IT468 Project Report on

Quantum Steganography using MVIsb-MQFS

Submitted in fulfillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
INFORMATION TECHNOLOGY
by

Madhav Dhingra (221IT042)
Sricharan Sridhar (221IT066)

under the guidance of

Prof. Bhawana Rudra

DEPARTMENT OF INFORMATION TECHNOLOGY
NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA
SURATHKAL, MANGALORE - 575025

October, 2025

ABSTRACT

Existing quantum steganography methods, particularly those reliant on the common Least Significant Bit (LSB) approach, face significant challenges that limit their practical application. A central problem is that these methods are primarily designed for fixed-point data, which is an inefficient representation for complex signals. When applied to more common floating-point signals, these traditional methods suffer from considerable precision loss and error accumulation. This fundamental limitation severely restricts both the potential data embedding capacity and the overall security of the hidden information. Compounding this issue, the use of traditional sequential embedding techniques makes hidden messages vulnerable to detection and extraction by unauthorized parties. To address these critical gaps, this work introduces and theoretically details the MVlsb-MFQS algorithm, a novel quantum steganography scheme. This algorithm is specifically designed to apply the LSB technique to a multichannel floating-point quantum representation (MFQS) of digital signals. The core innovation for capacity is leveraging the MFQS model, which enhances information hiding by augmenting the number of available channels for the LSB approach, thereby directly increasing the data embedding capacity. The MVlsb-MFQS algorithm also integrates multiple layers of security. It improves security and reduces time complexity by implementing a non-sequential embedding process, which uses a specific modulo value for encoding rather than a predictable sequential method. Furthermore, the algorithm employs channel qubits and position qubits as novel carriers for encoding the secret data, adding another dimension of security. To achieve an even higher degree of security, the research proposes transferring the entire steganographic operation into the quantum Fourier transformed domain. This comprehensive approach, combining a floating-point model with non-sequential, multi-carrier embedding in the frequency domain, is concluded to offer significant improvements in both embedding efficiency and security compared to existing methods.

Keywords— steganography, quantum key, encrypt, security, embedding, attacks

CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Overview

Information hiding is a fundamental component of secure communication, serving to enhance the reliability and confidentiality of data transmission. This paper proposes and theoretically details the MVlsb-MFQS quantum steganography algorithm, a novel scheme designed to operate on a multichannel floating-point quantum representation (MFQS) of digital signals. The core objective is to design and construct a quantum steganography algorithm that successfully applies the Least Significant Bit (LSB) technique to this MFQS model.
The primary contributions of this algorithm are fourfold:

I Enhanced Capacity: It aims to increase the data embedding capacity by leveraging the MFQS model, which augments the number of available channels for the LSB approach.

II Non-Sequential Embedding: It enhances security and reduces time complexity by implementing non-sequential embedding using a specific modulo value, rather than a predictable linear method.

III Novel Carriers: It introduces the use of channel qubits and position qubits as novel carriers for encoding information.

IV QFT Domain Operation: It proposes a further security enhancement by transferring the entire steganographic operation to the quantum Fourier transformed domain.

1.2 Motivation

Quantum steganography represents an advanced frontier in information security, offering distinct advantages over classical methods. Digital signals like audio, images, and video are commonly used as carriers due to their large size, which allows them to

hide more information. However, the field faces significant challenges that motivate this research.

The central problem is that current quantum steganography methods, particularly those using the LSB approach, are primarily designed for fixed-point data. This design choice creates critical issues when these methods are applied to more complex, and common, floating-point signals. The consequence is precision loss and the accumulation of errors, which severely restricts both the embedding capacity and the overall security of the hidden data.

Furthermore, many traditional steganographic techniques rely on sequential embedding. This predictable pattern makes the hidden message vulnerable, as it is relatively easy for unauthorized parties to detect and extract the secret data. While it is known that floating-point numbers can be more efficient and save on the number of qubits required compared to fixed-point numbers, research into floating-point quantum steganography is still in its early stages. This paper directly addresses this research gap by proposing a robust algorithm specifically for the floating-point domain, designed to overcome the limitations of capacity and security inherent in existing methods.

