International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0071
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 453 - 459

Quantum Key - Based Secure Image Steganography with AES Encryption

U. Gowri Sankar[1], Radhesh Kumar K M[2], Vasanth V[3], Yeswanth S[4]
[1,2,3,4] Erode Sengunthar Engineering College Erode, , 638052, and India
Emails: *gowriesec2020@gmail.com[1], radheshkumar2004@gmail.com[2], vasanthvelu0927@gmail.com[3], yesyeswanth232@gmail.com[4]*

Abstract
We are building a highly secure way of sending messages by combining the use of Quantum Key Distribution (QKD) to produce encryption keys and encrypting messages with a variant of AES-256 (a substitution cipher) and Least Significant Bit (LSB) steganography or hiding them in images. We are employing the BB84 protocol to produce these keys based on the quantum properties of the photonic (light) particles; we can detect any third parties attempting to intercept the key and measure it by the Quantum Bit Error Rate (QBER). Once we have produced a secure key, we then use it to encrypt the actual message with AES-256, and we hide that in a digital image (the cover image) with LSB steganography. Thus, if a third party were to capture the Stego image (the digital image containing the hidden encrypted message), they would not be able to decrypt the hidden message without the key that was produced using quantum cryptography. An analytics dashboard monitors the success of the key generation, the QBER value, and other performance metrics, giving a high degree of transparency and trustworthiness of the whole process.
Keywords: *Quantum Key Distribution; BB84 Protocol; LSB Steganography; Secure Communication*

1. Introduction
With the ever-increasing volume of sensitive data being transmitted over networks today, the challenge of ensuring the safety of the data during its transmission is more complex than in the past due to the rise in cyber threats and the development of new decryption techniques. The use of traditional cryptographic techniques is effective in protecting confidential information from unauthorized access; however, they will be vulnerable to future attacks of the quantum computing type, which will decrypt the classical encryption keys effortlessly. This is a huge challenge to organizations seeking to safeguard their sensitive data during transmission To overcome these challenges, this research proposes a multi-layered data security system based on the use of Quantum Key Distribution (QKD) in combination with the (AES-256) encryption algorithm and the Least Significant Bit (LSB) steganography method to ensure multi-layered data security. The use of the BB84 protocol in the proposed QKD system will ensure the secure exchange of keys based on the principles of quantum mechanics, where any attempt to intercept the key by an eavesdropper will result in a disturbance in the quantum state, which can be detected immediately. Once the quantum key has been produced and transmitted securely to the user, it can then be used in the AES-256 to encrypt the user's messages to ensure confidentiality at the cryptographic level. In addition to being cryptographically secure, to provide yet another layer of security, the encrypted message can be embedded inside a cover image using LSB steganography, thus concealing the existence of the secret message. The proposed hybrid system not only ensures that the encryption method used is secure against quantum attacks, but it also ensures that the hidden message is virtually undetectable due to its image being concealed. Therefore, the proposed hybrid system provides a comprehensive solution to the secure transmission of messages in the quantum computing age.

1.1. Quantum Key Distribution
Quantum key distribution (QKD), as the name suggests, is a technique by which two communicating entities can generate and exchange cryptographic keys with the help of secure communication, following the laws of quantum physics. The technique of QKD is different from all other conventional techniques in the sense that it relies on the properties of quantum

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0071
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 453 - 459

particles, usually photons, to ensure the security of the communication. The bits of the keys are encoded using different polarization states of the photons using the BB84 protocol, and the presence of an intruder in the communication will result in errors, known as the Quantum Bit Error Rate (QBER). Due to the presence of the intrusion-detection mechanism in QKD, the technique is very reliable and can be used to ensure the security of the data.

1.2. Stegnography

The BB84 protocol was developed by Charles Bennett and Gilles Brassard in 1984 and is currently the most used Quantum Key Distribution (QKD) protocol. This protocol uses the properties of photons to securely share a common secret key between two parties. In BB84, polarization bases are used to encode the bits. These polarization bases are rectilinear and diagonal bases. Photons are transmitted individually over a quantum channel. The receiver uses random bases to measure each photon. If both parties are using the same bases to generate a raw key, any attempt to intercept the photons will introduce errors to the photons' states. These errors are quantified by the Quantum Bit Error Rate (QBER).

