Robust Data Security via Frequency-Domain Steganography and Post-Quantum Cryptography.

Nischal V Pattedar
Department of Computer Science and Engineering,
Amrita School of Computing, Bengaluru,
Amrita Vishwa Vidyapeetham, India
bl.en.u4aie23021@bl.students.amrita.edu

Punav Anirudh Potluri
Department of Computer Science and Engineering,
Amrita School of Computing, Bengaluru,
Amrita Vishwa Vidyapeetham, India
bl.en.u4aie23025@bl.students.amrita.edu

Raunak Choudhury
Department of Computer Science and Engineering,
Amrita School of Computing, Bengaluru,
Amrita Vishwa Vidyapeetham, India
bl.en.u4aie23027@bl.students.amrita.edu

Gokul Shyam Lankoti
Department of Computer Science and Engineering,
Amrita School of Computing, Bengaluru,
Amrita Vishwa Vidyapeetham, India
bl.en.u4aie23015@bl.students.amrita.edu

***Abstract*—This research introduces a defense-in-depth security architecture by combining the secretive character of spectral steganography with the mathematical precision of post-quantum encryption. Fundamentally, this system will make use of a content-aware encryption engine that should carry out Shannon entropy analysis for the discriminative application of AES-256 on the high-sensitivity data while protecting session keys using the NIST-standardized lattice-based Kyber768 algorithm for any future quantum-computational threat resistance. After that, the retrieved ciphertext is divided up and covertly inserted into the host image's frequency domain using DCT coefficients in the Red, Green, and Blue channels. This process is known as split-payload orchestration. Texture-Adaptive Masking prioritizes areas with high texture in order to maximize imperceptibility, while Sparse Randomized Sampling distributes the data in a non-linear, keyed sequence, creating a communication channel that is both visually and mathematically indistinguishable from regular media.**

I. Literature Survey

Achieving an ideal balance between computing efficiency, resilience against sophisticated adversaries, and preservation of perceptual quality is becoming more and more important in recent developments in multimedia security. Conventional encryption and steganography methods are becoming inadequate due to the quick adoption of deep learning-based analysis tools and the impending threat of quantum computing. As a result, current research focuses on generative steganography, adversarial resilience, content-aware security, and hybrid cryptographic systems.

A. Content-Aware and Adaptive Encryption

In video encoding, conventional selective encryption methods frequently provide consistent protection across frames, which results in needless processing complexity and predictable statistical distortions. Sheng et al. [1] developed a content-aware selective encryption framework for H.265/HEVC that gives semantically sensitive video segments priority in order to overcome this restriction. Their technique uses a deep hashing network based on Central Similarity Quantization to selectively encrypt only sensitive Groups of Pictures (GOPs), like those that involve human beings. Coefficient-level obfuscation and hyper-chaotic Lorenz systems increase encryption even more. Semantic awareness greatly increases efficiency while preserving resilience against format-compliance and cryptanalytic attacks, according to experimental findings. This study emphasizes how intelligent, adaptive encryption techniques are becoming more and more important compared to static ones.

B. Robust and Adversarial Image Steganography

While adaptive encryption increases efficiency, secure covert communication is still vulnerable to current steganalysis, notably CNN-based detectors. To address this issue, Wang et al. [2] suggested an adversarial picture steganography technique that specifically targets deep learning-based steganalyzers. Their method clusters nearby pixels' modification directions based on gradient feedback from a target steganalyzer, retaining local pixel correlations and simulating natural image statistics. This methodology outperforms previous adversarial embedding approaches against both CNN-based and classic feature-based detectors. In addition to adversarial embedding, Zhang et al. [6] investigated the resilience of batch image steganography for online social networks. Their Multi-Stega approach reduces cumulative embedding artifacts across several JPEG images rather than treating each carrier separately. By integrating an embedding sign metric and dynamic payload allocation, the system greatly enhances detection resistance in lossy compression conditions common on real-world platforms. Huang et al. [10] investigated robustness against JPEG recompression using DCT Residual Modulation. By stabilizing quantized DCT coefficients and using error-dispersive Reed-Solomon coding, their technique achieves decreased bit error rates while preserving excellent anti-steganalysis properties. These investigations demonstrate a move from isolated embedding to statistically optimized, channel-aware steganography.

