Secure Communication using Quantum Video Steganography

Umadevi R[1], Vishal Jain[2]

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

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

mail2deviuma@gmail.com

Abstract

Quantum computing and video message concealment are combined in quantum video steganography. It appears to be a practical method for ensuring the security of multimedia while it is being transmitted. The paper proposes a configuration in which quantum-based video frames conceal encrypted data. Sending remains reasonably effective and visual changes are minimal. The QKD that runs in Qiskit provides the keys needed to lock and unlock the video. The hidden message enters through a quantum embedding stage once frames are transformed into quantum form. A quantum channel is used for the entire process. A decoder at the other end extracts and reconstructs the message. QBER, which measures faulty bits against total bits when noise appears, is used to gauge how well it performs. In practice, it can still be challenging to balance certain aspects of maintaining both security and quality. The concept attempts to address concerns about the video's durability and safety.

Keywords: Quantum Video Steganography, Quantum Key Distribution (QKD), Quantum Bit Error Rate (QBER), Secure Communication, Video Encryption, Quantum Computing.

Introduction

The growing reliance on digital communication systems has led to considerable difficulties in maintaining data confidentiality, integrity, and secure transmission. Traditional cryptographic methods safeguard data by encrypting it; however, such encrypted data can draw unwanted attention and increase the risk of cyberattacks. Steganography mitigates this issue by embedding secret information within digital media like images, audio, and videos, rendering the hidden data's presence challenging to detect. Among various steganographic mediums, video files provide greater capacity for embedding and improved security due to their substantial size and temporal complexity, making them ideal for secure communication purposes. Recent advancements in quantum computing and quantum communication have opened new possibilities for developing highly secure information-hiding techniques. Quantum Video Steganography combines the principles of quantum mechanics with traditional video steganography to provide a robust framework for covert communication. Quantum technologies such as Quantum Key Distribution (QKD) enable the generation of cryptographic keys with theoretically unbreakable security, while quantum-based data representation allows secure embedding and transmission of secret messages. By integrating quantum encryption with video steganography, it becomes possible to enhance resistance against interception, steganalysis, and other security threats.

Related work

Video steganography has become an important research area in multimedia security due to its ability to hide large volumes of secret information within video files while maintaining imperceptibility. Kunhoth et al. presented a comprehensive review of video steganography techniques, including spatial-domain, transform-domain, and compressed-domain approaches. Their study highlighted the advantages of video-based information hiding and discussed challenges such as robustness, security, payload capacity, and resistance to steganalysis attacks. The authors emphasized the need for advanced techniques capable of providing stronger security in modern communication systems [1]. Artificial intelligence has also contributed significantly to ultramodern steganographic systems. Namitha et al. introduced StegAbb, a GPT-3-based textbook steganographic frame designed for covert communication across Software Defined Radios (SDRs). The model generated natural- looking cover textbook with low detectability and achieved high decoding delicacy. This work demonstrated the effectiveness of AI- driven steganography in enhancing communication secretiveness and reducing the probability of discovery [2].

Meng et al. proposed a robust coverless Video steganography system grounded on inter-frame similarity and point matching ways. By exercising frame connections rather of bedding information directly into pixels, the system bettered resistance against steganalysis and Video manipulation attacks. The study showed significant robustness under colorful inimical conditions [3]. Deep literacy ways have farther advanced Video steganography capabilities. Mou et al. developed a large- capacity and flexible Video steganography frame using invertible neural networks (Auberges). The proposed system successfully bedded multiple secret vids into a single cover Video while maintaining high visual quality and security. Their findings demonstrated the eventuality of neural- network- grounded infrastructures for achieving large cargo capacities and flexible information recovery mechanisms [4].

Security pitfalls related to steganography have also been considerably studied. Gilkarov and Dubin delved steganalysis ways for detecting vicious Least Significant Bit (LSB) attacks bedded within AI models. Their work proposed supervised and unsupervised discovery mechanisms able of relating retired information within machine literacy models. The study stressed the growing need for advanced security fabrics that combine encryption, steganography, and discovery ways to insure secure communication systems [5].

Gadicha et al. (2021) proposed a multimode data encryption approach using amount steganography for secure image communication. The study combined amount cryptography principles with steganographic ways to enhance the confidentiality of retired information. Multiple encryption layers were applied before bedding the secret data into digital images, thereby adding resistance against unauthorized access and steganalysis attacks. The authors demonstrated that the integration of amount- grounded security mechanisms bettered data protection while conserving image quality and reducing the probability of discovery. The exploration stressed the eventuality of amount steganography as an effective result for coming- generation secure multimedia communication system [6]. Being studies have explored image, audio, Video, textbook, network, and amount steganography ways to enhance secure communication in IoT surroundings. utmost approaches employ spatial, transfigure- sphere, mongrel, and AI- grounded styles to ameliorate imperceptibility, robustness, and embedding capacity. Recent workshop integrate cryptography, machine literacy, deep literacy, blockchain, and amount computing to strengthen data confidentiality and resistance to attacks. still, challenges related to computational outflow, resource constraints, scalability, and real- time processing in IoT bias remain rightly addressed, indicating the need for featherlight and adaptive steganographic results [7].

