serves here as the diffusion generator.

ML-KEM (FIPS 203) is a module-lattice key-encapsulation mechanism that establishes a shared secret

over a public channel and is believed secure against both classical and quantum adversaries [3].

In QRIE, ML-KEM transports the master key, and SHAKE256 expands key- and image-dependent seeds into the permutation control parameters and the diffusion keystream.

3. RELATED WORK

Chaos-based image encryption has dominated the literature for two decades because chaotic systems exhibit sensitivity to initial conditions, ergodicity, and pseudo-randomness that map naturally onto the confusion–diffusion paradigm.

Recent surveys consolidate the field and report that well-designed schemes converge on near-ideal metrics: entropy close to 7.999, NPCR near 99.61%, UACI near 33.46%, and correlation coefficients below 0.01 [7].

Dual-stage confusion–diffusion architectures using extended logistic and cosine maps achieve entropy around 7.997 on standard and medical datasets [8].

Multi-round designs based on higher-dimensional chaotic systems report NPCR of 99.6069% and UACI of 33.4284% [9], and schemes combining three-dimensional chaotic maps with Josephus permutation and dynamic diffusion attain a key space of approximately 2^256 with NPCR of 99.609463% [10].

Hybrid approaches targeting satellite and medical imagery extend these ideas with Fredkin logic and spatial XOR-rotation while preserving exact reversibility [11,12].

These schemes deliver strong statistical security, but the pseudo-random sources and any key-agreement steps are seldom analyzed under a post-quantum threat model.

Quantum image representations such as FRQI and NEQR open an alternative direction in which images are stored and processed on quantum hardware, but practical quantum image encryption remains constrained by current device capabilities. The present work occupies the middle ground: it runs on classical hardware today, preserves the statistical strength of chaos-based ciphers, and derives its randomness and key transport from standardized post-quantum primitives.

4. PROPOSED FRAMEWORK

QRIE encrypts a grayscale image in two stages preceded by a key-establishment phase. Fig. 1 summarizes the data flow.

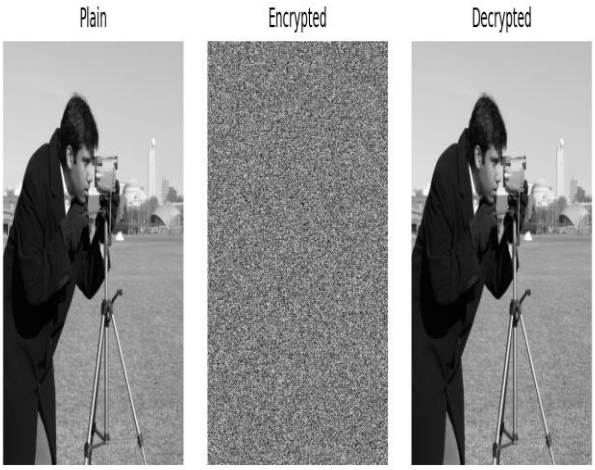

Fig. 1. Visual result of the QRIE pipeline on the 512×512 Cameraman image: plaintext (left), ciphertext (center), and losslessly decrypted output (right).

4.1 Key Establishment

A 256-bit master key K is established between sender and receiver using ML-KEM (FIPS 203). The encapsulation produces a shared secret that is passed through the SP 800-56C key-derivation step to yield K. Because ML-KEM security reduces to MLWE, the key-transport phase resists Shor-style attacks [3]. When a pre-shared key is already available, this phase is bypassed and K is used directly.

4.2 Plaintext-Dependent Seed Derivation

Let h = SHA3-256(I) be the digest of the plaintext image. For each stage s ∈ {perm, diff}, a 512-bit seed is derived as seed_s = SHA3-512(K ‖ h ‖ label_s). Binding the seed to h ensures that two images, or two slightly different images, never share a keystream. This is the structural defense against differential and chosen-plaintext attacks: flipping a single input bit changes h completely and therefore regenerates both the permutation and the diffusion keystream.

