RESEARCH ARTICLE

DOI: 10.54646/ijcci.2025.02

International Journal of Computer Communication and Informatics

# Quantum-Chaotic Encryption Integrated DCT-Based Steganography

M. Kalaiselvi [a], R.T. Suganya [a]

[a] Department of Computer Science and Engineering (Cyber Security), Dr. N.G.P. Institute of Technology, Coimbatore, Tamil Nadu, India.

* Corresponding Author: kalaiselvi.m@drngpit.ac.in

Received: 17-06-2025, Revised: 18-11-2025, Accepted: 24-11-2025, Published: 05-12-2025

**Abstract:** Ensuring safe and convenient access to essential services, including pension retrieval, is crucial in the current digital era. Passwords and PINs are examples of traditional authentication systems that frequently expose people to fraud and identity theft. In order to replace these traditional methods with biometric verification (such as fingerprint and facial recognition), this project suggests a Web Biometric Credentialing System for pension retrieval. The system incorporates Auth0 for secure identity and management of sessions and WebAuthn API for biometric authentication. This method greatly enhances security and user experience by enabling pensioners to verify their identity using biometric information. The technology makes sure that only authorized people can access sensitive financial data and, after successful verification, enables pensioners to safely retrieve their pension amounts. By lowering fraud, eliminating unwanted access, and streamlining the authentication procedure, the suggested solution improves security.

**Keywords:** Game Theory, Incentives, Security Economics, Retail Payment Security, MFA, JWT, Auth0 SDK.

## 1. Introduction

Image steganography allows safe and hidden communication by means of the hiding of secret information in digital photos. The most common Least Significant Bit (LSB) method is susceptible to image processing attacks and steganalysis. This work combines Quantum-Chaotic Encryption with DCT-based steganography in an effort to boost its security and offer a safe and hard-to-find way to hide data. A chaotic logistic map and Quantum Random Number Generator (QRNG) generate a random AES-256 key, which is strong against quantum and classical attacks. The encrypted information is stored in the DCT frequency space, which keeps it undetectable and robust against compression, noise, and modifications.

This technique employs quantum entropy, chaotic key diffusion, and frequency-domain embedding to provide improved security, strength, and resistance to steganalysis. This renders it most appropriate for post-quantum secure communication, copyright protection, and digital watermarking.

## 2. Problem Statement

Conventional LSB-based steganography is highly vulnerable to steganalysis, compression, and image alteration and therefore not secure for covert communication. Further, symmetric encryption protocols such as AES and DES may even become vulnerable in the future due to advances in quantum computing.

This project integrates Quantum-Chaotic Encryption with DCT-based steganography to enhance security and imperceptibility. By encrypting information in the frequency domain and embedding it, the system improves resistance to image processing attacks. Utilizing Quantum Random Number Generation (QRNG) and chaotic maps, it generates an unpredictable AES-256 key with high entropy and quantum resistance. This approach overcomes the limitations of traditional steganography, ensuring secure, strong, and imperceptible data transmission.

## 3. Literature Survey

Research on frequency-domain steganography, particularly using Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), has shown the effectiveness of including data in the frequency coefficients of cover images. This approach offers advantages over spatial-domain methods, such as improved resistance to common image- processing attacks, like compression. Studies highlight how frequency-domain steganography can provide better imperceptibility and robustness, making it ideal for secure communication. [1]

The paper highlights that traditional cryptographic algorithms like AES face challenges in real-time image encryption, making chaos-based encryption a viable alternative. It introduces a plaintext correlation mechanism to improve key security and integrates a ciphertext feedback diffusion method, ensuring resistance against chosen-plaintext and differential attacks. Experimental results validate the system's low computational complexity, high randomness, and strong encryption quality, making it suitable for IoT-based secure communications. [2]

The study presents a quantum image encryption scheme utilizing a uniquely designed pseudorandom number generator (PRNG) built on chaotic maps and hash functions. The encryption process employs two rounds of diffusion and scrambling using quantum gates such as CNOT, Toffoli, and Swap, ensuring high randomness and high resistance to brute-force attacks. By basing encryption parameters on the input image, the system's self-adaptive feature enhances security against known-plaintext and chosen-plaintext assaults. Experimental results

validate the scheme's strong security, robustness, and efficiency, making it a feasible approach for quantum-secure image transmission and storage. [3]

The study explores various steganographic approaches, emphasizing the importance of selecting suitable cover image formats and embedding methods to improve imperceptibility and security. The study compares DCT and DWT-based steganography techniques and highlights their resistance to steganalysis and compression attacks.

