Novel Text Steganography Approach Using Quantum Key Distribution: Survey Paper

Surya Prakash Yalla[1], Senapathi Hemanth[2], Sigatapu Tharun Kumar[3], Shaik Moulali[4], Sasapu Dileep[5]
Department of Information Technology[1,2,3,4,5]
GMR Institute of Technology[1,2,3,4,5]

Abstract

As technology advances, maintaining the security of the information in the communication channel from the intruders has become a greater challenge. To overcome this challenge steganography has been introduced which makes the shared data unavailable to the intruders. The process of steganography involves encoding a secret message in a suitable carrier message, such as text, a picture, audio, a video, a file, etc. Quantum steganography embeds the steganographic data into quantum circuit and transmit through the quantum channel. In this paper, a secured communication model is proposed through text steganography using quantum channels. The Global English language has been used to construct a text steganography procedure in this article. Text steganography is a process of hiding the secret message with the covered message or data and transmitting over a channel. This process involves Bernstein Vazirani algorithm and BB84 protocol. The data is integrated into a quantum circuit using the Bernstein Vazirani technique. BB84 protocol is used to obtain a secret key. An attacker or a hacker can't find out the actual quantum message without getting the access of the protocol. Finally, this paper provides a secure communication between the users using the quantum channels.

Key Words: BB84 Protocol, Bernstein vazirani Algorithm, Quantum Channel, Quantum Steganography.

DOI Number: 10.14704/nq.2022.20.13.NQ88118 **Neuro Quantology 2022; 20(13):923-929**

Introduction

The art of hidden communication over a traditional route is called steganography. Steganography, sometimes known as "covered writing," has Greek roots. Steganography is a method for preserving the presence of hidden communications in other media (picture, video, and audio communication). In the current context, multimedia items like audio, video, photographs, etc. are utilized as a cover medium by steganography systems since people routinely exchange digital images through various internet communication applications or transfer them over e-mail. Steganography is a technique that typically refers to hiding the same secret message within a cover object without altering the secret message's structure. Steganography uses two different kinds of materials: message and carrier. Carrier is the substance that contains the message, while message is the confidential information that has to be concealed.

Quantum steganography corresponds to quantum channel, was developed to enable secret quantum or classical messages. Two types of quantum steganography can be distinguished. One such method is known as QMS (Quantum Multisecret Sharing), which may be expanded to conceal the bits in multipartite quantum states for exchanging secret communications. Using local operations and conventional communication, some parties can retrieve the bits that are hidden using this kind of quantum steganography. The second technique is called QDH (Quantum Data Hiding), and it entails building a secure channel inside of a standard quantum channel in order to transmit private messages. When compared to QMS, QDH is more analogous to traditional steganography and has a greater capacity for transmitting covert messages. There are four categories for steganography.

Image Steganography: Image steganography is the use of images as popular cover objects for

steganography.

Video steganography: A technique for hiding information in video files, which are often collections of sound and images, is known as video steganography.

Audio Steganography: Audio steganography is the use of an audio signal carrier to cover up information.

Text steganography: Information may be concealed by using text steganography techniques as white spaces, capital letters, tabs, and Morse code .

Literature Survey

The novel quantum steganography technique has been proposed in this article, is based on quantum secure direct communication. In this study an unique quantum steganography has been proposed that builds on QDH and has a huge payload to increase the capacity of concealed channels. To convey secret messages, the novel protocol incorporates entanglements switching of Bell states with superdense coding. The proposed protocol specifies the capacity of the hidden channel has been raised four times when compared to earlier quantum steganographies, and the superposition channel can transfer more data than the original quantum channel. Regarding security, IBF's exceptional security demonstrates this protocol can dependably withstand intercept-resend assault and auxiliary particle attack. Since information and secret messages are distributed at random, the hidden channel inside IBF is very imperceptible and challenging to find. Finally This paper states that the detection of hidden message can be decreased by making more number of bell states.[1]