CHAPTER 2

LITERATURE REVIEW

2.1 Background and Related Works

A comprehensive survey of quantum image steganography from 2022 provides a broad classification of existing techniques, including LSB, EMD, and transform domain methods [1]. This survey highlights the persistent challenges in the field, namely the critical trade-off between capacity, security, and robustness, and points to emerging trends like the use of chaotic systems and machine learning [1].

The foundational LSB approach, while common, has been a primary target for steganalysis. A 2020 protocol, for example, was designed specifically to detect hidden messages in LSB-based stego-images [2]. It proved to be an effective countermeasure by measuring the coherence of the quantum states to distinguish them from original cover images [2]. This vulnerability has driven research toward more advanced methods. To improve security, a 2022 scheme utilized the principles of quantum walks to determine embedding locations [5]. This created a non-sequential, pseudorandom embedding pattern, which significantly increased security against statistical attacks when compared to simple linear LSB embedding [3].

To improve embedding capacity and imperceptibility, researchers have developed alternatives to basic LSB modification. A 2021 protocol adapted the classical EMD algorithm for the quantum domain, which successfully reduced distortion in the cover image and showed increased resistance to steganalysis [4]. Another 2021 paper developed a high-capacity scheme by embedding data into pixel values generated by a novel quantum interpolation algorithm, rather than just modifying existing bits [5]. Similarly, a 2023 scheme leveraged the Hue-Saturation-Intensity (HSI) color model to hide data in the less perceptually significant intensity (I) and saturation (S) channels, demonstrating both high capacity and enhanced security [6].

The field has also expanded beyond static images. A 2024 paper designed a steganography algorithm specifically for quantum audio signals, using entanglement-assisted modulation to adjust the probability of LSB modification, thereby enhancing imperceptibility [7]. In response, sophisticated steganalysis techniques for audio have also emerged, with a 2024 paper employing a Quantum Support Vector Machine (QSVM) to achieve high accuracy in detecting hidden content [8]. Other novel approaches include a 2025 paper that introduced a quaternion-based quantum image representation (QIR) to enable reversible steganography, where the original cover image can be perfectly restored after data extraction [9]. This body of work is part of the broader evolution of Quantum Secure Direct Communication (QSDC), which, as a 2024 survey charts, is seen as a critical component on the path to a future, secure "Qinternet" [10].

2.2 Outocome of Literature Review

The literature review reveals a clear and consistent trend: the field is moving away from simple LSB methods due to their proven vulnerabilities. Steganalysis protocols, whether based on quantum coherence or quantum machine learning, have demonstrated the high detectability of basic steganographic content. This has driven the research community to focus on enhancing three key areas: capacity, security, and robustness.

Security enhancements are primarily achieved by moving away from predictable, linear embedding patterns. The success of methods using quantum walks and the EMD algorithm shows a clear preference for non-sequential or pseudorandom embedding locations that resist statistical attacks. Capacity improvements are being realized by moving beyond simple bit modification, as seen in interpolation-based algorithms , or by leveraging more complex data representations like the HSI color model and quaternions.

Finally, the expansion into quantum audio and the development of reversible schemes indicate a maturing field. The surveys consolidate this by summarizing the state-of-

the-art and highlighting that the entire "Qinternet" concept relies on the development of robust, high-capacity, and noise-resistant protocols —precisely the limitations this project aims to address.

2.3 Problem Statement

The central problem identified from the literature and informing this project is that current quantum steganography methods using the LSB approach are primarily designed for fixed-point data. This is a significant limitation because these methods suffer from precision loss and error accumulation when they are applied to more complex floating-point signals.

This fundamental design flaw restricts both the embedding capacity and the overall security of the steganographic process. Furthermore, the field's reliance on traditional sequential embedding techniques creates a major vulnerability, making it easy for unauthorized parties to detect and extract the hidden messages.

2.4 Objectives of the Project

(1) To design and construct a quantum steganography algorithm, named MVlsb-MFQS, that is specifically designed to apply the LSB technique to a multichannel floating-point quantum representation (MFQS) of signals.