Additionally, it evaluates hybrid encryption methods, demonstrating that combining encryption with frequency- domain steganography significantly enhances security and robustness. [4]

The study investigates the effectiveness of transform domain, including DCT, DWT, and DFT for secure data embedding. The paper confirms that frequency-domain methods provide high embedding capacity while maintaining image quality, as indicated by PSNR and SSIM evaluations. It emphasizes that JPEG stego-images maintain their quality even after compression, making DCT and DWT-based steganography suitable for real-world applications. [5]

This study introduces a novel texture-based steganography approach that synthesizes stego textures rather than embedding data into an existing image. Using DCT-based frequency transformation, the method ensures high imperceptibility and robustness against steganalysis. The study highlights that texture synthesis allows for arbitrary embedding capacity, overcoming the limitations of traditional cover-image-based methods [6].

## 4. Related Works

Secure image steganography has evolved by integrating encryption techniques with frequency-domain transformations, particularly Discrete Cosine Transform (DCT), to enhance security and imperceptibility. In one approach, a DCT-based steganography method selectively embeds data in mid-frequency coefficients, obtaining a trade-off between imperceptibility and resistance to compression and noise attacks.

Additionally, a different method combined AES encryption with DCT-based steganography, guaranteeing that the hidden message would stay safe and unintelligible without the right decryption key, even in the event that a stegoimage was intercepted. While preserving the cover image's slight distortion, this integration greatly increases the anonymity of the contained data.

Furthermore, another technique used AES encryption in conjunction with DCT-based steganography to ensure that, even in the case that the stegoimage was intercepted, the concealed message would stay secure and unreadable without the proper decryption key. This integration

significantly improves the security of the embedded data while maintaining the minimal distortion of the cover image.

These works highlight the effectiveness of combining encryption with DCT-based steganography to achieve secure and imperceptible data embedding, forming the basis for more advanced and resilient steganographic communication systems.

## 5. Existing System

Traditional image steganography methods use Least Significant Bit (LSB) substitution. While LSB substitution is simple, it is highly susceptible to compression and steganalysis. However, most existing systems lack advanced encryption mechanisms, leaving embedded data vulnerable to extraction. While some approaches incorporate AES or DES encryption, they remain susceptible to future quantum attacks. This highlights the need for a more secure, quantum- resistant steganographic approach.

## 6. Proposed System

The proposed system enhances current steganography techniques by integrating RSA encryption with frequency domain methods like DCT and DWT. In this approach, the data is first encrypted using RSA encryption; ensuring only authorized users can access the hidden information by decrypting it with a private key. The encrypted data is then embedded in the frequency domain of the image using DCT or DWT, offering improved resistance against common image manipulation techniques, such as noise, compression, and cropping. This hybrid approach combines the benefits of strong encryption with the robustness of frequency domain steganography, ensuring secure, imperceptible, and resilient data hiding. The system is ideal for applications needing confidentiality and integrity of the hidden data, data protection, and secure communication.

### 6.1 Methodology

The proposed system integrates Quantum-Chaotic Encryption with DCT-based image steganography to enhance security and robustness. First, the secret message is encrypted using an AES-256 key, which is generated through Quantum Random Number Generation (QRNG) and a chaotic logistic map. This ensures high entropy and resistance against classical and quantum attacks.

The cover image is then converted using the Discrete Cosine Transform (DCT) from the spatial domain to the frequency domain. By splitting the image into distinct frequency components, this decomposition enables the encrypted data to be embedded selectively. The

system maintains resilience against compression, noise, and other image manipulations while guaranteeing imperceptibility through the modification of high-frequency DCT coefficients.

