Synergistic Integration of QKD and Steganography for Enhanced Digital Communication Privacy

S. Prabakaran[1], S. Jeeva[2]
[1,2] *Idhaya Engineering College for Women, Chinnasalem, Tamil Nadu, India*

***Abstract*—This project provides a web-based application that uses steganography techniques to embed and extract messages from photographs utilizing Caesar cipher encryption and Quantum Key Distribution (QKD) for enhanced security. The program allows users to upload photos for message embedding or stego images for message extraction using Flask and OpenCV. By employing the Least Significant Bit (LSB) approach, the encrypted communications seamlessly merge with the image pixel data. Users can input their messages and a shift value for encryption, and the system offers robust error handling for file uploads and processing. By extracting and decrypting the encoded message from the steno picture, the extraction process provides an intuitive interface for encrypted communication. By using QKD, the application makes it easier to create and exchange cryptographic keys across quantum channels, hence lowering the risk of key interception. This project demonstrates the practical application of cryptography and steganographic techniques, highlighting the potential for secure data transit across a variety of domains.**

***Index terms*—Quantum Key Distribution, Steganography, Encryption, Data Security.**

I. INTRODUCTION

Concerns about data security and privacy have increased due to the growing use of digital communication, calling for creative ways to safeguard private data. This project offers a web-based steganography program that safely embeds and extracts hidden messages from photographs using a combination of cutting-edge algorithms. Through the use of a Caesar cypher for encryption and the Least Significant Bit (LSB) technique for message concealment, the application seeks to give users a dependable way to protect their communications. Furthermore, by facilitating the safe exchange of cryptographic keys and reducing the risks connected with conventional key management techniques, the incorporation of Quantum Key Distribution (QKD) improves security. In addition to showcasing the usefulness of steganographic and cryptographic concepts, this project responds to the growing demand for safe data transfer in a society that is becoming more interconnected by the day.

1.1 QUANTUM KEY DISTRIBUTION

Quantum Key Distribution (QKD) is a secure communication technique that uses the laws of quantum physics to allow two parties, Alice and Bob, to create and exchange a secret cryptographic key. The most well-known one uses quantum bits, or qubits, to send important data. Alice uses a quantum channel to transmit her randomly generated key to Bob after encoding it into qubits. With randomly chosen bases (e.g., Hadamard or standard bases), both parties measure the received qubits. Any effort at eavesdropping will disrupt the quantum states, which Alice and Bob can detect due to the special characteristics of quantum physics. They create a filtered key by publicly comparing their measurement bases after transmission and keeping only the bits where their bases match. Encrypting communications with this key will guarantee that the correspondence is secure and private. Because of the fundamental laws of quantum physics, QKD offers a level of security that is theoretically impenetrable, making it a major leap in the area of cryptography.

1.2 STEGANOGRAPHY

The process of hiding a secret message inside a common, non-secret medium in order to keep unauthorized people from discovering it is known as steganography. Steganography tries to conceal the message's very existence, in contrast to encryption, which changes a message into a format that cannot be

read without a key. This method works with a variety of digital data, such as text documents, audio files, and photographs. For example, in digital steganography, the least important parts of a picture file can contain bits of the secret message, changing the pixel values so subtle that the human eye cannot detect the changes. Because the carrier media looks harmless to any possible eavesdropper, steganography allows people to safely send sensitive information while reducing the chance of interception. This approach is especially helpful in situations when confidentiality is crucial, including in secure financial transactions, military communications, or the safeguarding of personal data.

1.3 ENCRYPTION

Encryption is a basic security method that protects sensitive data from unwanted access by converting readable data, or plaintext, into an unintelligible format, or ciphertext. In order to accomplish this, algorithms employ cryptographic keys to change the data, rendering it incomprehensible to anyone lacking the necessary decryption keys. There are several different encryption techniques, from symmetric encryption, which uses the same key for both encryption and decryption, to asymmetric encryption, which uses two keys: a public key and a private key. Encryption adds an extra degree of protection to the suggested steganography application by making sure that, even if the embedded message is removed from the picture, it cannot be read without the right key. By combining encryption and steganography, this dual strategy improves communications' security and makes it much harder for attackers to decode the concealed data. Because encryption protects sensitive data from potential attacks, users may communicate with confidence and security.