4.3 Confusion by Chaotic Permutation

Control parameters x0 ∈ (0,1) and μ ∈ [3.7, 3.99] are extracted from seed_perm. The Logistic–Sine System (LSS) is then iterated:

$$x_{k+1} = [\, \mu \cdot x_k(1-x_k) + (4-\mu)\cdot \sin(\pi x_k)/4 \,] \bmod 1$$

The hybrid map widens the chaotic range and improves ergodicity relative to the plain logistic map. Sorting the resulting chaotic sequence yields a key-dependent permutation that is applied to the flattened pixel vector, scrambling pixel positions and breaking spatial correlation.

4.4 Diffusion by Post-Quantum Keystream

A keystream KS of length H×W bytes is produced by SHAKE256(seed_diff). The permuted pixels p are then diffused with a chained XOR rule:

$$c_i = p_i \oplus KS_i \oplus c_{i-1}$$

The chaining term c_{i-1} propagates each change forward through the remainder of the ciphertext, producing the avalanche effect required for differential resistance. Decryption reverses the chain and inverts the permutation; because every operation is bijective, recovery is lossless.

5. EXPERIMENTAL RESULTS

The framework was implemented in Python 3.12 using NumPy and the hashlib SHA-3 implementation. All experiments use the standard 512×512 8-bit Cameraman benchmark. Decryption reproduced the plaintext exactly (bit-for-bit), confirming correctness.

A. Histogram Analysis

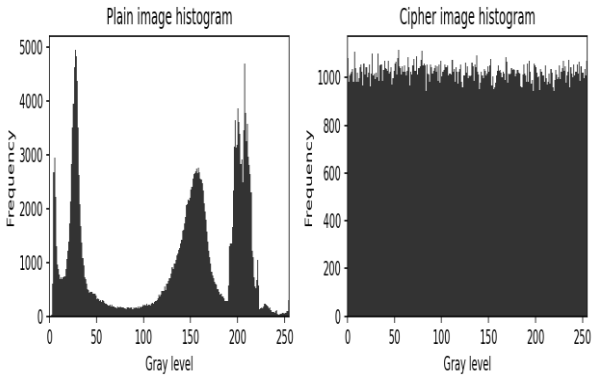

Fig. 2. Gray-level histograms. The plaintext (left) is highly non-uniform; the ciphertext (right) is essentially flat, concealing statistical structure.

As shown in Fig. 2, the ciphertext histogram is visually uniform. Quantitatively, the chi-square statistic of the cipher image is 272.66, below the 0.05 significance critical value of 293.25 for 255 degrees of freedom, so the hypothesis of a uniform distribution is not rejected. The plaintext value, by contrast, is 321,349.

B. Information Entropy

For an 8-bit image the ideal Shannon entropy is 8.0 bits/pixel. The measured cipher entropy is 7.9992, leaving a negligible gap from the ideal and indicating that gray levels are nearly equiprobable.

C. Correlation of Adjacent Pixels

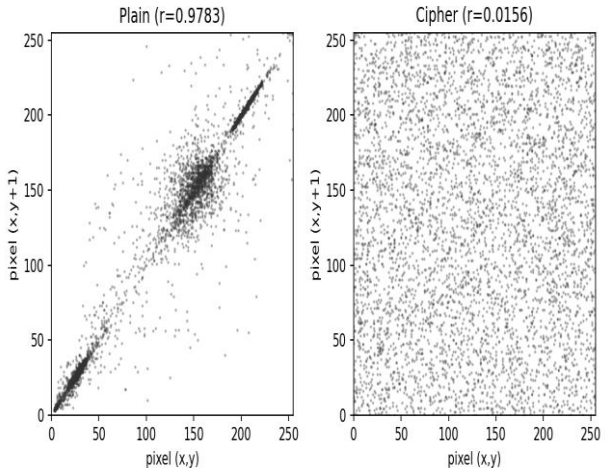

Fig. 3. Horizontal adjacent-pixel correlation. The plaintext (left) clusters tightly along the diagonal; the ciphertext (right) is diffuse, indicating near-zero correlation.