(2) To increase the data embedding capacity by leveraging the MFQS model. This model enhances information hiding by augmenting the number of available channels that can be used for the LSB approach

(3) To enhance the security of the steganographic process. This will be achieved by implementing non-sequential embedding (using a specific modulo value) and by transferring the entire operation to the quantum Fourier transformed domain.

CHAPTER 3

PROPOSED METHODOLOGY

3.1 MVIsb-MQFS

The core of the proposed methodology is the MVlsb-MFQS (referred to as MVI-MQFS in some diagrams) algorithm, which outlines the complete steganographic process from sender to receiver.

On the sender's side, the process begins with data preparation. Both the secret message (e.g., text) and the cover signal (e.g., an audio file or image) are converted into their respective binary string representations. A critical preliminary step is length encoding: the length of the secret message bitstream is calculated, converted into a 32-bit binary string, and then embedded into the first 32 bits of the carrier signal's bitstream. This 32-bit header is essential as it informs the decryption algorithm exactly how many bits of data to read, preventing errors.

To enhance security, the carrier signal is converted into the quantum Fourier transformed domain. This transfers the entire operation from the spatial or time domain to the frequency domain, making the embedded data more difficult to detect. The embedding itself is performed non-sequentially. The algorithm steps through the carrier's bitstream using a fixed 'modulo_value'. At each designated position, it hides one bit of the secret message. The embedding mechanism is a quantum XOR operation. At each position, the original carrier bit (host bit) and the corresponding secret message bit are used as inputs to a quantum circuit. A Controlled-NOT (CX) gate performs the quantum XOR, and the resulting stego bit overwrites the original host bit.

On the receiver's side, decryption is the reverse of this process. The receiver, who must possess the original, unaltered cover signal, first extracts the 32-bit header to know the message length. They then read the bits from the stego signal and the original signal at the same positions, which are determined by the same 'modulo_value'.

By applying the same quantum XOR operation ('stego_bit' XOR 'host_bit'), the original secret bit is perfectly recovered.

3.2 Handling Floating Point Numbers

A fundamental motivation for this methodology is to overcome the limitations of existing quantum steganography schemes. The central problem is that current methods are primarily designed for fixed-point data, which results in significant precision loss and error accumulation when applied to more complex floating-point signals. This limitation restricts both embedding capacity and security.

The proposed MVlsb-MFQS algorithm is explicitly designed to address this gap. The methodology is built to apply the LSB technique to a multichannel floating-point quantum representation (MFQS) of signals. While classical floating-point numbers can save on the number of qubits compared to fixed-point numbers , research in this quantum area is still early. The MFQS model is key to enhancing the ability to hide information. By increasing the number of available channels, it directly boosts the embedding capacity of the LSB approach, allowing for more data to be hidden within the floating-point representation without the precision loss associated with fixed-point methods.

3.3 Salience Maps

A novel enhancement to this methodology is proposed, specifically for image steganography, which integrates machine learning to improve imperceptibility. The core idea is to use salience maps to identify the best (least noticeable) locations within an image to hide data. It is generally understood that hiding data in the darker, non-salient, or background portions of an image makes it much harder to detect the steganographic data using basic preprocessing or visual inspection.