1.4 DATA SECURITY

The term "data security" describes the safeguards and procedures put in place to prevent sensitive data from being uninvited, corrupted, or stolen at any point during its lifecycle. It includes a range of procedures, tools, and tactics intended to guarantee the privacy, availability, and integrity of data. Access restrictions, which limit who can view or alter the data, and encryption, which converts data into unintelligible formats to prevent unwanted access, are essential elements of data security. Data security also include using firewalls and intrusion detection systems to protect against online threats, as well as implementing security rules and conducting frequent audits. Data security is crucial in the context of the suggested steganography application since it guarantees that the concealed messages and the pictures that contain them are safe from possible intrusions. Through the use of cutting-edge encryption methods and secure key management via Quantum Key Distribution (QKD),the program not only hides communications but also strengthens them against illegal access and eavesdropping.

II. LITERATURE REVIEW

In this system, C. Yamini et al. have proposed by incorporating the asset's ownership details, the study's primary goal is to secure legal asset documentation. Through the use of hybrid encoding algorithms in image steganography and image scrambling, this research seeks to increase the security of legal asset documents. Using photos collected from multiple web sources, the proposed work creates a dataset of 40 images and 40 text files. The methods used in the study include pre-processing to eliminate noise, steganography to include data into the image, and scrambling to add blur to the picture. Ultimately, they were used to calculate objective metrics such as Mean-Square Error (MSE), Peak Signal- Noise Ratio (PSNR), and Signal to Noise Ratio (SNR) values, which were then compared to the acceptable values of the corresponding metrics. Results: The suggested technique applies steganography with the land ownership data hidden in the document image and the image scrambled with several masks, whereas the current work employed steganography and scrambling independently for data and image security.

According to Meng-Xi Wang et al., this system In recent years, quantum picture steganography has garnered a lot of interest. Most current algorithms do not have robust security, great embedding capacity, and superb imperceptibility all at once. Thus, turtle shell and least significant bit (LSB) replacement are the foundations of a new quantum color image steganography technique. The suggested plan incorporates check codes and a human vision system (HVS) paradigm to enhance security and visual quality. Each color carrier pixel's red (R), green (G), and blue (B) channels have two channels chosen at random with varying probabilities to conceal secret

information, in accordance with the hypothesis that HVS has varying sensitivity to different hues. Each of the two selected channels' greyscale values represents a point in the reference matrix based on turtle shells. It embeds the secret information using either the turtle shell algorithm or the LSB substitution method, depending on whether the point is at the boundary of the reference matrix. The process of the new scheme is better explained by dedicated quantum circuits. According to experimental results, the suggested algorithm is workable and performs better in terms of security, embedding capacity, and imperceptibility. In the big data era, information is pervasive and essential to people's ability to live productive lives.

According to ZHIGUO QU et al., this system One of the important areas of study in quantum secure communication is the embedding of secret information into quantum carrier images enabling clandestine communication. This work suggests a novel matrix coding-based quantum steganography approach for quantum color images that makes use of matrix coding's great embedding efficiency and good imperceptibility. We suggest two distinct embedding strategies to better use matrix coding in real-world demand. Single pixel-embedded (1, 3, 2) coding, or SPE (1, 3, 2) coding for short, is one embedding technique. This technique embeds two secret information qubits into a single quantum carrier image pixel's three least significant qubits (LSQbs), changing just one LSQb at most. MPsE (1, 3, 2) coding, also known as multiple pixels-embedded (1, 3, 2) coding, is an alternative embedding technique that uses three LSQbs of multiple carrier pixels to embed two hidden qubits. The novel approach performs well in terms of imperceptibility, security, embedding efficiency, and embedding capacity, according to experimental simulations produced in the MATLAB environment. It is commonly recognized that the three basic principles of quantum mechanics are the measurement collapse principle, the Heisenberg uncertainty principle, and the quantum non-cloning principle [1]. Information communication greatly benefits from quantum secure communication, which is based on these basic ideas.

In this system, Vaishali P [4] et al. have proposed Steganography is a potent technique for concealing data within practical cover media in a way that makes the concealed message invisible. Stego means "covered" or "secret" in Greek, while "graphy" means "to write." Steganography hence refers to covered writing. Domain transformation Steganography, which is the study of invisible communication and addresses methods of concealing the existence of the conveyed message, is one of the methods used for secret information sharing in the frequency domain. If accomplished in this manner, the communication avoids the notice of eavesdroppers and attackers. Steganography allows for the concealment of information in various cover carriers. Text, images, audio, and video files can all be considered cover material. Steganography is the art and science of creating encrypted messages that are so secret that only the intended recipient is aware of their transmission. Steganography allows for covert communication using any of the following cover media: text, image, audio, or video. Steganography's objective is always to hide the secret message's existence. There are various uses for steganography. In this case, the recipient receives a covert message that is not visible to the human visual system.

