

# International Journal on Robotics, Automation and Sciences

## Quantum Steganography Using BB84 Protocol for Secure Data Hiding in Cover Text

Win Pa Pa Phyo\*, Hsu Wai Hnin, and Cho Cho Myint

**Abstract** – Many people use the internet for communication, but there is a problem with protecting their information. To ward off the attackers, they need secure communication such as cryptography and steganography techniques. To maintain the security of information, improving the technology of steganography is necessary. In this paper, we propose a novel method to create the secret quantum text steganography more difficult for attackers to intercept. Firstly, the proposed method generates a secret message as a binary string by combining the secret key of the BB84 protocol and message. Then, the secret message is embedded in the first character of each line in the cover text. In the cover text, the first character of each line is changed to the case of the specific character, such as uppercase or lowercase, according to the secret message to be hidden. The cover text uses the English language. Experimental results describe the effectiveness of the proposed method for hiding data within the cover text while maintaining a high level of security. The proposed model is able to secure data transmission because it was difficult for the attacker to reveal or intercept data.

**Keywords**— *Quantum Steganography, BB84 Protocol, Cover Text, Cryptography, Data Security, Communication Protocol.*

### I. INTRODUCTION

Today, people usually send messages via various internet-based communication applications such as

Email, Viber and other digital platforms. As the use of digital communication increases, protecting confidential information from unauthorized access has become an important issue. Steganography preserves data security over the internet by using different media types (such as images, audio, video, and text) to cover the secret message. In image steganography, the secret message is embedded in an image as noise, which is difficult to find by the attacker. Video steganography hides secret information within video file, while audio steganography embeds secret data into audio file as noise that are unheard to human. The most difficult kind of steganography is text steganography, which embeds secret data into a cover text. Text-based data steganography technology comprises three main types: format-based methods, random and statistical generation method, and linguistic method [1].

Quantum text steganography extends this concept by using quantum computing techniques to enhance the security, efficiency, and invisibility of message embedding within text [2]. Unlike classical text steganography, quantum text steganography conceals secret messages within the cover text by applying quantum principles such as superposition, entanglement, and quantum measurement. The fundamental unit of quantum information is the quantum bit (qubit), which can exist in multiple states simultaneously [3]. Quantum computing relies on

\*Corresponding Author email: dawwinpapaphyo22@gmail.com, ORCID:0009-0009-4018-2500

Win Pa Pa Phyo is with Computer Engineering and Information Technology Department, West Yangon Technological University, Yangon, Myanmar (e-mail: [dawwinpapaphyo22@gmail.com](mailto:dawwinpapaphyo22@gmail.com))

Hsu Wai Hnin is with Computer Engineering and Information Technology Department, West Yangon Technological University, Yangon, Myanmar (e-mail: [hsuwaipyplas01@gmail.com](mailto:hsuwaipyplas01@gmail.com))

Cho Cho Myint is with Computer Engineering and Information Technology Department, West Yangon Technological University, Yangon, Myanmar (e-mail: [itwytu2021@gmail.com](mailto:itwytu2021@gmail.com))

qubits and their ability to be manipulated using quantum gates. Quantum gates are used in quantum cryptography to produce quantum key distribution (QKD) like BB84. Quantum Key Distribution (QKD) techniques can be integrated into quantum text steganography systems, enabling the secure communication exchange between two parties [4].

This paper proposes a quantum-inspired text steganography approach using the BB84 protocol for secure data hiding in cover text. The proposed method generates a secure binary message using BB84-based key generation and embeds the encrypted message into the cover text through the first character in each line. The implementation is performed using a simulated quantum environment to evaluate computational efficiency and embedding performance.

## II. LITERATURE REVIEW

This paper used a quantum-based text steganography technique to hide the information into Indian regional language Bengali handwritten text as a cover text. The system used two-bit streams of the message to embed into the cover text to get high embedding capacity. This system used three algorithms. The first one was a message encryption/decryption algorithm. The second was a message embedding algorithm, and the last one was a message extracting algorithm. Cover text and secret message were used together with mathematical function and quantum approach using handwriting characters in Bengali language with mapping truth table of quantum gate was contributed to get the highest security [5].