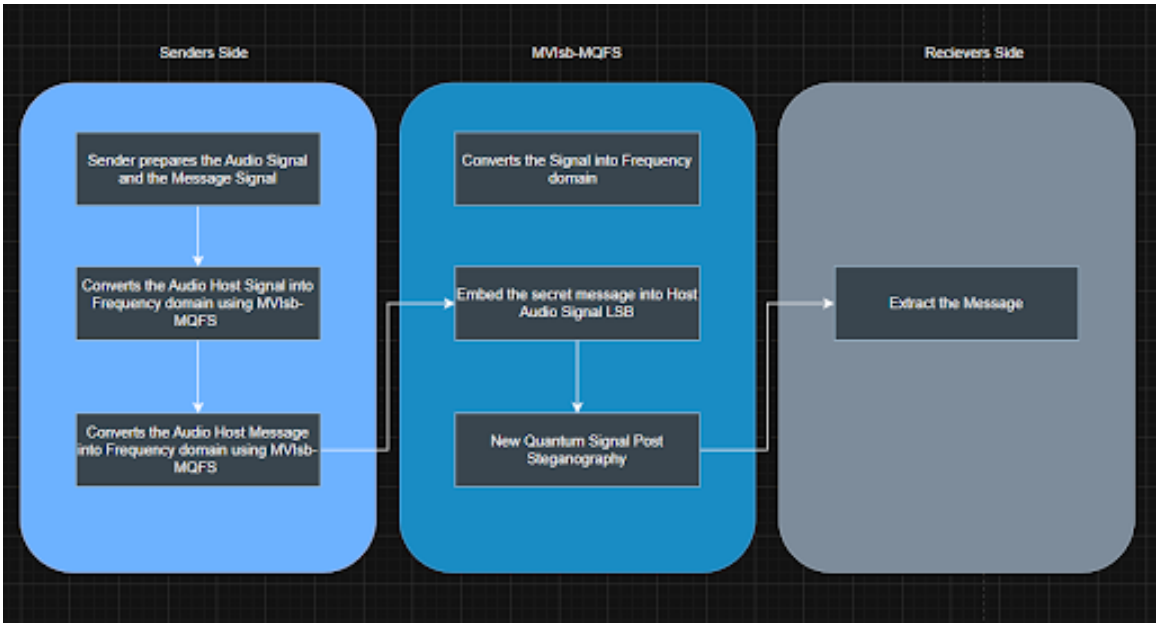

Figure 3.2.1: MVIsb-MQFS Workflow

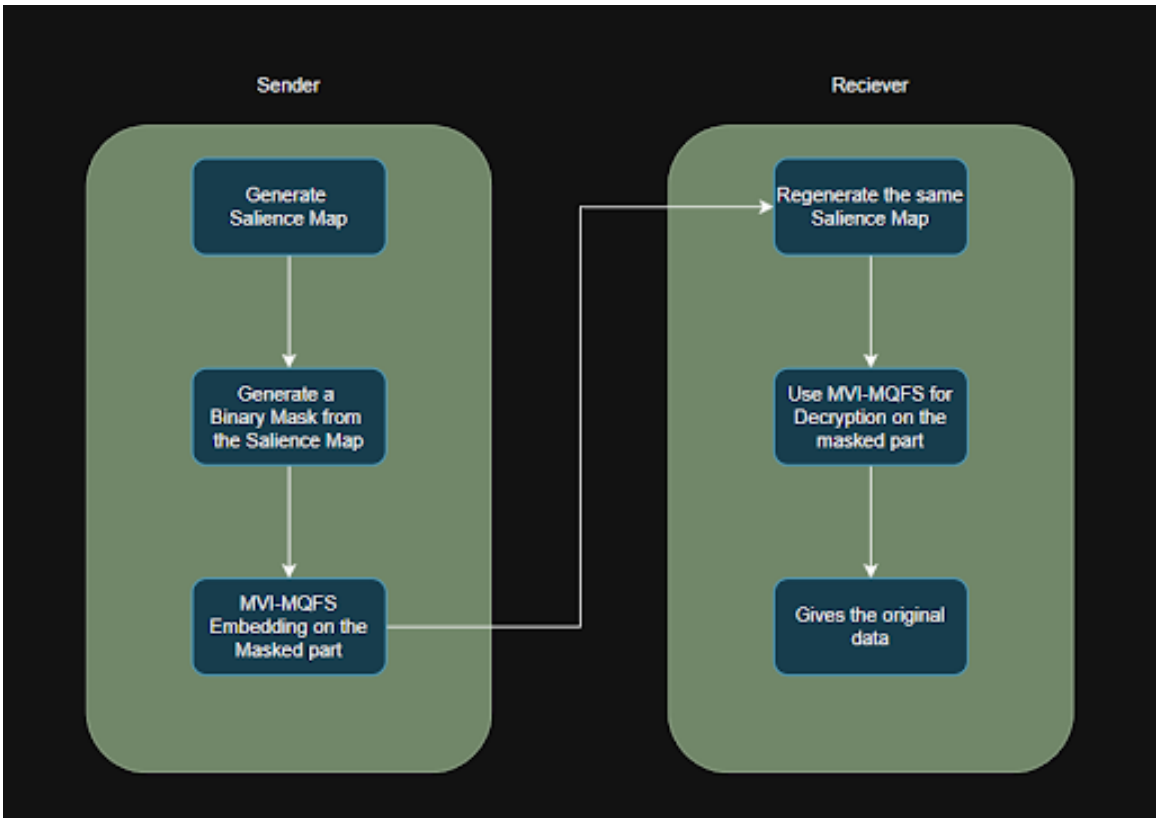

Figure 3.2.2: Salience Map based MVIsb-MQFS

The proposed process for this enhancement is as follows:A novel enhancement to this methodology is proposed, specifically for image steganography, which integrates machine learning to improve imperceptibility. The core idea is to use salience maps to identify the best (least noticeable) locations within an image to hide data. It is generally understood that hiding data in the darker, non-salient, or background portions of an image makes it much harder to detect the steganographic data using basic preprocessing or visual inspection.

The proposed process for this enhancement is as follows:

I Generate Salience Map: The sender first analyzes the cover image with a pre-trained AI model, such as MiDaS, to generate a salience or depth map.

II Identify Non-Salient Regions: This map identifies the non-salient background areas of the image—regions where modifications are less likely to be perceived by a human observer.

III Create Binary Mask: A binary mask is then created from this salience map, marking all non-salient pixels as "safe" for embedding data.

IV Embed Data: The MVI-MQFS (MVlsb-MFQS) embedding methodology, including the modulo-based non-sequential embedding, is then applied only to the pixels designated by this binary mask.

V Decryption: To decrypt the message, the receiver must use the same logic. They regenerate the exact same salience map from the original cover image. This allows them to identify the precise masked locations from which to apply the MVI-MQFS decryption process and successfully retrieve the original hidden data.

CHAPTER 4