In this work, a highly secure steganography method termed cryptography incorporated steganography is proposed for data in various file formats (CICS). The dual "Rivet, Shamir, and Adelman" encryption algorithms are used in the suggested technique to encrypt the original photos. In order to protect the data and maintain its integrity, the encrypted images are then covered with cover images or stego images. This algorithm helps in less memory consumption and quick decryption. Steganography based on DCT/DWT is used to cover the encrypted data after encryption, and RSA-CRT is used to extract the data and decrypt it on the receiving end to retrieve the original picture with increased capacity, security, and robustness. The suggested approach is implemented in MATLAB and measured the peak signal-to-noise ratio to analyse its performance.[2]

A method for hiding communications in other media is steganography. Steganography is a technique that typically refers to hiding the same secret message within a cover object without altering the secret message's structure. One term for steganography is "invisible" communication. Without understanding the correct steganography approach, recovering information is highly challenging due to invisibility or invisible factors. A discrete wavelet transform based steganographic approach has been proposed, Without causing any significant modifications to the cover pictures. The proposed technique compresses the image after the information has been hidden to save memory. It works in low frequency region. Discrete Wavelet Transform (DWT) is the method used for compression, and Inverse DWT (IDWT) is used to restore the original picture. Discrete Wavelet Transform For steganography, which converts images into frequency domain by splitting them into four separate frequency sub-bands. According to this research, the suggested technique provides excellent security and good durability.[3]

This paper examines the statistical characteristics of the stroke number parity of Chinese characters and comes to the conclusion that each character has this trait, which has a uniform distribution. In order to increase the embedding rate, this paper extends an existing coverless plain text steganography based on the stroke number parity of Chinese characters. With the use of texts pulled from the Internet, this approach creates a binary search tree that is then used to search the related texts using a secret binary digit string. The study's main objective is to find a character feature that can be used universally to represent a binary digit, such "0" or "1," and to develop a function that maps character characteristics to a Binary Digit String(BDS). The next step is to locate suitable texts for steganography using the mapping feature of the Internet.[4]

In our daily lives, maintaining the confidentiality of the secret information has proven to be very difficult. In this study, a text steganography technique has been developed using Gujarati, a regional language of India. Here, the quantum technique is also used to raise the bar for security. To increase the level of security, a Revised SSCE code has been used in this study. The updated SSCE code, a quantum strategy based on the use of two distinctive and rare Gujarati characters, and a mapping method of the quantum gate truth table have all been integrated with text steganography. The capacity to prohibit or hide particular characteristics from being available to others—aside from the genuine user—is known as information concealment. There are numerous sub disciplines. Steganography, which derives from Johannes Trithemus' (1462-1516) book "Steganographia" and means "covered writing" in Greek, is one of the most significant subfields of study.[5]

The best implementation of quantum cryptography uses Quantum Key Distribution (QKD) networks, which combine traditional cryptographic methods with quantum mechanics to guarantee complete security. This article discusses many ways to attack the BB84 quantum key distribution protocol as well as an analysis of these attacks. Data or streams can be sent from one side to another using cryptography. Here, the data is first encrypted by the sending party using a key and then the same encrypted data is subsequently decrypted by the receiving party using the same or a different key in accordance with a protocol agreed upon by both parties. The heart and soul of this entire process is now this key. Quantum cryptography is a technique that combines the principles of classical and quantum mechanics. In this case, quanta or photons are used to create a key for secure communication. Quantum cryptography is based on Heisenberg's Uncertainty Principle, which holds that one cannot accurately measure a photon's spin or polarisation without making mistakes or deviating from the way photons normally transmit information. For this reason, the idea as a whole offers "unconditional security".[6]

The need for privacy is growing, and securing transmission channels is now essential. Steganography, a technique for hiding private data in digital content so that only the intended receiver is aware of it, has grown in importance as a field of study. This white paper presents two steganographic techniques based on similarities between English script styles (SEFS). The font style of the main document is changed to a similar one to contain the secret message after encryption. Career document capitalization, punctuation, spaces, and the first and last letters of words of three or more letters are used. Applying these methods to different document formats and fonts allows for testing. As a result, the adversary's secret message was ambiguous, and the size of the Stego-document grew, greatly increasing its capacity. I got the same result when I applied the approach to C# to create a tool that hides important information in text documents.[7]

