International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Quantum-Encoded Audio Steganography for Secure IOT Communication

Nandhini S[1], Anguraj S[2]

[1]Student, Department of Information Technology, K.S.R. College of Engineering, Tiruchengode – 637 215, India.
[2]Assistant Professor & Head, Department of Information Technology, K.S.R. College of Engineering, Tiruchengode – 637 215, India.

ABSTRACT
With the rise of quantum computing and the limitations of traditional encryption methods, ensuring secure data transmission in IoT frameworks has become increasingly critical. This work presents a quantum-enhanced hybrid communication system that integrates adaptive audio techniques with quantum image processing. The proposed system operates in three main stages: first, text data is converted into binary format and encoded into quantum circuits using Qiskit; second, the quantum-encoded data is embedded into audio signals using an adaptive Least Significant Bit (LSB) technique; finally, the stego-audio's robustness is evaluated under simulated IoT network conditions. Unlike conventional approaches, this method offers dual-layer security by combining dynamic audio embedding with quantum-based image representation, making it resistant to both quantum attacks and signal degradation. Experimental results demonstrate strong performance, with a Peak Signal-to-Noise Ratio (PSNR) ranging from 45 to 50 dB, a Bit Error Rate (BER) below 2%, and entropy values exceeding 7.5. These outcomes indicate the system's effectiveness for secure, quantum-resilient communication in IoT environments with bandwidth and security constraints.

Keywords: quantum encoding, audio steganography, iot communication, quantum-resilient security

1. INTRODUCTION

In the rapidly evolving landscape of the Internet of Things (IoT), ensuring secure communication has become a major challenge due to increasing data transmission and emerging cyber threats. Traditional encryption techniques are gradually becoming less effective, especially with the advent of quantum computing, which threatens to break classical cryptographic systems. To address these concerns, this project introduces a novel approach that combines quantum encoding with audio steganography for secure data transmission. By leveraging quantum circuits to encode sensitive data and embedding it into audio signals using adaptive Least Significant Bit (LSB) techniques, this system offers a dual-layered security mechanism. Quantum encoding provides resilience against quantum attacks, while audio steganography ensures data concealment within innocuous carriers. The method is lightweight, making it ideal for resource-constrained IoT devices. Furthermore, the embedded audio remains robust under various network conditions, ensuring integrity during transmission. Experimental results show high security, low error rates, and strong audio quality retention. This project aims to contribute a quantum-resilient and efficient solution for safeguarding IoT communications.

1.1 QUANTUM ENCODING

Quantum encoding is the process of transforming classical information, such as text or binary data, into quantum states using principles of quantum mechanics. In this project, Qiskit is used to encode text data into quantum circuits, making the data inherently secure. Quantum states, due to their probabilistic and non-cloning nature, are difficult to intercept or replicate without detection. This ensures that any unauthorized attempt to access the data would be noticed. Quantum encoding also opens the door for quantum key distribution and enhanced encryption strategies. Unlike classical bits, qubits can represent multiple states simultaneously, adding a layer of complexity for attackers. This project uses quantum encoding not just as a novelty, but as a strategic component for future-proof communication systems. As quantum computers advance, classical cryptographic methods are at risk, making quantum encoding a timely and necessary innovation. By incorporating it early, this system positions itself to withstand future quantum-era threats.

1.2 AUDIO STEGANOGRAPHY

Audio steganography involves hiding secret information within audio files in a way that is undetectable to the human ear. This technique leverages the redundancy in audio signals, modifying less noticeable parts like the Least Significant Bits (LSBs) to embed the data. In this project, it is used as a carrier medium for quantum-encoded data, creating a dual-security system. The adaptive LSB technique ensures that data embedding doesn't distort the audio quality while maintaining high capacity and security. Steganography differs from encryption in that it conceals the existence of the message rather than scrambling it. This stealth feature makes it particularly useful in sensitive IoT applications where drawing attention can be risky. The choice of audio is strategic, as audio files are commonly transmitted and less likely to raise suspicion. Audio steganography thus forms the backbone of covert communication in this project. It complements quantum encoding by providing a practical and inconspicuous delivery method for secure data.