Following embedding, the image is rebuilt using the inverse DCT, producing a stego image visually identical to the original. This hybrid approach ensures secure, undetectable, and robust data hiding, making it ideal for covert communication and secure data transmission.

## 6.2 Architecture

### *6.2.1 Input Layer*

***Cover Image:*** Input image into which the secret data will be embedded. The image is preprocessed to ensure it is suitable for embedding, such as resizing or format conversion if necessary.

***Secret Data:*** The information to be hidden, which is a text and transformed to the suitable format by preprocessing.

### *6.2.2 Quantum Chaotic Encryption Layer*

***Key Generation:*** A Quantum Random Number Generator (QRNG) and a chaotic logistic map generate a highly unpredictable AES-256 encryption key, ensuring resistance to classical and quantum attacks.

***Encryption Algorithm:*** AES-256 is used to encrypt the secret data, guaranteeing that it will be safe even in the event that the stego-image is accessed.

### *6.2.3 Embedding Layer*

***Frequency Domain Transformation:*** The Discrete Cosine Transform (DCT) is used to transform the cover image from the spatial to the frequency domain.

***Data Embedding:*** The DCT coefficients that have been carefully chosen incorporate the encrypted data, ensuring. Imperceptibility while maintaining resilience against compression, noise, and image modifications.

### *6.2.4 Reconstruction Layer Inverse Transformation*

After embedding the secret data, use inverse transformation, such as Inverse DCT, for frequency domain techniques to reconstruct the image.

***Stego-Image Output:*** Create the final stego-image with the hidden data in it.

## 6.3 Limitations

One limitation of integrating Quantum-Chaotic Encryption with DCT-based image steganography is the computational overhead associated with Quantum Random Number Generation (QRNG) and chaotic key generation, which may impact performance in real-time applications. Additionally, ensuring key synchronization between sender and receiver is crucial, as even a minor variation in the chaotic key can make decryption impossible. While DCT-based embedding enhances security, it may introduce slight image distortion and reduce embedding capacity, limiting the amount of data that can be hidden. Lastly, the approach requires careful parameter selection for chaotic maps to maintain high entropy while avoiding key predictability.

## 6.4 Preprocessing

Preprocessing for Quantum-Chaotic Encryption integrated DCT-based steganography involves several steps. First, the cover image is resized and formatted to ensure compatibility. Pixel values are normalized for consistency, Binary is created from the secret data, binary form with padding if needed. A Quantum Random Number Generator (QRNG) and chaotic logistic map generate a high-entropy AES-256 key, after which the secret data is encrypted. The Discrete Cosine Transform (DCT) is used to convert the cover image into the frequency domain, identifying suitable regions for embedding in high-frequency components to enhance security while maintaining imperceptibility. Finally, preparations are made to embed the quantum-chaotically encrypted data securely.

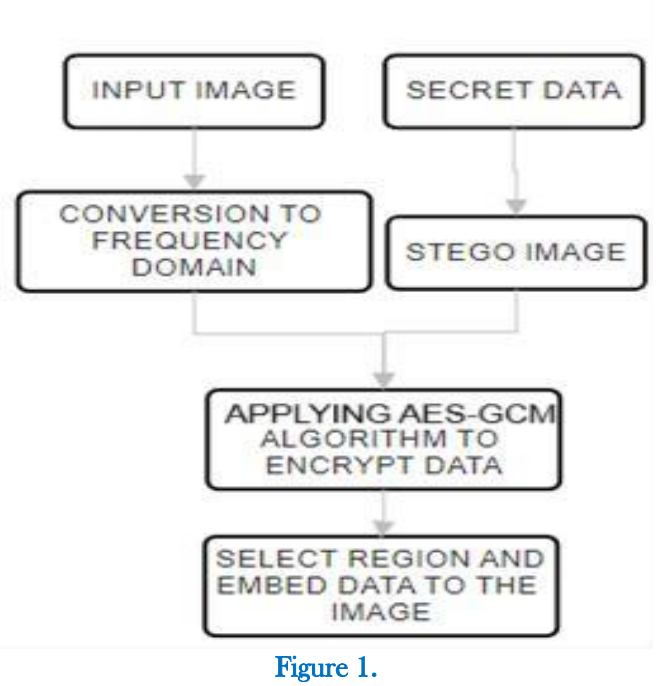


Figure 1.