With the fast development of natural language processing capabilities in recent years, text synthesis-based steganography has made considerable strides. Previous steganalysis techniques don't perform well enough to discover these steganography techniques, which is an ongoing issue that puts the security of cyberspace at serious risk. Experimental results show this model's ability to simultaneously achieve high detection performance and detection efficiency, which demonstrates state-of-the-art performance. Given that language is a heavily encoded sort of information, there are strong semantic coherences and correlations between words in the text, as shown in. Once the additional information has been incorporated into the text, it is possible to change the semantic relationships between these terms. Because of the great degree of coding, high level semantic interpretation of texts has always been challenging. Various studies and applications over the last few years have shown the neural network's potent capacity to extract and express characteristics without the need for manually created features by carrying out self-learning through a large amount of data.[8]

In general, quantum computing is using the principles of quantum physics to process data. The field of quantum cryptography known as quantum key distribution (QKD) provides a way for two parties to exchange a safe key. Many quantum researchers and cryptographers have identified flaws in the initial Quantum Key Distribution protocol since it was first introduced

in 1984 that might compromise the protocol's absolute security. These include an eavesdropper-launched Photon Number Splitting (PNS) attack, a high Qubit Error Rate, and a low Raw Key Efficiency. An eavesdropper could execute a photon number splitting attack against the BB84 protocol. In the BB84 protocol, Alice (the sender) is presumptively equipped with an ideal single-photon source that can generate polarised photons for transmission. The Quantum Bit Error Rate (QBER), which is determined by dividing the error rate by the key rate, can be used to determine whether or not an eavesdropper is present and how much data was gathered. Due to the BB84 protocol's high QBER, network communication involving secret key sharing may expose enough information to an observer. The raw key efficiency is calculated as the ratio of the shared raw/sifted key length to the sender's original random bit length between two communicating entities. [9]

The most flexible single-byte coding system now available is called American Standard Code for Information Interchange (ASCII), which is based on the Latin alphabet. It has been determined through research of the quantum text representation model put forth in the literature that one text message character is stored using a seven-qubit sequence. An enhanced ASCII-based quantum representation of text is presented in this proposed approach. Peak-signal-to-noise ratio (PSNR) comparisons are frequently used in quantum image steganography schemes to assess the authenticity of the stego image and the cover image. The new gray-scale picture steganography system proposed in this research leverages the NEQR representation to represent a 2^n * 2^n cover image and presents an enhanced quantum text representation to store secret text with 2^(n-1+n-2) symbol data. It is important to note that the extraction, reorganisation, and inverse scrambling of eight bit-planes which is required to acquire secret text is a completely blind procedure. Also included are simulation findings about the proposed scheme's robustness and visibility quality. The last analysis is of circuit complexity.[10]

Finding a bit string is the goal of the Bernstein-Vazirani algorithm. Beyond qubit systems, the Bernstein-Vazirani algorithm is presented in a variety of novel configurations in this article. Three discussions were conducted for this article. First, a discussion of the Bernstein-Vazirani bit string determination algorithm .In order to discover a bit string, the method has the capability of a quantum state's Hadamard transform in a two-dimensional space. The extended Bernstein-Vazirani approach for finding a natural number string is the subject of second discussion. The generalised approach in second discussion has the ability to find a string of natural numbers by using the standard Fourier transform of a quantum state in a finite-dimensional environment. The generalised Bernstein-Vazirani approach for finding an integer string is covered in third section.[11]

Typically, optical fibre networks transport enormous amounts of data and are widely employed in the backbone terrestrial and access networks across the world. The integration of QKD with currently operating conventional optical networks has been proposed as an alternative to using these fibres for quantum communication. In this study, the QKD process is based on (BB84) protocol. BB84 protocol was developed in the year 1984. This protocol employs four polarisation states of photons and operates according to the Prepare and measure (P&M) scheme and Heisenberg's uncertainty principle. The main idea of this BB84 protocol is to generate a secret key between the sender and receiver in which the secret is used in both encrypting and decrypting the data. This is used in developing a secured secret key and transferred to both the users through the communication channel.[12]

In this publication, a summary of text steganography's various methods and categorization is provided. Steganographic methods utilise characteristics of the used cover media or redundant information that the human perceptual system is unable to distinguish in order to conceal the secret.Character-level, bit-level, and mixed-type embedding are the three basic categories into which text steganography may be categorised.The secret message directly embedded as characters within the text content using the character-level embedding approach.The secret message is first converted into bits using the bit level embedding technique, either by encrypting it or using a binary representation of the ASCII value or any other

representation, and then it is embedded.Mixed-type embedding The secret message is initially transformed into its corresponding binary bits during embedding. Then, using some attribute, it translates these bits to English alphabets. The mapped alphabet is finally embedded into the cover work in a manner akin to character-level embedding.[13]