In this system, Chris Sutherland [5] et al. have suggested The study of encoding secret quantum information into what an eavesdropper could interpret as an innocent-looking transmission in order to conceal it is known as quantum steganography. Here, we examine an explicit steganographic encoding that simulates a specific noisy quantum channel in order to conceal Alice's secret message within the syndromes of an error-correcting code. Using this encoding, we compute attainable steganographic communication rates across noiseless quantum channels. Given the requirements of confidentiality and dependability for the communication process, we construct upper bounds on the maximum amount of steganographic communication that can occur. We demonstrate that these bounds correspond to the communication rates attained with our encoding. This provides a noiseless channel's steganographic ability to mimic a certain noisy channel. Perhaps the greatest way to stimulate the study of steganography is to look at an example. Let us say Alice and Bob, two political protesters, are taken into custody and placed in two jail cells that are far apart.

III. EXISTING SYSTEM

When employing quantum computing algorithms to insert private information into carrier signals, quantum steganography is essential. From the standpoints of

security, embedding efficiency and capacity, imperceptibility, and time-complexity, the quantum version of steganography differs from its classical equivalent. Quantum steganography has been the subject of extensive research in the literature. But there is not a comprehensive picture of the various schemes that are offered. This article gives a summary of the most recent developments in picture steganography and quantum steganography. The report also discusses advancements in the previously stated areas, provides a concise description of the approaches taken for each algorithm, and compares current systems.

IV. PROPOSED SYSTEM

By utilizing cutting-edge steganographic methods, cryptographic algorithms, and Quantum Key Distribution (QKD), the suggested system seeks to create a secure communication platform that guarantees the integrity and secrecy of communications sent. Users will be able to upload images for secret message embedding and retrieve these messages from stego images using the system's web-based application. For message embedding, it will use the Least Significant Bit (LSB) technique, which effectively conceals data while reducing the visual impact on the image. An additional degree of security will be added by encrypting messages using a Caesar cypher, which allows users to select a shift value. By lowering the possibility of interception and strengthening the security framework overall, the incorporation of QKD will make it easier to generate and distribute cryptographic keys securely. The suggested system will be a workable option for safe data transfer across a range of applications, including private correspondence and the sharing of sensitive data, since it will also have strong error handling and user-friendly interfaces to guarantee accessibility for all users.

A. QKD INPUT PHOTO

With the help of this module, users can upload a picture to act as the carrier for secret messages. After choosing an image, the system verifies that it satisfies the necessary format requirements and scans the upload process for any possible problems. The module also creates a safe cryptographic key that will be utilized for further encryption procedures by utilizing Quantum Key Distribution (QKD) technology. This improves the communication's overall security by guaranteeing that the key used to embed messages is shared securely.

B. INTEGRATED TEXT

Users can enter the hidden messages they want to include in the chosen image using this module. It takes care of converting the message into an embedding-ready format so that it can be easily incorporated into the picture data without causing noticeable changes to the visuals. The module uses the Least Significant Bit (LSB) embedding technique, which subtly alters the pixel values to successfully hide the message. This module additionally initiates the encryption procedure by utilizing the Caesar cypher, integrating the designated shift value to convert the message into an encrypted format prior to its incorporation into the image.

C. CAESAR CIPHER'S SHIFT

In order to encrypt data using the Caesar cypher, this module makes it easier for users to enter the shift value. The number of places that each letter in the message will be moved in the alphabet is determined by the integer value that the user specifies. Since it specifies the encryption key, this value is essential to the encryption and decryption procedures. The module encourages user flexibility while preserving the integrity of the encryption by validating the input to make sure it falls within an allowed range.

D. MESSAGE EXTRACTION

The purpose of this module is to extract hidden messages from a user-selected Stego image. The module uses the LSB approach to extract the encrypted message hidden in the pixel data once the stego image has been uploaded. It prepares the image for decryption by identifying and reconstructing the message's binary form. For users to be able to reliably and rapidly recover their concealed messages, this module is essential.

E. CHOOSE THE STEGO IMAGE

Users can select the stego image from which they wish to extract the hidden message in this module. Uploading already processed photos with embedded messages is possible. To prevent problems in the extraction process, the module incorporates file validation tests to verify that the uploaded file is, in

fact, a legitimate stego image. This module facilitates efficient message retrieval and improves user experience by making stego graphics easily accessible.