The system used quantum channels to apply text steganography. This model used BB84 key protocols to share secret key securely between two users. The cover message and secret message, using only the English language, were converted into binary representation. The converted binary message was encrypted with this key using XOR gate. Finally, the encrypted data was embedded into quantum circuit by using Bernstein Vazirani technique at the sender side. At the receiver side, the operation is performed opposite of the sender side. The proposed method was designed to secure information in communication channels and to prevent attacks from attackers [6].

This research proposed a text hiding method using two levels. The first one is finding letters for secret message and encode the location of this letter. The second one is transforming the letter's location into binary and hiding in cover text in a different way. This proposed method aims to achieve high level of security for text confidentiality [7].

The researcher introduced an innovative steganography protocol based on discrete modulation continuous variable QKD. Modification to the original protocol improved security and vulnerabilities to steganalysis. The paper described Martins quantum steganography (MQS) protocol. The proposed model modified traditional direct communication steganographic protocols by using reverse communication techniques. Discrete-Variable QKD (DV-QKD) used single photons, while Continuous-

Variable Quantum Key Distribution (CV-QKD) encodes information in continuous properties of light, such as amplitude and phase quadrature of coherent states. The system proposed a method to extend a QKD protocol into a steganographic scheme that eliminates vulnerabilities in the MQS protocol by reversing the direction of communication and hiding the quantum states as part of the classical reconciliation process [8].

The paper offered a detailed examination of QKD-based communication protocols and introduced a new system using BB84 algorithm. It represents a significant advancement in securing communication, with the potential to alter our perspective on quantum mechanics. This system provided a solution for secure communication between two parties in the meantime. This research highlights the importance of security protocols and techniques [9].

This study focused on studying of Quantum Key Distribution (QKD), especially detailed explanation of BB84 protocols. The paper described the concept of quantum superposition, quantum entanglement, quantum key distribution and BB84 protocol in detail. The paper proved that BB84 protocols is a strong security QKD scheme and applied in various applications. Additionally, the author examined the practical improvements in BB84 protocols, including the decoy states and advanced error correction methods [10].

This paper proposed the implementation of the BB84 protocol utilizing four distinct bases (phase gates), alongside the SARG04 protocol—an extension of BB84—designed to mitigate photon number splitting (PNS) attacks. The study also incorporates simulations of third-party (eavesdropping) attacks and analyses the impact of quantum noise. All experimental verifications and protocol simulations were conducted using the IBM Quantum Experience platform [11].

This paper introduced the B92 quantum protocol to transmit a secret message shared between two parties. In certain regions of the image are used to represent the least significant qubits of the pixels. The NEQR (novel enhanced quantum representation) and the platform used for testing the described idea is IBM Quantum Experience along with Qiskit [12].

Although previous studies have explored hybrid quantum-classical security frameworks that combine BB84-based key exchange with classical encryption algorithms to improve resistance against attacks. Based on the reviewed studies, most existing approaches focus either on advanced quantum communication protocols or multimedia-based steganography techniques. Therefore, this research proposes a hybrid approach that combines BB84-based key generation with text steganography to provide secure text communication while maintaining implementation simplicity.

## III. PROPOSED MODEL AND ALGORITHM

The proposed system is implemented using Python and Qiskit Aer Simulator in a classical computing environment. The BB84 protocol is simulated using quantum circuit including Pauli-X

gate, Hadamard gate(H), and Phase gate(S). The implementation does not utilize physical quantum hardware. The proposed model evaluates BB84 key generation through quantum simulation [13].

The Hadamard gate is used to transform computational basis states into superposition state during basis generation in BB84 protocol. The. For example, applying the Hadamard gate to  $|0\rangle$  produces the superposition state  $(|0\rangle + |1\rangle)/\sqrt{2}$ . The Hadamard gate is represented in (1).

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (1)$$

The Pauli-X gate performs a bit-flip operation that changes the qubit state from  $|0\rangle$  to  $|1\rangle$  or vice versa. The X gate is shown in (2).