Thus, the proposed Quantum Video Steganography frame integrates Quantum Key Distribution (QKD), Quantum Bit Error Rate (QBER) analysis, and amount- grounded embedding algorithms to give enhanced security, confidentiality, and trustability for unborn multimedia communication networks.

Proposed Methodology

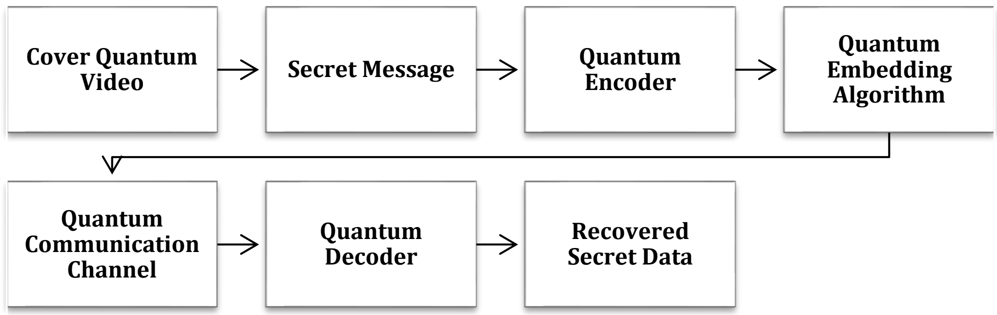

Figure 1. Architecture for Proposed Methodology

The proposed framework initiates with a Cover Quantum Video, which serves as the carrier medium for securely transmitting nonpublic information. A Secret Communication covering sensitive data is primary set and also reprocessed through a Quantum Encoder. The encoder converts the secret information into volume representations using qubits, enabling secure running of the data. This volume garbling process enhances confidentiality by using amount mechanical parcels similar as superposition and volume key- grounded encryption, making unauthorized access extremely delicate. After garbling, the secret information is bedded into the cover amount Video using a Quantum Embedding Algorithm. This stage precisely hides the decoded data within named video frames while conserving the visual quality and integrity of the original video. The embedding algorithm ensures that the dissimilarities remain imperceptible to mortal addressees and innocent to steganalysis attacks. Once the embedding process is completed, the stego Video is transmitted through a Quantum Communication Channel, which facilitates secure data transfer while maintaining the volume characteristics of the embedded information. The communication channel may be affected by environmental noise; thus, performance is estimated using criteria similar as Quantum Bit Error Rate (QBER). At the receiver side, the transmitted Video is reused by a Quantum Decoder, which excerpts the retired amount information from the entered stego Video. The decoder utilizes the corresponding amount key and decoding procedures to reconstruct the original secret communication directly. Eventually, the system generates the Recovered Secret Data, icing secure and dependable communication between the sender and receiver. This armature integrates amount cryptography and Video steganography to give enhanced security, robustness, and sequestration for coming- generation multimedia communication systems. Quantum Bit Error Rate(QBER) is a abecedarian performance metric used in amount communication systems to estimate the trustability and security of transmitted amount information. It represents the proportion of amount bits(qubits) that are inaptly entered compared to the total number of transmitted qubits. In Quantum Video Steganography, QBER is used to assess the impact of channel noise, hindrance, and implicit wiretapping attacks on the communication process. A lower QBER value indicates a more secure and dependable amount channel, while a advanced QBER suggests increased transmission crimes and reduced communication quality.

Quantum Bit Error Rate (QBER) is used to measure the percentage of incorrectly received quantum bits during transmission. It is calculated as:

$$QBER = \frac{N_{error}}{N_{total}} \times 100\% \qquad \text{...(1)}$$

Where N_{error} =Number of incorrect bits received

N_{total} =Total transmitted bits

Table 1. QBER Vs Noise Level

Noise Level (%)	Transmitted Qubits	Error Bits	QBER (%)
0	10000	25	0.25
2	10000	120	1.20
4	10000	240	2.40
6	10000	410	4.10
8	10000	690	6.90
10	10000	980	9.80