1.3. Least Significant Bit

The principle of LSB steganography is based on altering the least significant bits of the pixel value of an image. The alterations made to the image are minor to the extent that any alterations in the pixel intensity of the image are not visible to the naked eye. Therefore, as two bits of the encrypted message can be embedded in the least significant bit value of one or more pixel value(s) of the original image, the stego-image is very similar to the original image. The ability of LSB steganography to produce an image that is not altered in any way can be used to conceal confidential information. This can be enhanced by the use of other encryption methods in protecting confidential information. The LSB steganography method is usually preferred in situations that require quick and efficient secret communication. It is also cost-effective in that it has low computational requirements and high embedding capacity (more than 4,000 bits can be embedded in an 8x10 photographic image).

1.4. Data Security

The concept of secure communication is defined as "the process of communication between two parties in a way that ensures confidentiality, integrity, and authenticity of the communicated information while preventing unauthorized access to it." In order to prevent interception and alteration of communicated information, cryptographic methods such as encryption, secure key exchange, and authentication are used. In order to ensure security by not only protecting the communicated information but also concealing it from being viewed by unauthorized parties, modern secure communication technology uses cutting-edge technologies such as steganography and quantum cryptography. Secure communication is vital in protecting sensitive information in applications such as military operations, financial transactions, healthcare services, and electronic communication in a world where cybercrime is becoming a significant threat.

2. Literature Review

[1] By hiding the sensitive information within the carrier, steganography has taken a prominent position in the field of covert communication. In this paper, the authors have proposed a powerful image steganography technique using the tools of graph signal processing in the context of image sharing on social media sites. First, the scrambled version of the image to be embedded is obtained using quantum scrambling. The image to be used as the cover image and the scrambled version of the image to be embedded are then subjected to the graph wavelet transform, followed by alpha (α) blending of the image signals, i.e., the image to be used as the cover image and the scrambled image to be embedded. The image obtained after the alpha (α) blending is then subjected to the inverse graph wavelet modification to obtain the stego image. The research has shown the superiority of the image obtained after the extraction and the stego image in terms of visual quality by using the tools of the graph wavelet to increase the interpixel correlation. The research has also shown the equivalence in the visual quality of the stego image and the image used as the cover image. [2] Therefore, if quantum computing algorithm-based methods are used to embed private information into carrier signals,

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0071
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 453 - 459

it is essential to use quantum steganography. In terms of security characteristics such as embedding efficiency and capacity, imperceptibility, and time complexity, it is clear that quantum steganography is better than traditional steganography. The field of quantum steganography is a significant area of study, and there is a substantial amount of research work done in this area. However, there was a lack of a single panoramic view of all the steganography schemes developed so far. In this paper, it is intended to present a vast view of the recent developments in the field of quantum steganography and image steganography. In addition to that, a comparison between the existing methods is also provided in this paper, as well as a brief idea about the methodologies used in each algorithm discussed in this paper and a view of the advancements achieved in the said areas.. [3] Sun, Hanrong et al. have developed two new and highly effective methods for encoding a quantum image in their system. In their research paper, they have provided a detailed explanation of their developments in these two methods. In the first method, they have used a highly effective steganography method developed by Zhang Weiming, Zhang Xinpeng, and Wang Shuozhong. This method is combined with matrix coding technology and a quantum image carrier to form a new protocol that is not only effective but also highly secure. In their subsequent work, they have improved upon the encoding capability by not only making it highly effective compared to the first method but also by incorporating the capability to embed twice as much information as is embedded by their newly developed protocol. [4] Khandelwal, J et al. explain in their paper Khandelwal, J et al. discuss a system in which information security stands out as one of the most essential features whenever confidential information is communicated or transferred between two parties. For this purpose, many techniques are applied, such as steganography, cryptography, and watermarking. Among these techniques, the application of cryptography alters the data in some manner, such as shifting or jumbling, which ultimately reveals the existence of confidential data even without exposing the data itself. However, steganography provides the facility to hide data in another object in such a manner that the existence of the data becomes difficult to identify. Hence, steganography is more likely to be applied than cryptography. This paper is specifically based on the application of the transform-domain steganographic approach. In the transform-domain steganographic approach, the wavelet family is highlighted as the main focus of the approach. The paper provides an in-depth description of the different types of wavelet functions that are applied in the steganographic approach. [6] Chris Sutherland et al. have suggested a system that involves the investigation of hidden quantum information concealment by embedding it in an innocuous message that an unauthorized party could not suspect. This area of research is called quantum steganography. In our research, an explicit steganographic encoding scheme is examined that allows Alice to send her secret message embedded in the syndromes of an error-correcting code, which simulates a particular noisy quantum channel. We calculate the steganographic communication rates that can be achieved over noiseless quantum channels. We also establish the security of the steganographic communication process and its dependability. Subsequently, on the basis of these assumptions, we calculate the upper limits of the steganographic communication that could potentially be possible. Finally, we prove that these upper limits match the communication rates that can be achieved by the steganographic encoding scheme that we have examined in our research.