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (2)$$

The Phase gate modifies the phase of the quantum state and is used during basis preparation in the BB84 simulation. The S gate is presented in (3) [14].

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad (3)$$

Alice's key is generated using the random number, and the key changes into a binary string. Alice's key updates using the Pauli-X gate, Hadamard gate (H), and Phase gate (S gate) to produce Alice's basis, as shown in Figure 1.

Bob's basis is created using the Hadamard gate (H) and the Phase gate (S gate) in the quantum circuit according to the length of Alice's key. The quantum circuit displays Bob's basis, as shown in Figure 2.

Bob's key is generated by executing the results of the quantum simulator. The result of the execution is as shown in Figure 3.

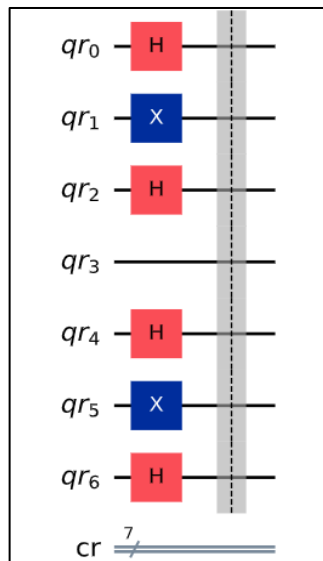


FIGURE 1. Alice's basis in quantum circuit.

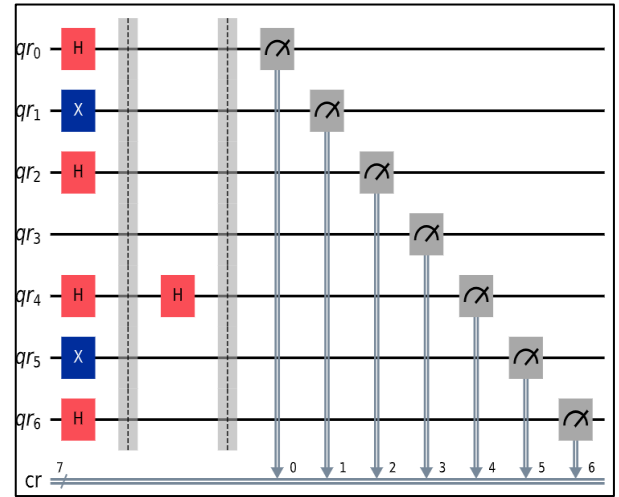


FIGURE 2. Bob's basis in quantum circuit.

```
Bob key : 0100110
Bob Basis ['S', 'S', 'S', 'S', 'H', 'S', 'S']
Alice key : 0100010
Alice Basis : ['H', 'S', 'H', 'S', 'H', 'S', 'H']
```

FIGURE 3. Execution result.

By using the BB84 protocol, Bob's basis and Alice's basis are used to generate the sifted key. If the value of Bob's basis and the value of Alice's basis match, then the value of Alice's key is added to the sifted key. If Bob's basis is 'H' and Alice's basis is 'S', which do not match, then Alice's key cannot be added to the sifted key. If Bob's basis is 'S' and Alice's basis is 'S', which match, then Alice's key is added to the sifted key. The sifted key is generated '1001', which is called the BB84 key in Figure 4.

```
sifted key 1001
Basis [1, 3, 4, 5]
```

FIGURE 4. BB84 key.

The encryption algorithm encrypts the message with a BB84 key to generate the secure message. The embedding algorithm embeds the secure message into the cover text to produce the stego text and the length of the secure message. The stego text is sent to the receiver using a quantum channel. The receiver uses the extraction algorithm to extract the secure message with a binary string. The decryption algorithm decrypts the binary string of the secure message with the BB84 key to generate the message. Figure 5 shows the block diagram of the proposed quantum steganography model.