RESULTS AND ANALYSIS

4.1 Demonstration of Salience-Based Masking

The results presented visually demonstrate the successful operation of the novel, AI-enhanced component of the proposed methodology. This component is designed to intelligently select embedding locations in an image to maximize imperceptibility. The presentation provides two images. The first is the original cover image, which is a photograph of a spiral stained-glass window. This image features a complex interplay of bright, colorful, and dark, non-descript regions.

The second image is the direct output of the analysis performed by the pre-trained AI model, MiDaS, as described in the methodology. This image is the generated salience map. In this visualization, the AI model has identified the most salient (prominent, bright, or in-focus) features of the window, which are covered by a distinct red overlay. Conversely, the non-salient or background areas—the darker, less-focused, or perceptually less significant parts of the image—are left uncovered.

This map is not the final stego-image itself; rather, it is the blueprint for the embedding process. From this salience map, a binary mask is created, which marks all the non-salient (uncovered) pixels as the "safe" locations for data embedding. This visual result confirms the successful operation of the AI model in programmatically distinguishing between perceptually important and unimportant regions of the cover image.

4.2 Analysis of the Proposed Novelty

The successful generation of this salience map is a crucial result, as it directly supports the project's objective of enhancing security and imperceptibility. The analysis of this result is based on the core premise outlined in the methodology: it is better