## 7. Results and Discussion

In this project, Encryption-Enhanced DCT-Based Image Steganography, a secure and imperceptible method for embedding confidential data within images was successfully implemented. The system integrates encryption prior to embedding, guaranteeing that the concealed data is shielded from unwanted access even in the event that the stego image is intercepted.

The Discrete Cosine Transform (DCT), which enables selective coefficient modification to preserve visual quality, is used in the embedding process to convert the cover image into the frequency domain. A lightweight encryption algorithm is used to encrypt the secret data prior to embedding, guaranteeing confidentiality while reducing computational overhead. After that, the encrypted data is incorporated into mid-frequency DCT coefficients to strike a compromise between robustness and imperceptibility.

The picture quality study, which was conducted using the Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM), indicates that the system adds very little distortion while maintaining the integrity of the cover image. The encryption module strengthens the system's defenses against brute-force and statistical steganalysis assaults by introducing an extra layer of security. Even if an attacker finds secret data, decryption is difficult without the correct key. In terms of efficiency, the system maintains a reasonable execution time, ensuring practicality for secure communication applications. While encryption adds slight computational overhead, the trade-off between security and performance remains optimized. Future improvements could include adaptive coefficient selection for increased resistance against compression attacks and the incorporating postquantum cryptography techniques for sustained security.

Overall, the system successfully enhances traditional DCT-based steganography by incorporating encryption, ensuring confidentiality, imperceptibility, and robustness, making it a viable solution for secure digital communication and data protection.

## 8. Conclusion

This project successfully demonstrated encryption-enhanced DCT-based image steganography, ensuring secure data embedding with minimal visual distortion. By integrating encryption before embedding, the system enhances confidentiality and resistance to steganalysis, making it a robust solution for covert communication and digital data protection.

## 9. Future Scope

The future scope of this project includes exploring post- quantum cryptographic techniques to enhance security against emerging quantum threats. Additionally, implementing

adaptive DCT coefficient selection using machine learning can improve robustness and imperceptibility. Further optimizations, such as lightweight encryption for resource- constrained devices, can expand the applicability of the system to IoT and real-time secure communications.

## References

[1] S. Rahman, J. Uddin, M. Zakarya, H. Hussain, A.A. Khan, A. Ahmed, M. Haleem. (2023). A comprehensive study of digital image steganographic techniques. IEEE Access, *IEEE*, 11, 6770–6791. https://doi.org/10.1109/access.2023.3237393

[2] H. Wen, C. Zhang, P. Chen, R. Chen, J. Xu, Y. Liao, Z. Liang, D. Shen, L. Zhou, J. Ke. (2021). A Quantum Chaotic Image Cryptosystem and its application in IOT Secure Communication. IEEE access, *IEEE*, 9, 20481-20492. https://doi.org/10.1109/ACCESS.2021.3054952

[3] R.I. Abdelfatah. (2022). Quantum Image Encryption Using a Self-Adaptive Hash Function-Controlled Chaotic Map (SAHF-CCM). IEEE Access, *IEEE*, 10, 107152-107169. https://doi.org/10.1109/ACCESS.2022.3212899

[4] T. Bikku, R. Paturi. (2019). Frequency Domain Steganography with Reversible Texture Combination. *Traitement du Signal*, 36(1), 109-117.https://doi.org/10.18280/ts.360114

[5] A.Z. Abd Aziz, M.F.M. Sultan, N.L.M. Zulkufli. (2024). Image steganography: Comparative analysis of their techniques, complexity and enhancements. *International Journal on Perceptive and Cognitive Computing*, 10(1), 59-70. https://doi.org/10.31436/ijpcc.v10i1.449

## Funding

No funding was received for conducting this study.

## Conflict of interest

The Author's have no conflicts of interest to declare that they are relevant to the content of this article.

## About The License

© The Author's 2025. The text of this article is open access and licensed under a Creative Commons Attribution 4.0 International License.