C. Lightweight and Contrast-Based Steganography

Despite their efficiency, deep learning-based algorithms have a significant computational cost that limits their practical application. To address this issue, Jamatia and Bhuyan [8] suggested a contrast-channel embedding method that uses deterministic contrast analysis instead of learning-based models. Their strategy improves imperceptibility while remaining simple by selecting embedding data in mid-range and severe contrast regions using dual-thresholding. This lightweight architecture provides a feasible alternative for real-time and resource-constrained applications, but its adaptability to advanced detectors is limited.

D. Generative and Provably Secure Steganography

Moving beyond modification-based approaches, Wang et al. [3] proposed SparSamp, a secure steganographic system that embeds messages during the construction of deep generative models. By utilizing sparse sampling without changing the underlying probability distribution, the approach achieves stringent theoretical security guarantees while preserving fast embedding speed. Similarly, Qasaimeh et al. [9] introduced a coverless steganography strategy based on GANs and compressive autoencoders, which dramatically increased embedding capacity and robustness. However, generative approaches frequently have large processing needs and sophisticated inversion operations, which limits their scalability.

E. Steganalysis and Adversarial Vulnerabilities

Steganographic techniques evolve, and so do detection strategies. Wei et al. [11] presented CTNet, a hybrid CNN-Transformer architecture that captures both local and global embedding artifacts, resulting in state-of-the-art detection accuracy for color image steganography. Kim et al. [12] showed that even advanced steganalysis algorithms are vulnerable to adversarial cases, highlighting significant trade-offs between detection accuracy and visual imperceptibility. These findings point to an increasing arms race between data concealing and detecting technologies.

F. Cryptographic Robustness and Post-Quantum Security

Beyond steganography, microarchitectural side channels and quantum computing are posing new challenges to cryptographic resilience. Barthe et al. [4] discovered that future processor improvements may cause significant leakage even in constant-time encryption schemes. Similarly, Du et al. [13] showed effective side-channel attacks on masked CRYSTALS-Kyber implementations, highlighting the vulnerability of ”pure” post-quantum deployments. Hybrid cryptographic frameworks have grown in popularity as a means of improving efficiency and resilience. Selvi and Sakthivel [14] demonstrated the efficacy of ECC-AES hybrid encryption for cloud security, whereas Hanna et al. [15] conducted comprehensive benchmarking of PQC algorithms on IoT devices, highlighting the importance of selected and optimized deployment. Recent research have extended this paradigm by investigating lattice-based cryptography for safe multi-cloud storage [16] and evaluating PQC performance across heterogeneous environments [17], highlighting the importance of cryptographic adaptability.

G. Secret Sharing and Distributed Security

Distributed security mechanisms improve fault tolerance. Xiong et al. [7] introduced a secure secret image sharing technique based on polynomial k-consistency that protects against noise, manipulation, and cropping attacks. Similarly, JPEG-integrated secret sharing techniques [18] ensure format compliance while reducing key management issues. These ideas highlight the benefits of distributed systems in reducing single points of failure.

H. Entropy-Optimized Encryption and the Emergence of Post-Quantum Cryptography

Recent research emphasizes both near-term breakthroughs in cryptography optimization and the long-term disruption posed by quantum computing. Stoycheva et al. [19] present an entropy-driven chaotic picture encryption strategy in which the parameters of a third-order Lorenz system are tuned to maximize Shannon entropy, which approaches the optimal value of 8. By incorporating AI-assisted initialization into a modified Price’s algorithm, the authors show faster convergence and superior security metrics, such as near-perfect entropy and negligible pixel correlation, demonstrating the efficacy of intelligent optimization in complex, non-linear cryptographic environments. In contrast, Gitonga et al. [20] investigate the macro-level consequences of quantum computing on cryptographic systems, demonstrating through simulation that widely used conventional techniques such as RSA-2048 and ECC-256 are significantly vulnerable to Shor’s algorithm. Their comparative research of post-quantum options indicates CRYSTALS-Kyber as a viable balance of performance and security, while hybrid classical-post-quantum schemes are suggested as a pragmatic transitional technique toward quantum-resilient encryption.

