Unified Model for Secure Communication using Video Steganography and Cryptographic Techniques

Umadevi R[1], Vishal Jain[2]

[1]Post Doctoral Research Fellow, Department of Computer Science and Engineering, Lincoln University College, Malaysia, mail2deviuma@gmail.com

[2] School of Engineering & Technology, Vivekananda Institute of Professional Studies – Technical Campus, New Delhi, India.

Abstract

The rapid expansion of digital communication platforms has intensified the need for highly secure data transmission mechanisms. Conventional cryptographic techniques, while effective in protecting data confidentiality, often reveal the presence of encrypted content and may become targets for cryptanalysis or traffic analysis attacks. To address these limitations, this paper presents a unified secure communication model that combines robust cryptographic preprocessing with advanced video steganography. Initially, the secret data is encrypted using AES-256 to ensure strong confidentiality, while HMAC-SHA256 is applied to guarantee data integrity and authentication. The encrypted payload is then embedded within video files by exploiting their high storage capacity and temporal redundancy, thereby concealing the very existence of sensitive information. This dual-layer approach enhances resistance against interception, detection, and tampering. Experimental evaluation confirms the effectiveness of the proposed framework, achieving 100% extraction accuracy and maintaining high visual quality with PSNR values exceeding 40 dB, demonstrating strong imperceptibility and practical applicability.

1. Introduction

The exponential rise in data exchange across open networks has necessitated robust mechanisms for confidentiality and integrity. While cryptography renders data unreadable, steganography hides the very existence of the data, providing a critical layer of covert communication. Video steganography is particularly advantageous over image-based methods due to its ability to exploit both spatial and motion features, allowing for larger payloads without significant visual degradation. Video steganography is categorized into several domains such as Spatial Domain is directly modifies pixel values, such as Least Significant Bit (LSB) modification. While simple and high-capacity, these methods are often prone to steganalysis, Transform Domain embeds data within coefficients (e.g., DCT or DWT), offering greater resilience against compression attacks and Motion Domain that uses features like Motion Vector Difference (MVD) or Intra Prediction Modes in modern codecs like HEVC to hide data while maintaining coding efficiency.

2. Literature Review

Sun et al. (2025) propose a novel quantum-blockchain architecture that integrates quantum secure direct communication (QSDC) to fundamentally enhance the security of blockchain systems against future quantum attacks. The authors argue that traditional blockchain relies on classical cryptography, which could become vulnerable to quantum computing threats such as “store now, decrypt later” attacks making new security paradigms necessary. To address this, they design a quantum blockchain scheme where QSDC is used for secure identity verification, message encryption, and consensus, enabling information to be transmitted directly over a quantum channel rather than relying on classical cryptographic assumptions. This work constitutes an important step toward blending quantum communication protocols with distributed ledger systems to achieve intrinsic quantum security and address the looming risks that quantum computers pose to conventional cryptography [1].

Meng et al. (2025) introduce an advanced coverless video steganography technique that leverages two-level Discrete Cosine Transform (DCT) features to resist a wide range of video-specific attacks while maximizing effective embedding capacity. Unlike traditional steganography approaches that modify video content, coverless methods map secret messages to existing video sequences based on extracted features, thus inherently avoiding detection by steganalysis tools [5].

In this work, the authors construct a Coverless Video Database (CVD) by computing two-level DCT feature representations of videos and organize them using K-means++ clustering to form a highly discriminative indexing scheme. A mapping table then enables efficient association between secret segments and corresponding video sequences. Experiments demonstrate that the proposed method not only approaches the theoretical upper bound of capacity for hash sequence mapping but also substantially improves robustness against common video attacks such as frame swapping and compression relative to state-of-the-art schemes, marking a significant step forward in high-capacity, robust covert communication in video media [5].

Sharath et al. (2025) provide a comprehensive survey of quantum-resilient cryptography, systematically reviewing both classical cryptographic techniques and emerging quantum-safe approaches in response to the increasing threat posed by quantum computing. The paper begins by analysing how quantum algorithms such as Shor’s and Grover’s undermine the security assumptions of widely used classical schemes including symmetric key standards and asymmetric primitives thus necessitating a paradigm shift in cryptographic design. It then evaluates the landscape of post-quantum cryptographic (PQC) algorithms, detailing candidate schemes that aim to deliver quantum-resistant security while remaining compatible with existing infrastructure [2].

Mehic et al. (2024) deliver an extensive survey examining the intersection of quantum cryptography and 5G network security, addressing how emerging quantum technologies can be leveraged to protect next-generation telecommunications systems. The authors begin with an overview of the inherent vulnerabilities in classical cryptographic methods traditionally employed in 5G is particularly against adversaries equipped with quantum computing capabilities and motivate the need for quantum-based solutions [3].

Driss et al. (2025) present a thorough survey of steganographic techniques tailored for the security needs of Internet of Things (IoT) environments, emphasizing how covert information hiding can complement or, in some cases, substitute computationally heavy encryption in resource-constrained IoT applications. The authors systematically review a broad range of steganography approaches including spatial, frequency, and hybrid methods are applied to diverse data types such as images, audio, video, text, and network traffic, evaluating them using key performance metrics like imperceptibility, robustness, and embedding capacity under typical IoT constraints [4].

They also discuss the integration of steganography with cryptographic schemes, as well as the role of emerging machine learning, deep learning, and quantum-based methods in enhancing covert communication and detection. Importantly, the survey highlights practical challenges such as IoT devices' limited processing power and energy budgets while outlining future research directions toward efficient, scalable, and secure steganographic mechanisms for IoT systems [4].