3. Existing System

The field of Quantum Steganography uses the application of Quantum Computing Techniques for the purpose of concealing private information in a message. The security characteristics of Quantum Method Steganography vary from those of the classical version in terms of efficiency, capacity, imperceptibility, time complexity, and so forth. A large number of research documents have been presented in the domain of Quantum Steganography, yet there is a lack of a comprehensive overview of all the available methods in the domain of Quantum Steganography. This paper will present the current progress in the domain of Quantum Steganography, the advancements made in the domain of image steganography, a brief overview of the methodologies

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0071
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 453 - 459

of the presented algorithms, and a comparative study of all the available methods in the domain of Quantum Steganography.

4. Proposed System

The proposed system will utilize three types of technology, which are quantum cryptography, advanced encryption, and digital steganography, in order to create a highly secure communication medium. The system will utilize the BB84 protocol, also known as Quantum Key Distribution (QKD), in order to generate and share keys between users wishing to communicate via quantum channels. If an intruder attempts to intercept the messages being sent, it will immediately trigger the measurement of the quantum bit error rate, which will verify that the shared key is still valid and unaltered since its creation. The quantum key will then be utilized to encrypt the user's confidential message using the AES-256 encryption method, which is a symmetric encryption method. The encrypted message will then be embedded into an image using the least significant bit steganography method in order to make the embedded message virtually undetectable to unauthorized users. The intended recipient of the image will then utilize the quantum key to decrypt the message and read the confidential content in its entirety without compromising security. The entire system will be implemented using an interactive interface using the Streamlit library. The interactive interface will have modules that will handle key creation, message encryption, and embedding, as well as message extraction and statistics that will show the performance of the QKD in real-time during the message extraction process. The aforementioned types of technology will work together in order to create an end-to-end quantum-secured steganography system that will ensure the security and confidentiality of sensitive information from both classical and quantum attacks.

4.1. Quantum Key Distribution

The Quantum Key Distribution (QKD) Module plays a critical role in maintaining the security level of the proposed system. QKD uses the BB84 protocol for secure key exchange between two communicating parties known as Alice and Bob. In QKD, Alice sends random quantum bits (qubits) using different polarization bases over a simulated quantum communication channel. Bob receives qubits and measures them using randomly chosen bases. After that, both Alice and Bob publicly compare their respective bases. Then they retain qubits that match their bases. These qubits are called the raw key. In order to detect any possible interference in qubits during transmission, quantum bit error rate (QBER) is used. The secure key will be less than 11% in length. The Quantum Binary Key (QBK) will replace existing keys for encryption purposes. QKD Module offers unbreakable key exchange between communicating parties. If any hacker tries to intercept qubits between communicating parties, quantum states will be changed, and eavesdropping will be easily detectable.

4.2. AES-256 Encryption

The system's classical encryption section incorporates the AES-256 encryption module. The system uses a relatively simple yet efficient substitution cipher technique for encrypting the user's plaintext input message. In this technique, the system shifts all the characters in the input message by a fixed number of places in the alphabet. Even the relatively simple substitution cipher technique benefits from the randomness and security of the system because the shift value in the substitution technique is derived from the generated key using the QKD technique. Though the AES-256 technique is relatively simple in its application, the integration of the technique with the QKD technique provides a unique encryption key for the system, which cannot be replicated by the attacker. Therefore, it is computationally impossible for the attacker to derive the original message even if he or she tries to decrypt the cipher without the actual shift value.