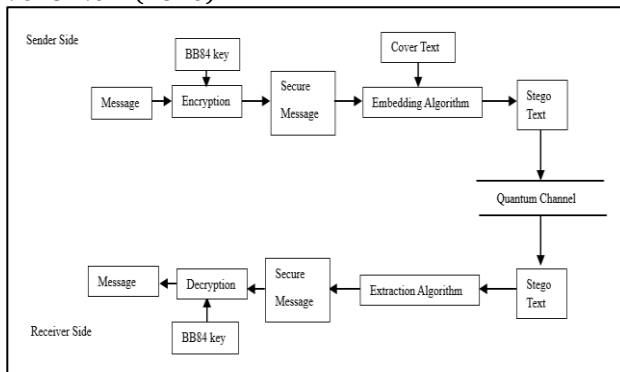


FIGURE 5. Proposed quantum steganography model.

The current implementation does not include quantum noise modelling, error correction, or privacy amplification mechanisms. In addition, the proposed model uses simulated quantum operations rather than real quantum communication channels.

In this model, the sender side uses the encryption algorithm, embedding algorithm, and the receiver side uses the extraction algorithm and decryption algorithm.

#### A. Encryption Algorithm

- Produce the BB84 key by using BB84 protocol.
- Select the message and pick each character in the message.
- Convert into the binary string using ASCII code.
- Uses the XOR function as a key operation. If the input binary digits are equal, then the output is 0. Otherwise, the different input binary digits produce the output 1.
- Encrypt the binary string with the BB84 key using the XOR function to produce the secure binary message.

#### B. Embedding Algorithm

- Select the cover text in English.
- Select the secure binary message (BMS) and execute the length of the message (L).
- If the BMS = "1", then find out the first character of each line in the cover text and convert it to the lower case.
- If the BMS = "0", then convert the first character of each line in the cover text to the upper case.
- Repeat the above step till the secure binary message is finished.
- Generate the stego text, L and the BB84 key to send to the receiver.

#### C. Extraction Algorithm

- Get the stego file, L, and the BB84 key.

- Read the first character (C) of each line in the stego file.
- If C = "uppercase", then bit crypto=0.
- If C = "lowercase", then bit crypto=1.
- If crypto<=L, then write crypto into b.
- Retrieve b as binary string message.

#### D. Decryption Algorithm

- Get b as a binary string message and BB84 key.
- If the length of b = 7, then change b into a number according to the ASCII encoding.
- Decrypt the number and BB84 key using the XOR function to retrieve the character of the original message.
- Repeat the above step till the binary string is finished.
- Retrieve the original message at the receiver's side.

The proposed embedding method uses uppercase and lowercase character transformation, which is simple and may be affected by text formatting changes or steganalysis techniques. However, this approach was chosen to keep the implementation process simple and to demonstrate the integration of BB84-based key generation with lightweight text steganography. The current implementation does not include quantum noise modelling, error correction, or privacy amplification mechanisms. In addition, the proposed model uses simulated quantum operations rather than real quantum communication channels.

## IV. RESULT ANALYSIS

The results of the proposed system of quantum text steganography are discussed in terms of security, capacity, and robustness. The sender's side creates the secret message using BB84 key according to BB84 protocol as shown in Figure 6.

Secret Message:: 10000011101100110010111001011100110

FIGURE 6. Secret Message at the sender's side.

The sender's side embeds the secret message into stego text using encryption and embedding algorithms as shown in Figure 7 and Figure 8.

The stego text and BB84 key are transmitted from the quantum channel. The receiver side retrieves the original message from the stego text using extraction and decryption algorithms, as shown in Figure 9. The result of the proposed system measures the time analysis, capacity consideration, and similarity measure.

Multiple English text messages were used as secret message with lengths ranging from 7 to 53 characters were tested using cover text files of

different sizes. The BB84 key length varied according to the binary representation and message size. The performance evaluation considered BB84 key generation time, stego text generation time, message extraction time, embedding capacity ratio, and similarity between cover text and stego text.

```
You do not do, you do not do
Any more, black shoe
In which I have lived like a foot
For thirty years, poor and white,
Barely daring to breathe or Achoo.
Daddy, I have had to kill you.
You died before I had time—
Marble-heavy, a bag full of God,
Ghastly statue with one gray toe
Big as a Frisco seal
And a head in the freakish Atlantic
Where it pours bean green over blue
In the waters off the beautiful Nauset.
I used to pray to recover you.
Ach, du.
In the German tongue, in the Polish town
Scraped flat by the roller
Of wars, wars, wars.
But the name of the town is common.
My Polack friend
Says there are a dozen or two.
So I never could tell where you
Put your foot, your root,
```