Synthesizing the examined literature highlights three key research needs. First, static and blind encryption or embedding techniques fail to account for semantic relevance and entropy fluctuations, resulting in inefficiencies and discernible patterns. Second, monolithic steganographic systems, whether modification-based or generative, are sensitive to modern Transformer-based detectors and have no fault tolerance when partially compromised. Third, while post-quantum cryptography is critical, current systems have side-channel vulnerabilities and performance limits, necessitating hybrid, adaptive, and distributed security architectures. To address these deficiencies, an integrated system that combines semantic-aware encryption, lightweight adaptive steganography, and cryptographically agile post-quantum security is required.

II. Methodology

The methodology for the proposed post-quantum steganographic framework is executed through a rigorous, four-stage procedural pipeline that integrates information theory, lattice-based cryptography, and spectral domain manipulation to establish a high-fidelity covert channel.

A. Content-Aware Cryptographic Pre-Processing

It all starts with a granular analysis of the input text in order to optimize the cryptographic overhead in relation to the informational density of the data.

1) Shannon Entropy Computation: In order to calculate the Shannon entropy, which measures the text's uncertainty, the system divides the plaintext into discrete tokens.

2) Bi-Fork Encryption Path: Normal entropy levels would follow a Vigenère poly-alphabetic cipher procedure, whereas token values exceeding a threshold value of 2.5 bits/char would avoid an AES-256 engine running in CBC mode.

3) Post-Quantum Key Encapsulation (KEM): The gadget employs the Kyber768 lattice-based methodology for key encapsulation to safeguard the session keys against attacks that could be executed by a computer utilizing techniques similar to those of a quantum computer.

The session keys are encapsulated (”wrapped”) using the receiver's post-quantum public key, ensuring that the key exchange remains mathematically intractable even for future quantum adversaries.

B. Split-Payload Orchestration and Mapping

Next, following the generation of the encrypted ciphertext, the ciphertext undergoes a structural rearrangement in order to organize the data for multi-channel distribution.

1) Payload Partitioning: The ciphertext is now separated into three logical sections: the header, the body, which contains the main message, and the metadata. This is done in order to provide the message structure.

2) Spectral Channel Allocation: To distribute the embedding burden across all channels in the spectral domain and hence avoid detection through statistical analysis, a partition is given one of three channels: Red, Green, or Blue.

C. Discrete Cosine Transform (DCT) Embedding

The physical concealment is performed in the frequency domain of the carrier image by a series of mathematical transformations.

1) Block-Based Transformation: The carrier image is split up into blocks of 8 by 8 pixels, and each block's spatial representation is shifted into a set of frequency coefficients using the Discrete Cosine Transform.

2) Texture-Adaptive Masking (TAM): The system calculates the variance of the DCT coefficients within each block. Blocks having their variance less than 200.0 are marked as ”smooth” and excluded from the embedding process to avoid visible artifacts.

3) Sparse Randomized Sampling: The system distributes the data bits in a non-linear manner over the image by shuffling the block coordinates using the Vigenère key as a deterministic seed.

4) Quantization-Based Embedding: To make the hidden data resistant to lossy compression or minor image processing, the secret bits are implanted by altering specific AC coefficients whose values are quantized to multiples of the persistence factor (20).

D. Recovery and Decapsulation Procedure

The recovery procedure requires a reverse operation of the embedding pipeline to recover the original plaintext message.

1) Seeded Block Reconstruction: The receiver can determine the exact set of textured blocks utilized in the encoding process using the same Vigenère keyword seed.

2) Coefficient Extraction: The quantized parities are converted back to the binary format after the updated AC coefficients for the Red, Green, and Blue channels are retrieved.

3) Post-Quantum Decapsulation: The AES and Vigenère cipher messages can be fully constructed by decrypting them by ”unwrapping” the session keys that are wrapped with the recipient's Kyber private key.