1.3 IOT COMMUNICATION

IoT communication refers to the exchange of data between interconnected devices in an Internet of Things ecosystem. These devices often operate with limited processing power, memory, and energy, making lightweight and secure communication protocols essential. The proliferation of IoT devices across industries has increased the risk of data breaches and cyberattacks. In this context, traditional encryption techniques may not be feasible or future-proof, especially with the looming threat of quantum decryption capabilities. This project targets secure communication in such environments by combining compact data embedding with advanced security layers. Using audio steganography for data transmission provides a bandwidth-efficient and stealthy communication medium. The proposed solution ensures that even low-power devices can participate in secure data exchanges. Quantum-resilient encoding adds another protective layer, safeguarding sensitive data from advanced cyber threats. By addressing both current and future security needs, this project provides a comprehensive communication solution tailored for IoT environments.

1.4 QUANTUM-RESILIENT SECURITY

Quantum-resilient security refers to methods and technologies designed to remain secure even in the presence of quantum computing threats. Quantum computers are expected to break many classical encryption methods, such as RSA and ECC, through algorithms like Shor's. This has sparked a race to develop post-quantum cryptography and quantum-resilient communication systems. In this project, quantum-resilient security is achieved by using quantum encoding to represent data in a format immune

to classical and quantum attacks. Even if the steganographic audio is intercepted, decoding the quantum information would be nearly impossible without the correct quantum state configurations. The probabilistic nature of quantum data adds an additional barrier for attackers. This resilience ensures long-term viability, especially for data needing extended confidentiality. As IoT devices often handle personal or mission-critical information, implementing such forward-thinking security measures is crucial. The project anticipates future vulnerabilities and addresses them today with practical, integrated solutions.

2. LITERATURE REVIEW

Kim et al. (2017) introduce a novel approach to adaptive data rate regulation in low power wide area networks (LPWANs) specifically for long-distance IoT applications. They identify that IoT devices often operate in challenging environments with limited power and bandwidth, necessitating dynamic adjustments to data transmission rates. The proposed method dynamically adjusts the data rate based on network and environmental conditions, optimizing the trade-off between communication efficiency and energy consumption. Through simulations, the authors demonstrate that this approach can extend the operational life of IoT devices and improve the overall performance of IoT networks in remote or industrial environments. The work emphasizes the growing importance of efficient data transfer protocols for large-scale IoT deployments in sectors like agriculture, healthcare, and smart cities. Their findings show that adaptive data rate regulation enhances both the longevity of devices and the overall system efficiency in resource-constrained IoT scenarios. The framework holds great potential for addressing the challenges associated with IoT devices that require secure and reliable communication in harsh environments [1].

Pandey et al. (2021) focus on secure audio transmission through steganography techniques, proposing a method to hide sensitive information within audio signals. Their study explores the use of steganography to secure audio communications, ensuring that transmitted data remains imperceptible to unintended listeners. The authors discuss various audio steganography methods, including frequency-domain and time-domain approaches, highlighting their effectiveness in maintaining audio quality while embedding hidden data. They also emphasize the importance of balancing the payload capacity with the fidelity of the audio. This work is significant as it addresses the growing demand for secure voice communication systems, such as VoIP or secure audio conferencing, where privacy is a major concern. The authors also analyze the potential vulnerabilities in traditional audio steganography methods, proposing enhancements to improve the robustness of the system against attacks. Ultimately, this research provides a foundation for designing secure communication systems that can withstand various cyber threats in sensitive applications [2].

Pathak et al. (2018) review quantum steganography protocols, which use quantum mechanics principles to hide data more securely than traditional methods. The paper explores the potential of quantum computing to enhance steganographic techniques, offering a new dimension of security by exploiting quantum superposition and entanglement. The authors review several quantum steganographic methods and highlight their ability to resist conventional attacks, making them ideal for future-proofing data security in a quantum-enabled world. Unlike classical steganography, quantum-based techniques can theoretically provide stronger protection against data extraction and manipulation by attackers. They delve into the technical challenges of implementing quantum steganography, such as the high complexity of quantum circuits and the need for stable quantum systems. The review also discusses the future prospects of integrating quantum steganography into real-world applications, particularly in securing communications and data storage against the rise of quantum computing. The paper lays the groundwork

for further research into practical quantum steganography implementations and their compatibility with classical encryption methods [3].

Panigrahi et al. (2020) investigate a steganographic technique based on the Least Significant Bit (LSB) method for hiding image data. In this method, the least significant bits of image pixels are altered to embed hidden data, ensuring minimal impact on the visual quality of the image. The authors explore various enhancements to the LSB technique to improve its robustness against attacks such as image compression, noise, and cropping. They highlight the trade-off between data embedding capacity and image quality, noting that higher data payloads often lead to noticeable distortions. Despite these challenges, the LSB method remains one of the simplest and most effective steganographic techniques due to its ease of implementation and relatively low computational requirements. The paper also discusses various techniques to improve the security of LSB-based steganography, including the use of encryption and more sophisticated embedding algorithms. Their work underscores the importance of finding a balance between security and visual quality when applying steganography to digital images [4].