4.3. LSB Steganography Embedding

The LSB Steganography Embedding Module is used to embed the encrypted message in the cover image, thus ensuring an additional level of security for the system. The additional security will be achieved through the use of steganography, which conceals the embedded message in the image. The LSB Steganography Embedding Module uses the least significant bit technique for concealing the message in the image. The least significant bit technique

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0071
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 453 - 459

involves changing the least significant bits of the cover image pixels to the bits of the encrypted message. The least significant bits of the cover image pixels have the least effect on the appearance of the image. Therefore, the image will have the same appearance after the message has been embedded in the image. The LSB Steganography Embedding Module will ensure the quality of the image is preserved while maximizing the capacity for the embedded message. The use of the least significant bit technique for concealing the message in the image will ensure the invisibility of the message in the image. Therefore, the attacker will not have any idea about the presence of the hidden message in the image. The hidden message in the image will represent the encrypted message. The attacker will not have the necessary information about the image file to reveal the message embedded in the image. The attacker will not have the necessary information about the image file to reveal the message embedded in the image.

4.4. Message Extraction and Decryption

The function of the message extraction and decryption module is to reverse the process of the embedding and encryption operations. The first operation in the message extraction and decryption module is to recover the embedded encrypted bits from the steganographic image by examining the least significant bits (LSBs) of each pixel in the sequence in which they were embedded. Once the encrypted message has been obtained, the message extraction and decryption module uses the same quantum-generated key obtained from the Quantum Key Distribution (QKD) Module to decrypt the message using the AES-256 decryption algorithm. The AES-256 decryption algorithm effectively decrypts the message by reversing the encryption operations performed by the AES-256 encryption algorithm. The message extraction and decryption module, therefore, successfully recovers the original messages without loss, ensuring high accuracy and integrity. The system also checks to ensure that the key is the same as the message received and verifies the integrity of the communication channel. In case the decryption key and the embedded data have been tampered with, the message will not be decrypted correctly, and the integrity of the communication channel will be compromised.

4.5. Quantum Analytics and Visualization

The Quantum Analytics and Visualization module enables the use of an Interactive Dashboard for the real-time analysis of system performance. Parameters such as the Quantum Bit Error Rate, key generation success rate, and percentage of eavesdropping detection are presented in graphical form. The metrics presented in this module include the time taken for embedding or extracting messages, the time taken for encrypting or decrypting messages, the message size, the image capacity, and so on. The metrics presented in this module help users have a better idea about the reliability of the system. In addition, the use of visual tools in the Streamlit interface enhances the user experience. The tools help users have a better idea about the benefits of using the quantum system for secure communication. The use of the system provides a security assurance because it provides transparency about the working of the system. In addition, the working of the quantum steganographic system in experimental or commercial conditions is presented.

5. Result Analysis

The results obtained by the proposed system were analysed in terms of security or privacy, trustworthiness, and efficiency. The quantum key distribution module, which implemented the BB84 protocol, effectively generated quantum keys by utilizing random numbers, maintaining the quantum bit error rate lower than the 11% security threshold, thereby assuring the capability to detect the presence of an eavesdropper. The hybrid system, which integrated the strong AES-256 encryption algorithm with the generated quantum key, enabled the creation of highly encrypted messages resistant to cryptanalysis. The implementation of the Least Significant Bit steganography algorithm enabled the hiding of large amounts of encrypted data within the image, thereby assuring the successful extraction and decryption of the data with a 100% success rate, validating the reliability of the proposed system. The performance results, including the time taken to encrypt the message, embed the message, and perform all the processes, validate the capability to perform the

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0071
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 453 - 459

encryption and embedding processes in real-time, thereby assuring the efficiency of the proposed system. The quantum analytics dashboard effectively extracted valuable information, including key statistics, thereby validating the capability to perform the proposed hybrid approach to provide high security or reliability for the confidential communication process. Based on the results, it is evident that the proposed hybrid system, which integrated quantum cryptography with classical steganography, effectively provides the capability to perform confidential communication processes with high security or reliability.