Table 1 presents the performance evaluation of the proposed Quantum Video Steganography system using the Quantum Bit Error Rate (QBER) under varying noise situations. The outcomes show that as the noise position in the volume communication channel increases from 0 to 10, the number of incorrect bits entered also increases meaningfully, leading to a consistent rise in QBER values. At 0 noise, only 25 error bits are observed out of 10,000 transmitted qubits, performing in a low QBER of 0.25, which specifies largely dependable communication. Still, when the noise position reaches 10, the number of error bits increases to 980, producing a QBER of 9.80. It determines the direct impact of channel noise on amount transmission delicacy. Despite the increase in crimes, the QBER values remain below the generally accepted security threshold for Quantum Key Distribution (QKD) systems, indicating that the proposed framework can maintain secure and dependable communication under reasonable noise conditions. Thus, QBER aids as an effective measure for evaluating the robustness and security performance of the proposed volume communication model. Figure 2 illustrates the relationship between channel noise position and Quantum Bit Error Rate (QBER) in the proposed Quantum Video Steganography system. The graph shows a steady increase in QBER as the noise position rises from 0 to 10, indicating that transmission crimes come more frequent under noisy channel conditions. At lower noise situations, the QBER remains close to zero, representing high communication trustability and accurate qubit transmission. As the noise position exceeds 6, the rate of increase becomes more pronounced, reflecting the growing impact of channel disturbances on amount communication. nonetheless, the observed QBER values remain below the typical security threshold for Quantum Key Distribution (QKD), attesting the robustness and effectiveness of the proposed frame for secure multimedia communication.

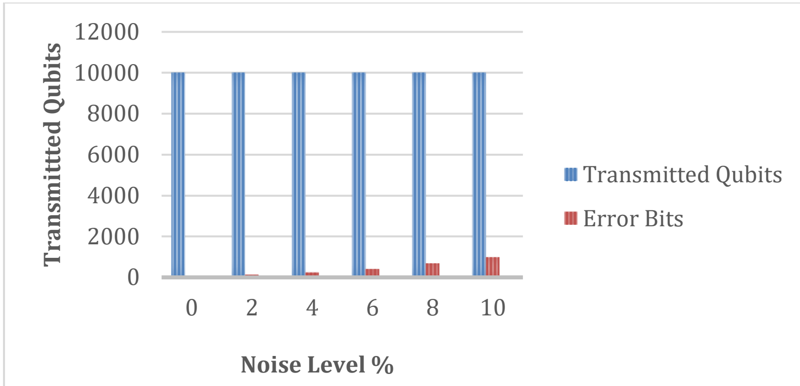

Figure 2. Parameter Evaluation for Error Bits

Conclusion

The proposed exploration reports the need for secure multimedia communication by integrating amount computing with Video steganography. A Quantum Video Steganography frame was developed using Quantum Key Distribution (QKD) for secure crucial generation and communication encryption. Secret data is bedded into amount Video frames and transmitted through a amount communication channel. Experimental evaluation on the UCF101 dataset verified effective data hiding with minimum impact on Video quality. The Quantum Bit Error Rate (QBER) analysis showed that transmission crimes increase with channel noise but remain within good security limits.

References

1. J. Kunhoth, N. Subramanian, S. Al-Maadeed, and A. Bouridane, “Video Steganography: Recent Advances and Challenges,” *Multimedia Tools and Applications*, vol. 82, pp. 41943–41985, 2023, doi: 10.1007/s11042-023-14844-w.
2. M. V. Namitha, G. R. Manjula, and M. C. Belavagi, “StegAbb: A Cover-Generating Text Steganographic Tool Using GPT-3 Language Modeling for Covert Communication Across SDRs,” *IEEE Access*, vol. 12, pp. 82057–82067, 2024, doi: 10.1109/ACCESS.2024.3411288.
3. L. Meng, X. Jiang, T. Sun, Z. Zhao, and Q. Xu, “A Robust Coverless Video Steganography Based on the Similarity of Inter-Frames,” *IEEE Transactions on Multimedia*, vol. 26, pp. 5996–6011, 2024, doi: 10.1109/TMM.2023.3345166.
4. C. Mou, Y. Xu, J. Song, C. Zhao, B. Ghanem, and J. Zhang, “Large-Capacity and Flexible Video Steganography via Invertible Neural Network,” *IEEE Transactions on Circuits and Systems for Video Technology*, 2023.
5. D. Gilkarov and R. Dubin, “Steganalysis of AI Models LSB Attacks,” *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4767–4779, 2024, 10.1109/TIFS.2024.3383770.
6. A. B. Gadicha, V. B. B. Gupta, V. B. Gadicha, K. Kumar, and M. M. Ghonge, “Multimode approach of data encryption in images through quantum steganography,” in *Multidisciplinary Approach to Modern Digital Steganography*. Hershey, PA, USA: IGI Global, 2021, pp. 99–124, [DOI: 10.4018/978-1-7998-7160-6.ch005](https://doi.org/10.4018/978-1-7998-7160-6.ch005).

7. M. Driss, L. Berriche, S. Ben 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.