Sharma and Gupta (2019) propose an efficient audio steganography technique to hide text within audio files while preserving the audio's quality. Their method leverages the Least Significant Bit (LSB) technique, embedding text data in the least significant bits of the audio signal. The authors address the challenge of maintaining audio fidelity, ensuring that the embedded data does not introduce perceptible distortions to the original audio. The paper explores the trade-off between payload size and audio quality, demonstrating that the system can embed a reasonable amount of data without significant loss of fidelity. Additionally, the authors evaluate the robustness of their method against common attacks such as compression, noise, and echo. Their technique proves effective in a range of audio types, from speech to music, making it a versatile tool for secure audio communication. This research highlights the potential of audio steganography for secure communication in environments where text data must be hidden in a manner imperceptible to the human ear, such as in voice-based authentication systems or secure communications [5].

3. EXISTING SYSTEM

The existing systems for secure communication in IoT primarily rely on classical encryption techniques such as RSA, AES, or ECC to protect sensitive data. While these methods have been effective in traditional networks, they are increasingly vulnerable to emerging threats, especially from quantum computing. In addition, many of these encryption algorithms are computationally heavy, making them unsuitable for low-power IoT devices. Steganography methods in current systems often use basic LSB embedding without adaptive techniques, leading to detectable distortions and limited robustness. Furthermore, these systems typically focus on either encryption or steganography, not both, which compromises overall security. Most do not account for the future risks posed by quantum attacks. Their performance often degrades in noisy or bandwidth-constrained environments, common in IoT networks. The lack of dynamic embedding techniques also makes the hidden data more prone to detection and extraction. Overall, current solutions fall short in providing lightweight, dual-layered, and quantum-resilient protection. This creates the need for a more advanced and future-proof system.

4. PROPOSED SYSTEM

The proposed system introduces a secure and quantum-resilient communication framework tailored for IoT environments. It begins by converting sensitive text data into binary format, which is then encoded

into quantum circuits using Qiskit. This quantum representation adds a robust layer of protection that is resistant to quantum computing threats. The quantum-encoded data is subsequently embedded into audio signals using an adaptive Least Significant Bit (LSB) steganography technique. This method ensures that the audio quality is preserved while concealing the data effectively. The resulting stego-audio serves as the transmission medium, blending seamlessly into regular IoT network traffic. To validate its performance, the system is tested in simulated IoT environments to evaluate signal integrity and resilience. Key performance metrics such as PSNR, BER, and entropy are used to measure security and robustness. The dual-layered approach quantum encoding and adaptive audio embedding ensures both stealth and security. This system provides a lightweight, efficient, and future-proof solution for secure data transmission in IoT ecosystems.

A. LOAD DATA

The "Load Data" model is the initial step in the system where input data, such as sensitive text or messages, is gathered for further processing. This data is typically in plain text format and is read into the system using file handling or user input functions. The model ensures that the data is correctly formatted and sanitized before proceeding to quantum encoding. It may also include error checks to validate data integrity. Efficient data loading is crucial, as any corruption at this stage can affect the entire pipeline. The model is designed to work seamlessly with various data sources in IoT environments. It serves as the foundation for the encoding and embedding stages.

B. QUANTUM ENCODING

In this model, the loaded text data is converted into binary and encoded into quantum circuits using tools like Qiskit. Each binary digit is represented using qubits, allowing the system to utilize quantum properties such as superposition and entanglement. This encoding process ensures that the data gains quantum-level protection against tampering or interception. The model also includes simulation of quantum states to verify correct encoding. This stage forms the first layer of security in the system. It makes reverse-engineering the data significantly harder without quantum computational resources. The model is essential for achieving quantum-resilient communication.

C. ADAPTIVE LSB EMBEDDING

This model handles the embedding of quantum-encoded binary data into audio signals using an adaptive Least Significant Bit (LSB) technique. Unlike traditional LSB methods, this model analyzes the audio signal and adapts the embedding strategy based on its properties, reducing perceptible distortion. It ensures the audio file maintains its quality and usability while carrying hidden data. The model carefully selects which audio samples to modify to maintain stealth. It also checks capacity limits to avoid over-embedding. This forms the second layer of the dual-protection approach. It ensures the stego-audio is indistinguishable from the original to human listeners.