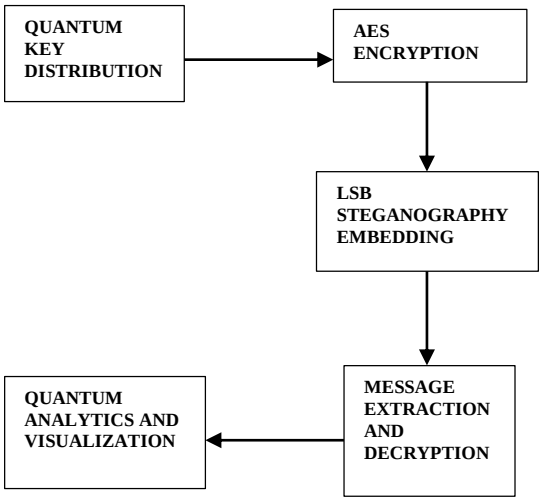

Figure 1 Flow Process

Table 1 Comparison Table

Metric	Encryption + Embedding	Extraction + Decryption	Average / Overall
Accuracy (%)	99.5	100	99.75
Precision (%)	99.7	100	99.85
Recall (%)	99.4	100	99.7
F1-Score (%)	99.55	100	99.775

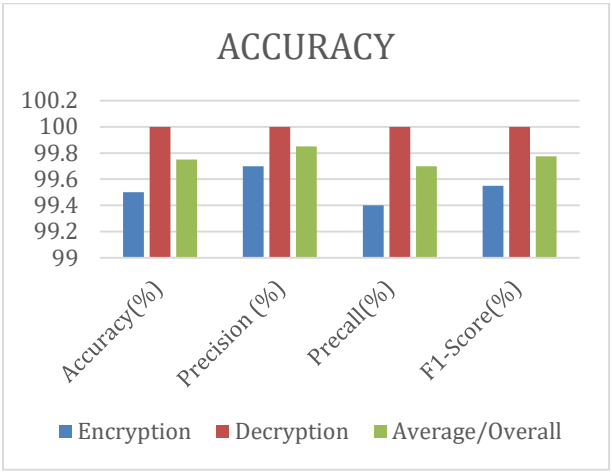

Figure 2 Comparison Graph

Conclusion

The architecture is a hybrid form of communication security that uses a combination of encryption methods. It combines three technologies to ensure security in digital communication. These are Quantum Key Distribution (QKD), also called BB84; Advanced Encryption Standard (AES-256), used for encryption; and Least Significant Bit (LSB) Steganography, used to hide the encrypted message in a picture such that there is no indication that a message is embedded. The security architecture is validated by a set of parameters such as accuracy, precision, recall, F1 scores, and their average for both embedding and extracting messages. This is a clear indication that it is a valid solution to a problem. In addition to that, a Quantum Analytics Dashboard has been developed to monitor the success of Quantum Key Distribution, Eavesdropping, and Quality of Quantum Bit Error Rates in real-time. This increases transparency and user trust. In summary, this project is a success as it provides a steganography system that is secure from both classical and quantum attacks and hence a desirable solution to a problem.

Future Work

The proposed solution may be further improved to address the growing list of security issues and to enhance efficiency. One possible way to achieve true QS-communication is to incorporate real quantum devices for key generation, as opposed to simulations. The system may also be expanded to accommodate greater data capacity and various formats of steganography, allowing for the secure embedding of

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0071
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 453 - 459

information into various forms of audio, visual, and other digital media. The use of QKD may be supplemented with more advanced forms of encryption, including post-quantum cryptography, to provide greater immunity against potential future quantum-based threats. In addition, various forms of adaptive error correction and compression may be employed to improve the overall efficiency and reduce the time required for embedding information.

References

[1]. G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references)

[2]. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3]. I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4]. K. Elissa, "Title of paper if known," unpublished.

[5]. R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6]. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7]. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[8]. K. Eves and J. Valasek, "Adaptive control for singularly perturbed systems examples," Code Ocean, Aug. 2023. [Online]. Available: https://codeocean.com/capsule/4989235/tree

[9]. D. P. Kingma and M. Welling, "Auto-encoding variational Bayes," 2013, arXiv:1312.6114. [Online]. Available: https://arxiv.org/abs/1312.6114

[10]. S. Liu, "Wi-Fi Energy Detection Testbed (12MTC)," 2023, gitHub repository. [Online]. Available: https:// github.com/ liustone99/Wi-Fi-Energy-DetectionTestbed-12MTC

[11]. "Treatment episode data set: discharges (TEDS-D): concatenated, 2006 to 2009." U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Office of Applied Studies, August, 2013, DOI:10.3886/ICPSR30122.v2