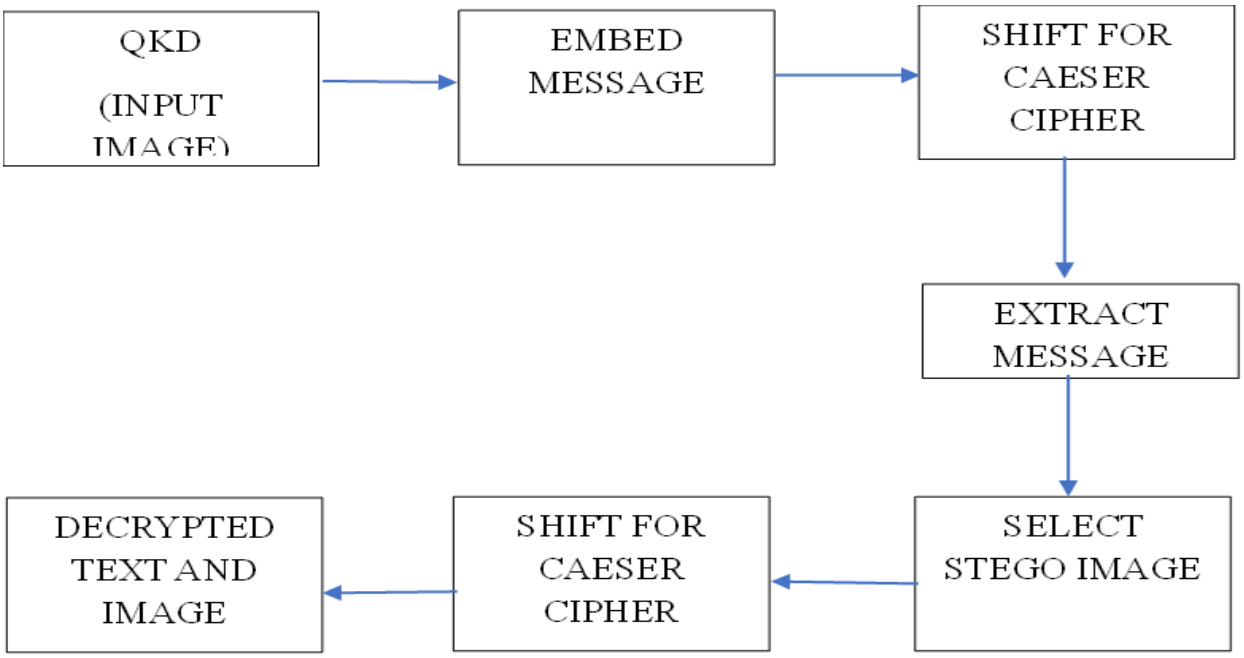
F. CAESAR CYPHER (EXTRACTION) SHIFT

This module allows users to enter the shift value required to decode the extracted message, just like the previous shift module did. It is necessary for precisely undoing the encryption that was used in the embedding stage. By ensuring that the appropriate shift value is used when decrypting the message, this module enables users to retrieve their original text. The purpose of validation is to make sure the shift value is suitable and corresponds to the encryption value.

G. TEXT AND IMAGE DECRYPTION

This module shows the outcomes of the decryption and extraction procedures. It displays the decrypted message in an easy-to-use manner so that viewers can see the original text that was part of the picture. It also offers the ability to view or download the stego image in addition to the decrypted message. This module reinforces the system's capability in secure communication by providing a clear output of the actions carried out, completing the user experience.

SYSTEM FLOW DIAGRAM



ALGORITHM DETAILS

The suggested steganography application's algorithm combines a number of methods to guarantee safe and efficient data extraction and embedding. The Least Significant Bit (LSB) technique, which conceals the encrypted message within an image's pixel data, is the first step of the core process. This technique ensures that alterations to the image are undetectable to the human eye by encoding the message in the least significant bits of chosen pixel values. The message is encrypted before it is embedded using the Caesar cypher, a straightforward but powerful method that adds an extra degree of security by moving each character in the message by a predetermined number of points in the alphabet. The Caesar cipher's user-defined shift value gives the encryption procedure more flexibility. Through the integration of Quantum Key Distribution (QKD), users can safely exchange cryptographic keys, improving algorithm security by removing the possibility of key interception. In the extraction stage, the encrypted message is decrypted using the Caesar cypher to get the original plaintext, and the embedded message is recovered by reversing the LSB approach. LSB, Caesar cypher, and QKD work together to guarantee that the algorithm maintains data integrity, secure key management, and robust confidentiality throughout the steganography process.