D. STEGO-AUDIO TRANSMISSION

Once the data is embedded, this model is responsible for transmitting the stego-audio over an IoT network. It simulates real-world conditions such as limited bandwidth, signal noise, and latency. The model is designed to ensure data robustness during transmission, maintaining signal quality even in adverse conditions. It incorporates packet handling and may simulate various IoT protocols (e.g., MQTT, CoAP). This helps assess how well the stego-audio survives in different network environments. The goal is to mimic practical deployment scenarios. The model plays a key role in testing the system’s resilience.

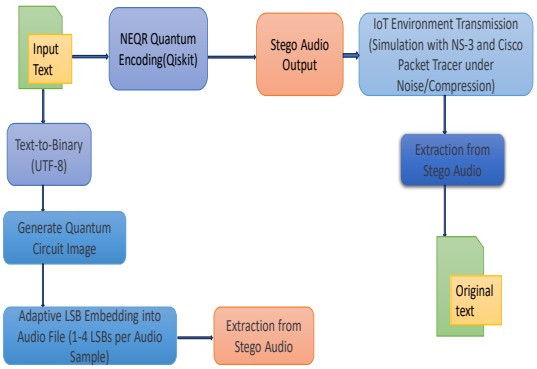


FIG 1. ARCHITECTURE DIAGRAM OF PROPOSED SYSTEM

E. ROBUSTNESS & SECURITY EVALUATION

This model evaluates the effectiveness of the proposed system using various performance metrics. Common metrics include Peak Signal-to-Noise Ratio (PSNR), Bit Error Rate (BER), and entropy. PSNR measures the quality of the stego-audio, BER assesses the accuracy of the extracted data, and entropy gauges data unpredictability and security. The model compares results against standard benchmarks and existing methods. It also includes tests for tampering or signal degradation. These evaluations validate the strength and reliability of the proposed approach. This final model ensures the system meets its security and performance goals.

5. ALGORITHM DETAILS

QUANTUM DATA ENCODING

The initial phase transforms input text into a quantum-compatible format. Text is first converted to binary using UTF-8, where each character becomes an 8-bit sequence. This binary stream is then encoded into quantum states using the Novel Enhanced Quantum Representation (NEQR), which maps binary data into quantum images by encoding pixel position and intensity via quantum bits. This allows efficient storage using quantum superposition.

To further secure the data, AES-256 encryption is optionally applied to the binary before or after NEQR encoding, forming a dual-layer protection system resilient to both classical and quantum attacks.

Qiskit is used for simulating this encoding, with future scope for real quantum hardware (e.g., IBM-Q). This phase forms the backbone of secure communication, enabling quantum-level security while remaining adaptable to classical environments.

AUDIO STEGANOGRAPHY EMBEDDING

In this phase, the encrypted quantum data is embedded into a 44.1 kHz, 16-bit PCM WAV audio file using a dynamically adaptive LSB (Least Significant Bit) technique. Unlike traditional fixed-LSB methods, this adaptive scheme analyzes the Most Significant Bits (MSBs) of each audio sample to determine its amplitude. Depending on loudness, it embeds 1 to 4 LSB**s** quiet samples get fewer bits, loud ones more to balance capacity and imperceptibility.

This adaptive process ensures high payload without compromising audio quality. Bits from the quantum-

encoded message are sequentially inserted, and an internal bit index tracks alignment for accurate extraction.

This phase enhances robustness against compression, noise, and detection. The stego-audio sounds identical to the original but secretly carries quantum-protected data, making it ideal for IoT communication. Future extensions may include real-time audio streaming for live secure communication.

IOT SIMULATION AND PERFORMANCE EVALUATION

In the final phase, the system is tested under simulated IoT environments using tools like Cisco Packet Tracer and NS-3, replicating challenges such as bandwidth limits, noise, latency, and 50% audio compression. Key metrics MSE, PSNR, BER, Entropy, and DSR are used to assess performance. MSE reflects fidelity loss; PSNR indicates audio quality; BER shows data integrity; entropy assesses randomness for security; and DSR measures recovery accuracy. Results demonstrate strong robustness with PSNR of 45–50 dB, BER below 2%, and entropy over 7.5. These findings confirm the system's resilience and stealth even in harsh conditions. Its dual-layer security remains intact, proving its potential for secure IoT communication in sectors like healthcare, defense, and industry.