FIGURE 7. Cover text.

```
you do not do, you do not do
Any more, black shoe
In which I have lived like a foot
for thirty years, poor and white,
Barely daring to breathe or Achoo.
daddy, I have had to kill you.
You died before I had time—
marble-heavy, a bag full of God,
ghastly statue with one gray toe
Big as a Frisco seal
And a head in the freakish Atlantic
where it pours bean green over blue
in the waters off the beautiful Nauset.
i used to pray to recover you.
ach, du.
in the German tongue, in the Polish town
Scraped flat by the roller
of wars, wars, wars.
but the name of the town is common.
my Polack friend
Says there are a dozen or two.
so I never could tell where you
put your foot, your root,
```

FIGURE 8. Stego text.

```
Extract to Original message:: Meeting
```

FIGURE 9. Decrypt message.

#### A. Time Analysis

The time analysis of the proposed system consists of time for the BB84 key, embedding time, and extraction time [15]. The time of the proposed system depends on the BB84 key, original message, and cover text size. The time for the BB84 key takes to create the key using BB84 protocol in quantum circuit. The time is 0.557 seconds in the quantum circuit. The

embedding time takes to hide the secret message in the cover text using the embedding algorithm in quantum steganography. The time is 0.1258 seconds. The extraction time takes to retrieve the hidden message from the stego text, which is 0.001 seconds. So, the effectiveness of the proposed system is fast and more efficient. The computation time of stego and message generation is as shown in Table 1 and Figure 10.

TABLE 1. The computation time of stego and message generation.

| Message Length | Computation Time (in seconds) |                |                  |
|----------------|-------------------------------|----------------|------------------|
|                | BB84 key Generate             | Stego Generate | Message Generate |
| 7              | 0.884                         | 0.0169         | 0.001            |
| 9              | 0.718                         | 0.0164         | 0.001            |
| 10             | 0.689                         | 0.0137         | 0.001            |
| 12             | 0.759                         | 0.0156p        | 0.001            |
| 20             | 0.661                         | 0.0186         | 0.001            |
| 30             | 0.422                         | 0.0131         | 0.001            |
| 43             | 0.479                         | 0.0264         | 0.001            |
| 53             | 0.514                         | 0.021          | 0.001            |

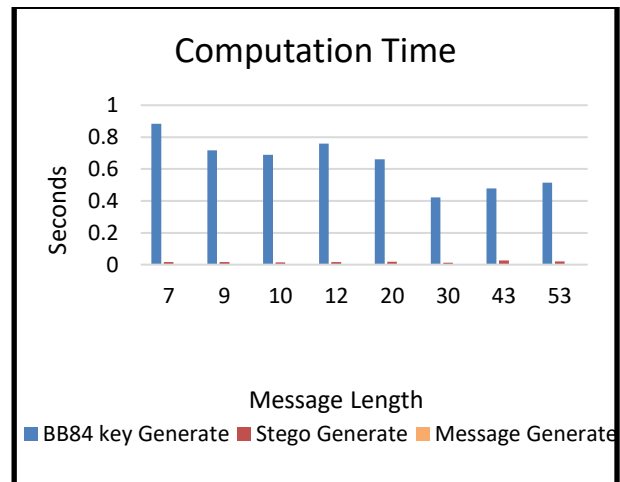


FIGURE 10. Computation time of BB84 key, stego and message generation.

If the message length is 7 and the BB84 key generation time is 0.884 seconds, then the stego generation time is 0.0164 seconds and the message generation time is 0.001 seconds in Table I. If the message length is 53 and the BB84 key generation time is 0.543, the stego generation time is 0.021 seconds and the message generation time is 0.001 seconds. If the message length is large, the stego generation time is slightly more than 0.0169 seconds. So, the proposed system is efficient.