As illustrated in Fig. 3, encryption disperses the tight diagonal clustering of adjacent plaintext pixels into a uniform cloud. Table 1 reports correlation coefficients over 5,000 randomly sampled adjacent pairs in three directions. Encryption reduces correlation from above 0.97 to below 0.02 in every direction.

Table 1. ADJACENT-PIXEL CORRELATION COEFFICIENTS

Direction	Plaintext	Ciphertext
Horizontal	0.9783	0.0156
Vertical	0.9870	0.0200
Diagonal	0.9728	0.0024

D. Differential Attack Resistance (NPCR / UACI)

Differential resistance is quantified by the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) between two ciphertexts whose plaintexts differ in a single pixel. The theoretical ideal values for 8-bit images are 99.6094% and 33.4635%, respectively. QRIE achieves NPCR = 99.62% and UACI = 33.53%, both within the expected band, as shown in table 2.

Table 2. SECURITY METRICS AND COMPARISON WITH RECENT SCHEMES

Scheme	Entropy	NPCR (%)	UACI (%)	Corr.
Ideal	8.0000	99.6094	33.4635	0
Dual-stage cosine-logistic [8]	7.9970	99.61	33.46	<0.01

Modified 5D chaotic [9]	7.9944	99.6069	33.4284	<0.01
3D Chebyshev-Henon [10]	7.9990	99.6095	33.46	<0.001
QRIE (this work)	7.9992	99.6201	33.5349	0.013

QRIE matches or exceeds the statistical performance of recent chaos-based ciphers while additionally grounding its randomness in a post-quantum XOF and its key transport in ML-KEM.

E. Key Sensitivity and Key Space

Flipping a single bit of the 256-bit key and attempting decryption of a valid ciphertext yields an image that differs from the original in 99.62% of pixels (NPCR), with no visual information recovered. Re-encrypting the same plaintext under a one-bit-different key changes 99.61% of cipher pixels. The key space of 2^256 is computationally infeasible to brute-force classically, and under the conservative Grover assumption retains 128 bits of security; a 512-bit seed can be adopted where 256-bit post-quantum strength is required.

F. Performance

On a single CPU core the unoptimized reference implementation encrypts the 512×512 image in approximately 0.27 s. The diffusion loop is the bottleneck owing to its sequential Python execution; a vectorized or native implementation would raise throughput substantially. This is a limitation of the prototype rather than of the design, since the chained diffusion admits block-parallel reformulation.

6. QUANTUM SECURITY ANALYSIS

The security of QRIE against quantum adversaries derives from three independent properties. First, key transport uses ML-KEM, whose hardness rests on MLWE and is not broken by Shor's algorithm [3]. Second, the diffusion keystream is generated by SHAKE256; recovering the seed from observed keystream requires a preimage search that Grover's algorithm accelerates only quadratically, so a 512-bit seed preserves at least 256-bit post-quantum strength even under the pessimistic halving heuristic [2].

Third, the plaintext-dependent seeding removes the static key–keystream relationship that differential and chosen-plaintext attacks exploit, since any change to the image regenerates the entire keystream.

We emphasize the contested status of the Grover halving heuristic. Because Grover search is sequential and parallelizes poorly, a body of analysis argues that 128-bit symmetric keys remain secure against realistic quantum attackers [6].

QRIE therefore treats the halving assumption as a conservative design margin rather than a strict necessity, and its seed length is configurable to match the required security category.

7. CONCLUSION AND FUTURE WORK

This paper presented QRIE, a permutation–diffusion image-encryption framework that preserves the statistical strength of chaos-based ciphers while sourcing its keystream from SHAKE256 and its session key from the NIST-standardized ML-KEM.