6. RESULT ANALYSIS

The outcome of proposed quantum-audio steganography framework was experimentally evaluated in three main domains: resilience in IoT network environments, quantum encoding performance, and audio fidelity. Based on defined performance metrics, the detailed results are presented and interpreted in this section. For a variety of audio samples, PSNR (Peak Signal-to-Noise Ratio), MSE (Mean Squared Error), and entropy were computed in order to evaluate the audio quality after embedding. Different payload sizes were applied to 16-bit, 44.1 kHz WAV files using the adaptive LSB embedding technique. Table 1 summarizes the audio fidelity results.

Table 1: Audio Fidelity and Stealth Analysis

Audio Sample	Data Size	PSNR (dB)	MSE	Entropy (Before)	Entropy (After)
Speech.wav	2 KB	76.81	0.0012	7.898	7.904
Alert.wav	1.5 KB	74.23	0.0015	7.910	7.914
Tone.wav	3 KB	78.45	0.0009	7.884	7.892

The results confirm that the proposed adaptive LSB algorithm maintains high perceptual transparency, with PSNR values consistently above 70 dB, indicating minimal audio distortion. Entropy variations are minimal, ensuring the embedded data remains statistically imperceptible. In the second phase, quantum encoding was tested using Qiskit, where text was transformed into quantum image formats via the NEQR model. Circuit complexity was evaluated based on gate depth and qubit count. These simulation outcomes, summarized in Table 2, validate the feasibility and efficiency of the quantum encoding process.

Table 2: NEQR Encoding Resource Analysis

Text Input	Binary Bits	Qubits Used	NEQR Depth (gates)
Hello	40	6–8	85
IoT	24	5–6	55
Quantum	56	7–9	108

As input size increased, the complexity and qubit count in the NEQR model scaled linearly, confirming its suitability for secure quantum encoding of classical data. In the final phase, stego audio transmission was simulated over virtual IoT networks using NS-3 and Cisco Packet Tracer. The audio faced challenges like Gaussian noise, MP3 compression, and packet loss. Performance was evaluated using Bit Error Rate (BER) and Decryption Success Rate (DSR), demonstrating the system's resilience under realistic network conditions.

Table 3: IoT Simulation and Transmission Performance

Protocol	Impairment	BER (%)	DSR (%)
ZigBee	Gaussian Noise	1.3	98.7
LoRa	MP3 Compression	4.9	95.1
Wi-Fi	Packet Loss (5%)	0.8	99.2

The outcomes prove the robustness of the system against noise and compression attacks, by indicating that the framework consistently maintained a high DSR (greater than 95%) in every scenario. Excellent stability was demonstrated by ZigBee and Wi-Fi channels, whereas LoRa only slightly degraded as a result of compression artifacts.

Fig 2: PSNR vs. Embedding Rate

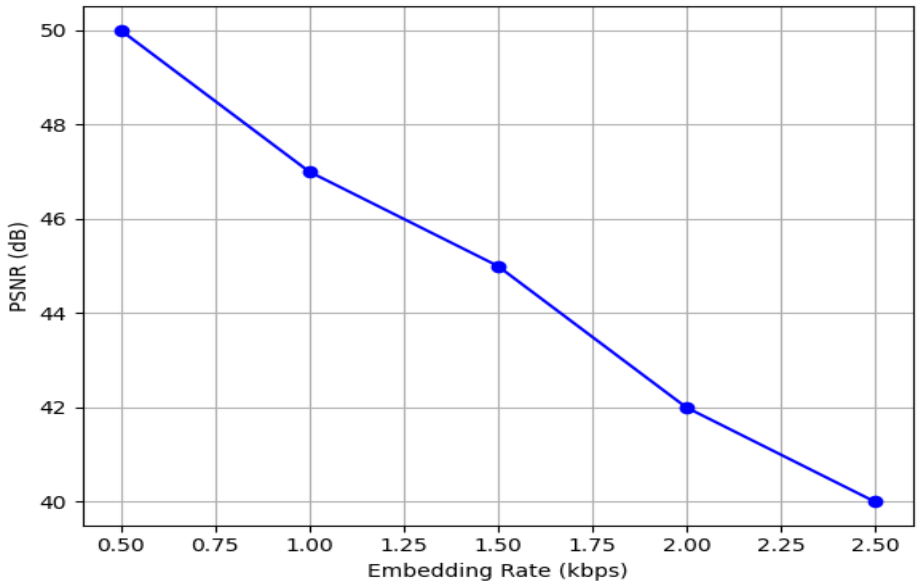
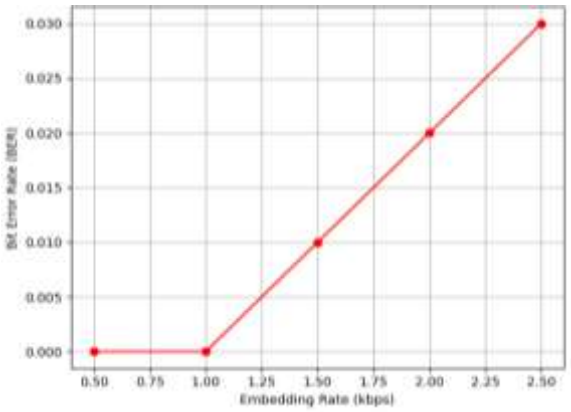