#### B. Capacity Consideration

The capacity is the amount of secret message (bits or bytes) hidden in the cover text [16]. The performance of the proposed system indicates the ratio of the secret message (bits) to the size of the cover text. The capacity ratio is represented in (4).

$$\text{Capacity ratio} = \frac{\text{Amount of hidden message in bits}}{\text{Size of hte cover tex in bits}} \quad (4)$$

The proposed system can hide two bits of a secret message using one character. The capacity of the proposed system depends on the size of the secret message hidden in the cover text. If the size of the secret message is 91 bits, and the size of the cover text is 88359 bits, then the capacity is 0.001, and the embedding capacity is low. If the size of the secret message is 357 bits, and the size of the cover text is 88359 bits, then the capacity is 0.004. If the size of the secret message is large, then the percentage capacity of the proposed system is great, and the embedding capacity is high, as shown in Table 2.

TABLE 2. Capacity ratio of secret message and cover text.

| Amount of Secret message in bits | Size of Cover text in bits | Capacity Ratio |
|----------------------------------|----------------------------|----------------|
| 91                               | 88359                      | 0.001          |
| 231                              | 88359                      | 0.0026         |
| 350                              | 88359                      | 0.0039         |
| 357                              | 88359                      | 0.004          |

### C. Similarity Measure

The similarity measure of the proposed system uses Jaro Jaro-Winkler Similarity metric between the cover text and stego text. The Jaro-Winkler metric is a measure of the similarity between two strings of the cover text and stego text [17]. The lower the Jaro-Winkler distance for two strings, is less similarity between the two strings [18]. The Jaro-Winkler similarity is calculated given two strings  $S_1$  and  $S_2$  their distance  $D$  as

$$D = \frac{1}{3} \left[ \frac{m}{|S_1|} + \frac{m}{|S_2|} + \frac{m-t}{m} \right] \quad (5)$$

where  $m$  is the number of matching characters and  $t$  is the number of transpositions, and  $|S_1|$  is the length of string  $S_1$  and  $|S_2|$  is the length of string  $S_2$  [19]. In the proposed embedding approach, the Jaro score of comparing cover text and stego text is 0.9 because they are closely similar.

Histogram of cover text is shown in Figure 11 and stego text is shown in Figure 12. Histogram is used to measure the effectiveness of the embedding algorithm in the proposed system. The histogram of the cover text and the stego text are closely the same and show high similarity because the proposed embedding method is efficient and secure.

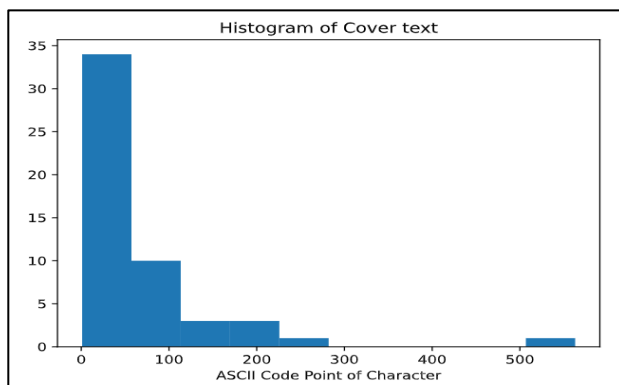


FIGURE 11. Histogram of cover text.

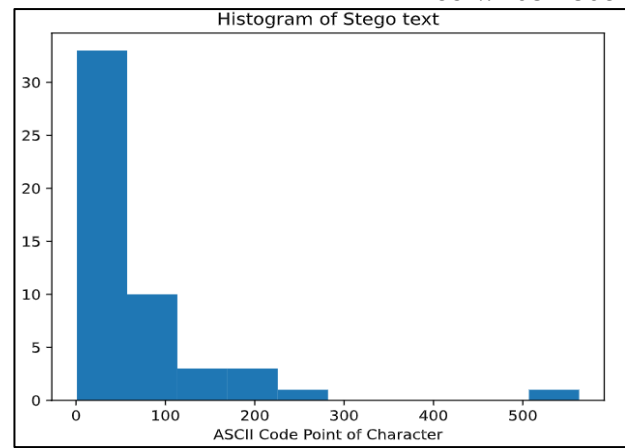


FIGURE 12. Histogram of stego text.