In this study, we will discuss several steganographic techniques while taking into account the cover data. This study discusses the many steganographic techniques used in text, picture, and audio steganography. To avoid their comprehension, messages are encrypted using cryptography. The message will be hidden on the opposite side through steganography, making sure that no one knows where it came from. When steganography fails and a message can be recognised, in certain circumstances it is still useless since it has been encrypted using cryptographic methods. Text steganography can be achieved by altering the formatting or the attributes of specific textual elements. In audio steganography, a secret message is added to the digitised audio signal, subtly altering the accompanying audio file's binary sequence. Image steganography pictures that conceal information.[14]

With the use of "multimedia" files, this document has attempted to explain the many methods for implementing steganography. A relatively new area of data processing called steganalysis aims to recognise steganographic covers and, if feasible, extract messages from them. In cryptography, it is comparable to cryptanalysis.In addition to preventing the information from being read, the goal is to conceal it. A secret message is impossible to differentiate from white noise using these new methods. No evidence exists for the message's existence, even if it is suspected . Steganography is a tool that terrorists might employ to plan their assaults and keep their conversations private.[15]

COMPARISION TABLE :

	Author	Approach	Advantages
Paper 1	Qu, Z. G., Chen, X. B., Zhou, X. J., Niu, X. X., & Yang, Y. X.	Unique quantum steganography based on QDH.	Increases the capacity of concealed channels.
Paper 2	Vinothkanna, M. R.	Cryptography incorporated steganography Approach	Less memory consumption and quick decryption.
Paper 3	Gupta, S., & Jain, R.	Discrete wavelet transform based steganographic approach	Works in low frequency region
Paper 4	Wang, K., & Gao, Q.	coverless plain text steganography based on PCCSN	They can be used in quick messages.
Paper 5	Banerjee, I., Bhattacharyya, S., & Sanyal, G.	Revised SSCE code Approach	This technique keeps the stego and cover lengths constant.
Paper 6	Aggarwal, R., Sharma, H., & Gupta, D	BB84 quantum key distribution protocol	Create a key for secure communication
Paper 7	El Rahman, S. A.	steganographic technique based on English script styles	Increase of size of the Stego-document.
Paper 8	Yang, Z., Huang, Y., & Zhang, Y. J.	Issues of Text Steganalysis	

Paper 9	Hong, K. W., Foong, O. M., & Low, T. J.	Quantum Cryptography	It enables the accomplishment of several cryptographic tasks that are thought to be impractical using merely conventional communication.
Paper 10	Luo, J., Zhou, R. G., Liu, X., Hu, W., & Liu, G.	Quantum steganography based on ASCII	Better visibility quality
Paper 11	Nagata, K., Farouk, A., & Nakamura, T	Bernstein-Vazirani algorithm on qubit system.	The Bernstein-Vazirani algorithm recognises a secret binary string in a quick pass.
Paper 12	Sharma, P., Agrawal, A., Bhatia, V., Prakash, S., & Mishra, A. K	BB84 protocol	Detects the presence of eavesdropper.
Paper 13	Krishnan, R. B., Thandra, P. K., & Baba, M. S.	Text steganography Approach	Steganography has the benefit of typically allowing messages to be sent covertly without the transmission being detected.
Paper 14	Hariri, M., Karimi, R., & Nosrati, M.	Comparsion of Steganographic mehod	
Paper 15	Doshi, R., Jain, P., & Gupta, L.	Steganalysis	Cracks the hidden data

Conclusion

Digital steganography is the skill of covertly concealing a hidden message inside of a cover medium, and it was inspired by the old secret communication techniques. This study proposes a method for text steganography utilising the English language and the quantum truth table mapping methodology. Since text documents offer the least amount of redundant information, choosing them as a cover medium is therefore the most challenging. In normal steganography techniques, public channels are used to communicate which may prone to loss of security. So to overcome the problem a novel steganography technique is proposed which utilizes the quantum channel for communication purpose. According to comparisons made across several study articles, it was shown that Character and String Mapping is the most effective since it uses the fewest cover characters to encrypt a hidden character in text steganography. So the character and string mapping is used in this technique. The result of the suggested method demonstrate that stego production on the receiver side is quicker than on the sender side. Results have proved that the input message and output message are same. This study offers a detailed analysis of steganographic research articles. The models, and comparsion of each work are detailed. The scope of this study can be increased by incorporating additional regional Indian languages.