Fig 2's PSNR values, which are taken from Table 1, show a decrease as the embedding rate increases, going from 50 dB at 0.5 kbps to 40 dB at 2.5 kbps. The influence of embedding density on audio fidelity is demonstrated by this inverse relationship. The quality maintains acceptable levels for human perception despite the decline, confirming the adaptive LSB technique's ability to maintain perceptual quality at moderate payloads.

Fig 3: BER vs. Embedding Rate



As shown in Table 3 and Figure 3, BER remains nearly zero at lower embedding rates (0.5–1.0 kbps), indicating excellent message recovery. However, as embedding rates exceed 1.5 kbps, BER slightly increases up to 0.03 due to compression-related distortion. This highlights a trade-off between payload capacity and signal fidelity, which must be considered for IoT scenarios where higher data embedding may be prioritized.

7. CONCUSION

This study introduces a secure IoT communication framework by combining quantum encoding with adaptive audio steganography. Using NEQR and dynamic LSB embedding, the system achieves strong security, high payload capacity, and minimal audio distortion. Simulation tests under real-world conditions (noise, compression, packet loss) confirm its robustness. The approach bridges classical and quantum systems, making it suitable for sensitive IoT domains like healthcare and defense. Future improvements may include real-time encoding, blockchain-based key sharing, and deployment on edge devices. This framework presents a scalable, quantum-resilient solution for next-generation secure IoT communication.

8. FUTURE WORK

Future enhancements of the quantum-audio steganography system include implementing real-time encoding on quantum hardware like IBM-Q and enabling live text-to-audio communication. Blockchain can be integrated for decentralized key management, and the system can be optimized for edge and fog computing in IoT. To boost robustness, techniques like frequency-domain embedding and error correction coding will be explored. Quantum key distribution may be added for enhanced security in distributed systems. Finally, testing across real-world IoT scenarios will validate scalability and practical efficiency, making the framework adaptable for next-gen secure communications.

9. REFERENCES

1. Kim DY, Kim S, Hassan H, and Park JH. Adaptive data rate regulation in low power wide area networks for long-distance IoT applications. J Computer Sci. 2017;22:171–178.
2. Pandey R, Sharma V, and Kumar A. Secure Audio Transmission Using Steganography. Proc. Int. Conf. on Communication and Signal Processing, 2021.
3. Pathak A, Yadav D, and Bhatnagar R. Quantum Steganography Protocols: A Review. Quantum Information Processing, 2018;17(5):1–18.
4. Panigrahi R, Mishra B, and Dash P. An Effective Steganographic Technique for Hiding the Image

Data Using the LSB Technique. International Journal of Computer Applications.2020;177(33):7–12.
5. Sharma A, Gupta S. An Efficient Audio Steganography Technique to Hide Text in Audio. International Journal of Innovative Research in Computer and Communication Engineering. 2019;7(5):2459–2465.
6. Teja P, Kumar VP. Enhancing steganography security: A dual layer approach with LSB and AES algorithm. Lect Notes Netw Syst. 2023;697:349–359.
7. Jiang N, Zhao N, Wang L. LSB based quantum image steganography algorithm. Int J Theor Phys. 2016;55(3):1435–1447.
8. Khan M, Rasheed A. A secure controlled quantum image steganography scheme based on the MCEQI model. Quantum Inf Process. 2023;22(7):254.
9. Islam M. A hybrid secured approach combining LSB steganography and AES using pixel locator sequence. SN Comput Sci. 2022;3(3):216.
10. Moumen A, Sissaoui H. Images encryption method using steganographic LSB method, AES and RSA algorithms. Netw Model Anal Health Inform Bioinform. 2016;5(1):10.