### V. CONCLUSION

This paper explored the combination of Quantum text steganography using English language and BB84 protocols to secure data hiding in cover text. The secret message is converted into a binary string using ASCII code and combined with the BB84 secret key. The secure binary message is embedded in the first character of the cover text to change to uppercase or lowercase. The cover text does not change its original format or character. The generated stego text is transmitted to the receiver using the quantum channel. The receiver retrieves the stego text in the original message using the extraction and decryption algorithm. The test result demonstrate that the proposed system maintains the high similarity between cover text and stego text while resulting low computational time for embedding and extraction processes. So, the proposed system ensures the secure messages remain imperceptible to steganalysis.

### ACKNOWLEDGEMENT

The authors would like to thank the Computer Engineering and Information Technology Department, West Yangon Technological University, Myanmar for always supporting and encouraging individuals who aspire to be validated in their fields. We want to thank peer reviewers for helping to review the paper. The authors wish to acknowledge the anonymous reviewers who made some very important comments and suggestions to help improve the quality and readability of this paper.

### FUNDING STATEMENT

There are no funding agencies supporting the research work.

### AUTHOR CONTRIBUTION

Win Pa Pa Phy: Data Curation, Writing –Original Draft Preparation;

Hsu Wai Hnin: Supervision, Writing – Review & Editing;

Cho Cho Myint: Administration, Review & Editing.



## CONFLICT OF INTERESTS

No conflict of interests was disclosed.

## ETHICS STATEMENTS

Ethical approval was not applicable to this research since it did not involve human participants, animals, or sensitive data.

## DECLARATION OF AI-ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

No artificial intelligence tools were used in the research or writing of this article.