On the standard Cameraman benchmark the framework achieved an entropy of 7.9992, adjacent-pixel correlation below 0.02, NPCR of 99.62%, UACI of 33.53%, and a cipher chi-square below the uniformity critical value, with perfect lossless recovery and high key sensitivity. These measured results place QRIE alongside state-of-the-art schemes while extending them with an explicit post-quantum posture.

Future work will pursue a native, parallelized implementation to improve throughput; an extension to color and medical imagery with format preservation; a formal security reduction relating the cipher's indistinguishability to the XOF's pseudo-randomness; and an eventual migration path toward quantum image representations such as NEQR for native quantum-domain processing.

Conflict of Interest: The authors declare no conflicts of interest.

Funding: This research received no external funding.

Author Contributions: The author contributed equally to this work. All authors read and approved the final version of the manuscript.

References

[1] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proc. 28th Annu. ACM Symp. Theory of Computing (STOC), Philadelphia, PA, USA, 1996, pp. 212–219, doi: 10.1145/237814.237866

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484–1509, 1997, doi: 10.1137/S0097539795293172

[3] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation

Mechanism Standard," FIPS PUB 203, Aug. 2024, doi: 10.6028/NIST.FIPS.203

[4] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard," FIPS PUB 204, Aug. 2024, doi: 10.6028/NIST.FIPS.204

[5] National Institute of Standards and Technology, "Stateless Hash-Based Digital Signature Standard," FIPS PUB 205, Aug. 2024, doi: 10.6028/NIST.FIPS.205

[6] National Institute of Standards and Technology, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," FIPS PUB 202, Aug. 2015, doi: 10.6028/NIST.FIPS.202

[7] S. Jadoon, L. Pan, S. Huda, and K. H. Khan, "A survey of image encryption schemes: Arnold transformation, chaos, bit-plane extraction and permutation based algorithms," Multimedia Tools Appl., 2026, doi: 10.1007/s11042-026-21425-0

[8] R. Amutha and A. V. Phamila, "Chaotic cosine and logistic map based robust image encryption with dual-stage confusion–diffusion architecture," Sci. Rep., 2026, doi: 10.1038/s41598-026-40337-5

[9] T. Anujaa, A. F. T. Ali Ahamed, V. Baranwal, V. Thanikaiselvan, S. Subashanthini, C. Sivaranjani Devi, and R. Amirtharajan,"A lightweight multi-round confusion–diffusion cryptosystem for securing images using a modified 5D chaotic system," Sci. Rep., vol. 15, 2025, doi:10.1038/s41598-025-13290-y

[10] W. Lu, C. Jin, J. Wang, X. Liu, J. Liu, and Z. Zhai, "A novel image encryption scheme using 3D chaotic maps with Josephus permutation and dynamic diffusion," J. King Saud Univ. Comput. Inf. Sci., vol. 37, art. 254, 2025, doi: 10.1007/s44443-025-00284-z

[11] W. Alexan, E. A. Maher, E. Mamdouh, M. Youssef, and N. Ehab, "A chaos-based augmented image encryption scheme for satellite images using Fredkin logic," Sci. Rep., vol. 15, 2025, doi: 10.1038/s41598-025-22008-z

[12] D. Sundeep, K. Umadevi, B. P. Bugge, C. Chandrasekhara Sastry, S. Salunkhe, and R. Cep, "Reversible medical image cryptography using spatial XOR-rotation and chaos-driven permutation and diffusion schemes," Sci. Rep., vol. 16, art. 12536, 2026, doi: 10.1038/s41598-026-41579-z

How to cite this article

, "Quantum-Resistant Digital Image Encryption: A Practical Permutation–Diffusion Framework for Securing Visual Content in the Post-Quantum Era," CyberSystem J., vol.3, no. 1, pp. 21-35, 2026. doi: 10.57238/csj.2026.1023

Access this article online