Figure 4.1.1: Cover Image

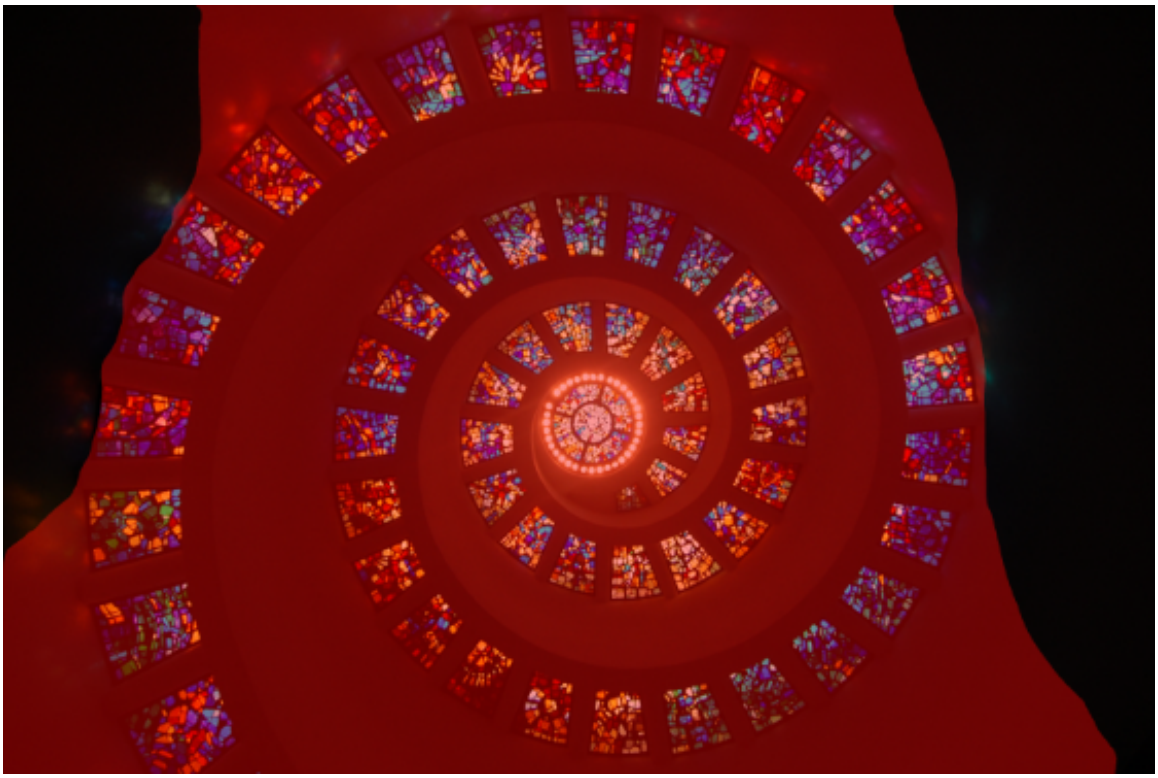

Figure 4.1.2: Stego Image

to hide data in the darker, non-salient portions of an image, because identifying the stego data using basic preprocessing becomes much harder.

By using an AI-driven approach to select embedding locations, the proposed method avoids the critical flaw of naive LSB steganography. Standard LSB modification might alter bits in a highly visible, salient area (like the bright center of the stained glass), creating detectable anomalies. The novel methodology, however, ensures that modifications are restricted only to regions where they are less likely to be noticed by a human observer.

This approach enhances security on two fronts:

I Against Human Inspection: It significantly reduces the risk of the hidden message being detected by simple visual inspection.

II Against Statistical Analysis: By embedding data in seemingly random, non-linear locations dictated by the image's content (the non-salient regions), it increases resistance to basic statistical attacks that hunt for the unnatural, uniform patterns often left by simpler embedding algorithms.

This AI-generated mask is the new image medium upon which the MVI-MQFS (MVlsb-MFQS) methodology is then applied. This result is also critical for the decryption process, as the receiver must be able to regenerate the exact same salience map to identify the masked parts and successfully extract the original data. The clear and well-defined map shown in the results demonstrates the feasibility and reliability of this deterministic, AI-driven masking process, validating it as a significant enhancement to the overall quantum steganography framework.

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

Based on the theoretical design of its quantum circuits and operational flow, the proposed MVlsb-MFQS scheme is concluded to offer significant improvements in both embedding efficiency and security when compared to existing methods. By leveraging a multichannel floating-point representation (MFQS), the algorithm directly addresses the precision loss and capacity limitations inherent in fixed-point schemes. Security is systematically enhanced by rejecting traditional sequential embedding in favor of a modulo-based non-sequential approach and by transferring all operations to the quantum Fourier transformed domain. The novel addition of an AI-driven salience map for image steganography further hardens the method against human-perceptual detection and basic preprocessing attacks.