## REFERENCES

- [1] M. Htet and S. W. Phyto, "A Novel Text Steganographic Technique Using Specific Alphabets", *Journal of Computer Science*, vol.2, no.1, pp.1-11, 2020.  
DOI: <https://doi.org/10.31357/jcs.v2i1.2721>
- [2] P. Y. Surya, H. Senapathi, T.K. Sigatapu. M. Shaik and D. Sasapu, "Novel Text Steganography Approach Using Quantum Key Distribution: Survey Paper", *An Interdisciplinary Journal of Neuroscience and Quantum Physics*, vol. 20, no. 30, pp. 923-929, 2022.  
DOI: <https://doi.org/10.14704/nq.2022.20.13.NQ88118>
- [3] A. Kumar and S. Garhwal, "State-of-the-Art Survey of Quantum Cryptography", *Archives of Computational Methods in Engineering*, vol. 28, pp. 3831-3868, 2021.  
DOI: <https://doi.org/10.1007/s11831-021-09561-2>
- [4] S. K. Sahu and K. Mazumdar, "State-of-the-art analysis of quantum cryptography: applications and future prospects", *Frontiers in Physics*, vol. 12, no. 1456491, 2024.  
DOI: <https://doi.org/10.3389/fphy.2024.1456491>
- [5] I. Banerjee, K. Bandyopadhyay, A. Mohan, and A. Kumar, "Quantum Text Steganography Using Numeric Handwriting of Indian Regional Language," *International Journal of Engineering Trends and Technology*, vol. 68, no. 7, pp. 42–49, 2020.  
DOI: <https://doi.org/10.14445/22315381/ijett-v68-i7p207s>
- [6] D.Lavanya, G. Uma Sai Naresh, B. Bhaskar Sai and K. Purna Chandra Rao," Quantum Text Steganography by Using BB84 Protocol", *Journal of Engineering Sciences*, vol.14, no. 03, pp. 603-611, 2023.  
URL: <https://jespublication.com/upload/2023-V14I3069.pdf>
- [7] Alaa Abdullah Idress and Y. H. Ismael, "Proposed Method for Text Steganography", *Journal of Modern Computing and Engineering Research*, vol. 2024, pp. 1-8, 2024.  
URL: <https://jmcer.org/wp-content/uploads/2024/02/PROPOSED-METHOD-FOR-TEXT-STEGANOGRAPHY-2.pdf>
- [8] R. Joshi, A. Gupta, K. Thapliyal, R. Srikanth, and A. Pathak, "Hide and seek with quantum resources: new and modified protocols for quantum steganography," *Quantum Information Processing*, vol. 21, no. 5, 2022.  
DOI: <https://doi.org/10.1007/s11128-022-03514-9>
- [9] S. P. Yalla, A.Uriti, A. Sethy and S. V. E., "Secure method of communication using Quantum Key Distribution", *Applied and computational engineering*, vol. 30, no. 1, pp. 32–37, 2024.  
DOI: <https://doi.org/10.54254/27552721/30/20230065>
- [10] M. SujayKumar Reddy, M. Sayan and B. Chandra Mohan, "Comprehensive Study of BB84, A Quantum Key Distribution Protocol", *International Research Journal of Engineering and Technology (IRJET)*, vol.10, no.3, 2023.  
URL: <https://www.irjet.net/archives/V10/I3/IRJET-V10I3161.pdf>
- [11] S. Ghosh, H. Mishra, B. K. Behera, and P. K. Panigrahi, "Experimental realization of BB84 protocol with different phase gates and SARG04 protocol", *arXiv preprint arXiv:2110.00308*, 2021.  
DOI: <https://doi.org/10.48550/arXiv.2110.00308>
- [12] A-G. Tudorache, V. Manta, and S. Caraiman, "Quantum Steganography Based on the B92 Quantum Protocol", *Mathematics*, vol. 10, no. 16, pp. 2870, 2022.  
DOI: <https://doi.org/10.3390/math10162870>
- [13] M. Czernmann, P. Trócsányi, Z. Kis, B. Kovács, and L. Bacsárdi, "Demonstrating BB84 Quantum Key Distribution in the Physical Layer of an Optical Fiber Based System", *Infocommunications Journal*, vol. 13, no. 3, pp. 45-55, 2021.  
DOI: <https://doi.org/10.36244/ICJ.2021.3.5>
- [14] H. Kaur and R. Singh, "A Review on Quantum Key Distribution and BB84 Protocol", *International Journal of Information Technology*, vol. 15, no. 2, pp. 985-994, 2023.  
DOI: <https://doi.org/10.1007/s41870-022-01082-5>
- [15] M. Usman, S. Latif, and T. Mahmood, "Text Steganography Techniques: A Survey and Performance Analysis", *Multimedia Tools and Applications*, vol. 81, pp. 12415-12445, 2022.  
DOI: <https://doi.org/10.1007/s11042-021-11762-5>
- [16] Chunduru Anilkumar, Swathi Lenka, N. Neelima, S. V E, "A Secure Method of Communication through BB84 Protocol in Quantum Key Distribution", *Scalable Computing Practice and Experience*, vol.25, no.1, pp.25-33, 2024.  
DOI: <https://doi.org/10.12694/scpe.v25i1.2152>
- [17] G.Vaishnavi and K.Mayura, "Quantum Cryptography for a Secure Communication", *International Journal of Research in Computer Applications and Information Technology (IJRCAIT)*, vol.7, no.1, pp.17-29, 2024.  
URL: [https://ijrcat.com/index.php/home/article/view/IJRCAIT\\_07\\_01\\_003](https://ijrcat.com/index.php/home/article/view/IJRCAIT_07_01_003)
- [18] G. Chris, A. G. Mercy, "The Role of Quantum Cryptography in Enhancing Cybersecurity", *International Journal of Research Publication and Reviews*, vol.5, no.11, pp. 889-907, 2024.  
DOI: <https://doi.org/10.55248/gengpi.5.1124.3135>
- [19] J. Ahn, H. Kwon, B. Ahn, K. Park, T. Kim, M. Lee, J. Kim and J. Chung, "Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD)," *Energies*, vol. 15, no. 3, pp. 714, 2022.  
DOI: <https://doi.org/10.3390/en15030714>