III. Results and Discussion

The suggested steganographic system's testing outcomes confirm that the robust, high-performance communication channel effectively combines post-quantum security with high-fidelity data concealing. Using Vigenère ciphers for common text, procedural analysis of the content-aware encryption phase has demonstrated that the threshold in Shannon entropy at 2.5 bits per character effectively bifurcates the workload so that tokens of high complexity remain protected by AES-256 without computational inefficiency. The Kyber768 lattice-based technique effectively manages the 1184-byte public key overhead needed for NIST Security Level 3 and ensures that the underlying session keys are safe from quantum-computational ”store-now, decrypt-later” tactics. The Discrete Cosine Transform (DCT) is responsible for embedding the data on the Red, Green, and Blue components, and steganographic findings show the effectiveness of the frequency domain approach. However, in order to prevent the embedding process from adding any artifacts to the smoother areas of the images, the Texture-Adaptive Masking technique employed in the process guarantees a 100% imperceptibility level by embedding the information only on the blocks whose variance is higher than 200.0. Additionally, the quantization stage's use of a persistence factor of 20 guarantees that the embedded bits are unaffected by the mathematical rounding mistakes produced during the saving and reconstruction of the images. The impacts of traditional steganalysis are eliminated when the Sparse Randomized Sampling process with a Vigenère key-based deterministic seed is successful in ensuring that the message fragments are randomly dispersed in a non-linear fashion across the carrier. Ultimately, the process confirms the hypothesis that the original message is rigorously traceable to the owner of the associated lattice-based private key, even in the case of a message being split across several spectral channels in a ”Split Unlearning.”

IV. Conclusion

In a post-quantum survival setting, the suggested system effectively implements a robust ”defense-in-depth” solution that bridges the gap between quantization and high-capacity covert channels. This security system guarantees that protected data is mathematically secure against classical or quantum attacks by combining Kyber768 lattice-based key encapsulation techniques with entropy-smart hybrid encryption. The methodical orchestration approach that includes Texture-Adaptive Masking, Sparse, and split-payload embedding in Red, Green, and Blue frequency channels All protected data is guaranteed to be mathematically randomly dispersed in the frequency domain and to be visually undetectable thanks to randomized sampling. Overall, this study demonstrates that these deterministic seeding techniques and frequency-domain quantization stages are a reliable solution that guarantees a survivability solution that safeguards data integrity in its absolute form.

References

[1] Sheng, Qingxin, et al. ‘Content-Aware Selective Encryption for H.265/HEVC Using Deep Hashing Network and Steganography’. ACM Trans. Multimedia Comput. Commun. Appl., vol. 21, no. 1, Association for Computing Machinery, Dec. 2024, https://doi.org/10.1145/3698400.

[2] Wang, Dewang, et al. ‘Enhancing Adversarial Embedding Based Image Steganography via Clustering Modification Directions’. ACM Trans. Multimedia Comput. Commun. Appl., vol. 20, no. 1, Association for Computing Machinery, Sept. 2023, https://doi.org/10.1145/3603377.

[3] Wang, Yaofei, et al. ‘SparSamp: Efficient Provably Secure Steganography Based on Sparse Sampling’. Proceedings of the 34th USENIX Conference on Security Symposium, USENIX Association, 2025.

[4] Barthe, Gilles, et al. ‘Testing Side-Channel Security of Cryptographic Implementations against Future Microarchitectures’. Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery, 2024, pp. 1076–1090, https://doi.org/10.1145/3658644.3670319. CCS 2024.

[5] Jiang, Yanna, et al. ‘Split Unlearning’. Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery, 2025, pp. 948–962, https://doi.org/10.1145/3719027.3744787. CCS 2025.

[6] Zhang, Yi, et al. ‘An Image Robust Batch Steganography Framework with Minimum Embedding Signs’. IEEE Transactions on Information Forensics and Security, vol. 20, Institute of Electrical and Electronics Engineers (IEEE), 2025, pp. 10745–10760, https://doi.org/10.1109/tifs.2025.3615446.

[7] Xiong, Lizhi, et al. ‘Robust Secret Image Sharing Scheme Based on Polynomial k-Consistency’. IEEE Transactions on Circuits and Systems for Video Technology, vol. 35, no. 9, Institute of Electrical and Electronics Engineers (IEEE), Sept. 2025, pp. 8880–8892, https://doi.org/10.1109/tcsvt.2025.3554842.