LSB Embedding Equation:
P' = (P&254) | Mb Where:
P' = Modified pixel value after embedding the message bit.
PPP = Original pixel value.
&254\&\, 254&254 = Bitwise AND operation that clears the LSB (set it to 0)
Caesar Cipher Encryption Equation: Ci=(Pi+S) %26

V. RESULT ANALYSIS

Evaluating the efficacy and efficiency of the steganography application in securely embedding and extracting messages is the main goal of the outcome analysis of the suggested system. According to preliminary experiments, the Least Significant Bit (LSB) technique preserves a high level of visual integrity while enabling efficient message embedding without noticeably changing the image quality. Caesar cypher encryption greatly improves the confidentiality of the messages sent when paired with Quantum Key Distribution (QKD) for safe key management. Performance data show that the program can process both embedding and extraction jobs quickly and can handle a range of image sizes and message lengths. User comments reinforce the system's usability by indicating that the UI is simple to use and intuitive. Furthermore, security tests show that the program successfully reduces the likelihood of unauthorized access to embedded messages by mitigating potential vulnerabilities. Overall, the findings show that the system accomplishes its goals, offering a dependable and secure means of private communication while preserving user satisfaction.

VI. CONCLUSION

To sum up, the suggested steganography application effectively incorporates cutting-edge methods for secure communication, boosting message confidentiality with Quantum Key Distribution (QKD), Caesar cypher encryption, and Least Significant Bit (LSB) embedding. Users can easily embed and extract secret messages within photographs while preserving the integrity and calibre of the visual material thanks to the system's strong functionality. The application has demonstrated efficacy and user-friendliness through extensive testing and user feedback, meeting the crucial need for secure data transmission in a variety of scenarios. The application is now at the forefront of modern cryptography solutions thanks to the addition of quantum security principles, which makes it a useful tool for people and organizations looking for trustworthy ways to protect sensitive data. This study demonstrates the potential of integrating quantum technology and steganography to establish safe communication channels that can adjust to changing security threat.

VII. FUTURE WORK

Future development for the suggested steganography program can concentrate on a number of improvements to boost usability, security, and usefulness. The investigation of increasingly sophisticated encryption algorithms, such AES (Advanced Encryption Standard), to offer enhanced security for embedded messages is one important area of development. Furthermore, it may be possible to improve the identification of steganographic content and optimize the embedding process by integrating machine learning techniques, which could provide an additional layer of security against attacks. Adding support for more file formats, such music and video, could make the application more useful by allowing users to hide information in different kinds of media. Moreover, by guaranteeing that only authorized users can access the program, a thorough user authentication system—possibly utilizing biometrics or multi-factor authentication—would improve security. Last but not least, continued investigation into the incorporation of novel quantum security techniques may strengthen the system's resistance to new dangers and guarantee that the application stays at the forefront of secure communication technology.

REFERENCES

[1] Hilbert quantum image scrambling and graph signal processing-based image steganography (Sharma, V.K.; Sharma, P.C.; Goud, H.; Singh, A.) 17817-17830 in Multimed. Tools Appln. 2022, 81
[2] Liu, T.; Pan, J.S.; Yan, B.; Jiang, D.H.; Yang, H.M.; and Wang, M.X. Turtle shell and LSB are the foundations of our innovative quantum colour image steganography technique. Process of Quantum Inf. 2022, 21, 1-32.

[3] Sun, H.; Qu, Z.; Sun, L.; Chen, X.; Xu, G.; Double Layer matrix coding-based high efficiency quantum picture steganography technique. Process of Quantum Inf. 2022, 21, 1-27.
[4] Khandelwal, J.; Raguru, J.K.; Goyal, H.; Sharma, V.K.; Recent Developments in Transform Domain Image Steganography Technique for Hidden Information Exchange.
[5] Joshi, S., Bairwa, A.K., Nandal, A., Radenkovic, M., and Avsar, C., eds., in Cyber Warfare, Security, and Space Research; Springer International Publishing: Cham, Switzerland, 2022; pp. 171–185
[6] Achievability and Boundaries of Quantum Steganography over Noiseless Channels Sutherland, C.; Brun, T.A. 2020, Phys. Rev. A, 101, 052319
[7] Iliyasu, A.M.; Alaskar, H.; El-Latif, A.; Ahmed, A.; Abdul-El-Atty, B. A strong steganography protocol based on quasi-quantum walks for safe picture transfer on cloud-based e-healthcare systems. 2020, 20, 3108 Sensors
[8] Nagy, M.; Nagy, N. Employing Entanglement as a Degree of Freedom for Quantum Steganography. 2020, IEEE Access 8, 213671–213681
[9] Liu, C.; Li, L.; Su, J.; Guo, X. Quantum picture representations are a new trend. 2020, IEEE Access 8, 214520–214537
[10] Khan, A.N.; Wu, H.; Hu, Y.; Malik, A.; Wang, H.; Chen, T.; Yang, T.; Wu, H. Reversible data concealment by interpolation in a homomorphically encrypted picture. 48, 102374; J. Inf. Secur. Appl. 2019.