Acknowledgement

The authors acknowledge the Institution for encouraging the research.

Conflict of Interest

None.

Funding Source

None.

References

Qu, Z. G., Chen, X. B., Zhou, X. J., Niu, X. X., & Yang, Y. X. (2010).Novel quantum steganography with large payload. Optics Communications, 283(23), 4782-4786.

Vinothkanna, M. R. (2019). A secure steganography creation algorithm for multiple file formats. Journal of Innovative Image Processing (JIIP), 1(01), 20-30.

Gupta, S., & Jain, R. (2015, December). An

innovative method of Text Steganography. In 2015 Third International Conference on Image Information Processing (ICIIP) (pp. 60-64). IEEE.

Wang, K., & Gao, Q. (2019). A coverless plain text steganography based on character features. IEEE Access, 7, 95665-95676.

Banerjee, I., Bhattacharyya, S., & Sanyal, G. (2012). Text Steganography Using Quantum Approach in Regional Language with Revised SSCE. International Journal of Computer Network & Information Security, 4(12).

Aggarwal, R., Sharma, H., & Gupta, D. (2011). Analysis of various attacks over BB84 quantum key distribution protocol. International Journal of Computer Applications, 20(8), 28-31.

El Rahman, S. A. (2019). Text steganography approaches using similarity of English font styles. International Journal of Software Innovation (IJSI), 7(3), 29-50.

Yang, Z., Huang, Y., & Zhang, Y. J. (2019). A fast and efficient text steganalysis method. IEEE Signal Processing Letters, 26(4), 627-631.

Hong, K. W., Foong, O. M., & Low, T. J. (2016, December). Challenges in quantum key distribution: a review. In Proceedings of the 4th International Conference on Information and Network Security (pp. 29-33).

Luo, J., Zhou, R. G., Liu, X., Hu, W., & Liu, G. (2019). A novel quantum steganography scheme based on ASCII. International Journal of Quantum Information, 17(04), 1950033

Nagata, K., Farouk, A., & Nakamura, T. (2022). Various new forms of the Bernstein–Vazirani algorithm beyond qubit systems. In Simplified Quantum Computing with Applications. IOP Publishing.

Sharma, P., Agrawal, A., Bhatia, V., Prakash, S., & Mishra, A. K. (2021). Quantum key distribution secured optical networks: a survey. IEEE Open Journal of the Communications Society.

Krishnan, R. B., Thandra, P. K., & Baba, M. S. (2017, March). An overview of text steganography. In 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN) (pp. 1-6). IEEE.

Hariri, M., Karimi, R., & Nosrati, M. (2011). An introduction to steganography methods. World Applied Programming, 1(3), 191-195.

Doshi, R., Jain, P., & Gupta, L. (2012). Steganography and its Applications in Security. International Journal of Modern Engineering Research (IJMER), 2(6), 4634-4638.

Wahab, O. F. A., Khalaf, A. A., Hussein, A. I., & Hamed, H. F. (2021). Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. IEEE Access, 9, 31805-31815.

Lee, C., Sohn, I., & Lee, W. (2022). Eavesdropping Detection in BB84 Quantum Key Distribution Protocols. IEEE Transactions on Network and Service Management.

Niemiec, M., & Pach, A. R. (2013). Management of security in quantum cryptography. IEEE Communications Magazine, 51(8), 36-41.

Inoue, K. (2006). Quantum key distribution technologies. IEEE journal of selected topics in quantum electronics, 12(4), 888-896.

Cao, Y., Zhou, Z., Chakraborty, C., Wang, M., Wu, Q. J., Sun, X., & Yu, K. (2022). Generative Steganography Based on Long Readable Text Generation. IEEE Transactions on Computational Social System.