[8] Jamatia, Rupa, and Bubu Bhuyan. ‘A Contrast-Channel Embedding Approach for Image Steganography: Balancing Capacity and Imperceptibility’. IEEE Access: Practical Innovations, Open Solutions, vol. 13, Institute of Electrical and Electronics Engineers (IEEE), 2025, pp. 180539–180565, https://doi.org/10.1109/access.2025.3618875.

[9] Qasaimeh, Malik, et al. ‘Robust Steganographic Approach Using Generative Adversarial Network and Compressive Autoencoder’. Multimedia Tools and Applications, vol. 84, no. 26, Springer Science and Business Media LLC, Nov. 2024, pp. 31479–31516, https://doi.org/10.1007/s11042-024-20422-5.

[10] Huang, Yingkai, et al. ‘Robust Image Steganography against JPEG Compression Based on DCT Residual Modulation’. Signal Process., vol. 219, no. C, Elsevier North-Holland, Inc., June 2024, https://doi.org/10.1016/j.sigpro.2024.109431.

[11] Wei, Kang-Kang, et al. ‘CTNet: A Convolutional Transformer Network for Color Image Steganalysis’. J. Comput. Sci. Technol., vol. 40, no. 2, Springer-Verlag, May 2025, pp. 413–427, https://doi.org/10.1007/s11390-023-3006-3.

[12] Kim, Hyeonseong, et al. ‘Performance Comparison of Adversarial Example Attacks against CNN-Based Image Steganalysis Models’. Electronics, vol. 14, no. 22, MDPI AG, Nov. 2025, p. 4422, https://doi.org/10.3390/electronics14224422.

[13] Du, Jianfeng, et al. ‘Revisiting the Masking Strategy: A Side-Channel Attack on CRYSTALS-Kyber’. IEEE Transactions on Information Forensics and Security, vol. 20, Institute of Electrical and Electronics Engineers (IEEE), 2025, pp. 3387–3399, https://doi.org/10.1109/tifs.2025.3550061.

[14] Selvi, P., and S. Sakthivel. ‘A Hybrid ECC-AES Encryption Framework for Secure and Efficient Cloud-Based Data Protection’. Scientific Reports, vol. 15, no. 1, Springer Science and Business Media LLC, Aug. 2025, p. 30867, https://doi.org/10.1038/s41598-025-01315-5.

[15] Hanna, Yacoub, et al. ‘A Comprehensive and Realistic Performance Evaluation of Post-Quantum Security for Consumer IoT Devices’. Internet of Things (Amsterdam, Netherlands), vol. 33, no. 101650, Elsevier BV, Sept. 2025, p. 101650, https://doi.org/10.1016/j.iot.2025.101650.

[16] Iyswarya, R., and R. Anitha. ‘Secure Data Storage in Multi-Cloud Environments Using Lattice-Based Saber with Diffie-Hellman Cryptography and Authentication Based on PUF-ECC’. Data Knowledge Engineering, vol. 161, no. 102512, Elsevier BV, Jan. 2026, p. 102512, https://doi.org/10.1016/j.datak.2025.102512.

[17] Abbasi, Maryam, et al. ‘A Practical Performance Benchmark of Post-Quantum Cryptography across Heterogeneous Computing Environments’. Cryptography, vol. 9, no. 2, MDPI AG, May 2025, p. 32, https://doi.org/10.3390/cryptography9020032.

[18] Guan, Yulong, et al. ‘A JPEG Compressed Image Encryption Method Based on Shamir Secret Sharing Scheme’. Cluster Computing, vol. 28, no. 15, Kluwer Academic Publishers, Oct. 2025, https://doi.org/10.1007/s10586-025-05554-z.

[19] Stoycheva, Hristina, and Georgi Mihalev. ‘Entropy-Based Optimization in Chaotic Image Encryption Algorithms with Implementation of Artificial Intelligence’. EEPES 2025, MDPI, 2025, p. 16, https://doi.org/10.3390/engproc2025104016

[20] Gitonga, Charles Kinyua. ‘The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography’. European Journal of Information Technologies and Computer Science, vol. 5, no. 1, European Open Science Publishing, Jan. 2025, pp. 1–10, https://doi.org/10.24018/compute.2025.5.1.146.