The future work for this research aligns with the broader goals of the quantum communications field. The immediate and logical progression from this theoretical framework is to move into practical implementation and empirical validation. This would involve simulating the quantum circuits required for the MVlsb-MFQS algorithm and its novel, salience-based variant.

A comprehensive performance evaluation would be the next critical phase. This would require rigorously testing the algorithm's core claims, such as:

I Quantitatively measuring the increased embedding capacity afforded by the multichannel floating-point quantum representation (MFQS) model.

II Evaluating the imperceptibility of the stego-signal, using standard metrics like Peak Signal-to-Noise Ratio (PSNR) for the AI-enhanced image methodology.

III Conducting a thorough security analysis by subjecting the algorithm to the very steganalysis techniques identified in the literature, such as coherence-based detection protocols and advanced quantum machine learning (Q-SVM) detectors.

IV Optimizing the AI-driven methodology by testing different models beyond MiDaS to find the optimal balance between safe embedding zones and data capacity.

This research path directly contributes to the field's grander objectives. The literature review highlights the ongoing evolution of Quantum Secure Direct Communication (QSDC) and its foundational role in the path toward a fully realized, secure "Qinternet". The successful development, optimization, and practical implementation of robust, high-capacity, and noise-resistant protocols are identified as critical steps toward achieving this future quantum internet. The MVlsb-MFQS algorithm, with its focus on high-capacity floating-point data and enhanced security, is precisely one such protocol. Therefore, the long-term goal of this work is to validate this algorithm as a practical, efficient, and secure component for the next generation of quantum communication.

REFERENCES

[1] N. Min-Allah, N. Nagy, M. Aljabri, M. Alkharraa, M. Alqahtani, D. Alghamdi, R. Sabri, and R. Alshaikh. Quantum image steganography schemes for data hiding: A survey. *Applied Sciences*, 12(20):10294, 2022.

[2] Z. Qu, Y. Huang, and M. Zheng. A novel coherence-based quantum steganalysis protocol. *Quantum Information Processing*, 19(11):362, 2020.

[3] R. Abd-El-Atty, A. A. Iliyasu, H. Alaskar, A. A. El-Latif, and S. E. Abd-El-Atty. A novel image steganography scheme based on quantum walks. *Symmetry*, 10(16):2870, 2022.

[4] Z. Qu, H. Sun, and M. Zheng. An efficient quantum image steganography protocol based on improved EMD algorithm. *Quantum Information Processing*, 20(2):53, 2021.

[5] S. Zhao, F. Yan, K. Chen, and H. Yang. Interpolation-based high capacity quantum image steganography. *International Journal of Theoretical Physics*, 60(11):3722–3743, 2021.

[6] J. Sun, W. Wang, P. Yan, and H. Zhang. Quantum steganography scheme and circuit design based on the synthesis of three grayscale images in the HSI color space. *Quantum Information Processing*, 22(10):349, 2023.

[7] C. Hao, X. Yang, Q. Ma, D. Qu, R. Wang, and T. Zhang. Quantum audio LSB steganography with entanglement-assisted modulation. *Quantum Information Processing*, 23(3):106, 2024.

[8] J. Chaharlang, M. Mosleh, and S. Rasouli-Heikalabad. Quantum reversible audio steganalysis using quantum Schmidt decomposition and quantum support vector machine. *Journal of Information Security and Applications*, 82:103755, 2024.

[9] R. Deepika, K. Thirugnanasambandam, and K. Muthunagai. QIR: A novel quaternion-based image representation for reversible image steganography. *Connection Science*, 37(1):2507830, 2025.

[10] D. Pan, G. L. Long, L. Yin, Y. B. Sheng, D. Ruan, S. X. Ng, J. Lu, and L. Hanzo. The evolution of quantum secure direct communication: On the road to the Qinternet. *IEEE Communications Surveys & Tutorials*, 26(3):1898–1949, 2024.