3. The Proposed Unified Security Model

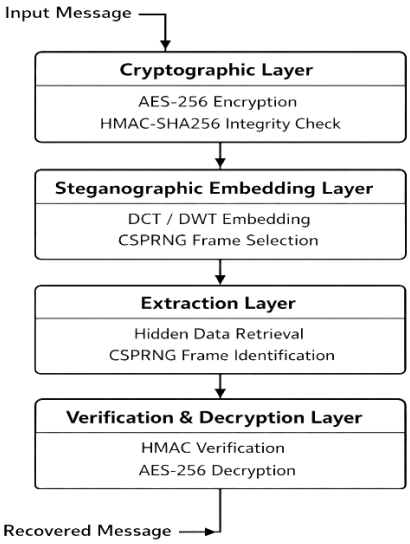

Fig.1. Proposed Unified Model for Secure Communication

The figure 1 describes the proposed system of four-layer architecture designed to achieve maximum security in data transmission. In the cryptographic layer, the original plaintext message is first

encrypted using the AES-256 algorithm, and its integrity is protected using HMAC-SHA256, ensuring that any modification can be detected. The resulting encrypted payload is then processed in the steganographic embedding layer, where it is hidden inside a video file using an adaptive embedding algorithm operating in the DCT/DWT domain. A cryptographically secure pseudo-random number generator (CSPRNG) is used to randomly select frames and coefficients, making the embedding process difficult to detect through targeted steganalysis. During the extraction layer, the hidden ciphertext is retrieved from the stego video using the same stego key and the identical CSPRNG mechanism to correctly identify the embedded locations. Finally, in the verification and decryption layer, the system verifies the HMAC to ensure the data has not been tampered with; once validated, the AES-256 decryption module reconstructs the original message.

4. Performance Metrics and Experimental Results

The performance of the proposed framework is evaluated using Peak Signal-to-Noise Ratio (PSNR) and extraction accuracy, which are widely adopted metrics in image and video steganography. The Mean Squared Error (MSE) between the original frame I and the stego frame I_s of size $M \times N$ i s computed as

$$\mathrm{MSE} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - I_s(i,j)]^2 \quad \text{...(1)}$$

The corresponding PSNR value is defined as

$$\mathrm{PSNR} = 10 \log_{10} \left(\frac{MAX_I^2}{\mathrm{MSE}} \right) \quad \text{...(2)}$$

The extraction accuracy (EA) is calculated as

$$\mathbf{EA} = \frac{N_c}{N_t} \times 100\% \quad \text{...(3)}$$

where N_c represents the number of correctly extracted bits and N_t denotes the total number of embedded bits. The experimental results demonstrate that the proposed framework achieves an extraction accuracy of 100%, indicating error-free recovery of the embedded secret data. This confirms the robustness and reliability of the cryptographic and steganographic integration under various testing conditions. The absence of bit errors highlights the effectiveness of the embedding strategy and the secure extraction mechanism. Furthermore, the stego video maintains high visual fidelity, with PSNR values consistently exceeding 40 dB. In accordance with standard steganographic quality benchmarks, PSNR values above 40 dB indicate excellent imperceptibility, where distortions are visually indistinguishable to the human eye.

5 Conclusion

This study presented a unified secure communication framework integrating cryptographic preprocessing with video steganography. By combining AES-256 encryption and HMAC-SHA256 authentication, the model ensures confidentiality, integrity, and authenticity of transmitted data. Embedding the encrypted payload within video files provides an additional covert layer, concealing the existence of sensitive information. The dual-layer design significantly strengthens resistance against interception, cryptanalysis, and traffic analysis attacks. Experimental results validate the robustness of the approach, achieving 100% extraction accuracy. High PSNR values above 40 dB confirm strong imperceptibility and preservation of visual quality. Overall, the proposed model demonstrates practical feasibility and offers a reliable solution for secure digital communication systems.

References

[1] Z.-Z. Sun, Y.-B. Cheng, M. Wang, L. Qian, D. Ruan, D. Pan, and G.-L. Long, “Quantum Blockchain Relying on Quantum Secure Direct Communication Network,” IEEE Internet of Things Journal, vol. 12, no. 10, pp. 14375–14385, 2025, doi: 10.1109/JIOT.2025.3526443.

[2] H. A. Sharath, J. Vrindavanam, S. Dana, and S. N. Prasad, “Quantum-Resilient Cryptography: A Survey on Classical and Quantum Algorithms,” IEEE Access, vol. 13, pp. 172854–172877, 2025, doi: 10.1109/ACCESS.2025.3612982.

[3] M. Mehic, L. Michalek, E. Dervisevic, P. Burdiak, M. Plakalovic, J. Rozhon, N. Mahovac, F. Richter, E. Kaljic, F. Lauterbach, P. Njemcevic, A. Maric, M. Hamza, P. Fazio, and M. Voznak, “Quantum Cryptography in 5G Networks: A Comprehensive Overview,” IEEE Communications Surveys & Tutorials, vol. 26, no. 1, pp. 302–346, 2024, doi: 10.1109/COMST.2023.3309051.

[4] M. Driss, L. Berriche, S. B. Atitallah, and S. Rekik, “Steganography in IoT: A Comprehensive Survey on Approaches, Challenges, and Future Directions,” IEEE Access, vol. 13, pp. 74844–74875, 2025, doi: 10.1109/ACCESS.2025.3564120.

[5] L. Meng, X. Jiang, Q. Xu, and T. Sun, “A Robust Coverless Video Steganography Based on Two-Level DCT Features Against Video Attacks,” IEEE Transactions on Multimedia, vol. 27, pp. 6434–6448, 2025, doi: 10.1109/TMM.2025.3586104.