Prerequisites for the Establishment of a Quantum Steganography Communication

Veselka Stoyanova
Artillery, AD and CIS faculty
National Military University Vasil Levski
Shumen, Bulgaria
veselka_tr@abv.bg

***Abstract*— Several approaches and techniques exist to make communication via the internet secure, one of these approaches is steganography. Computer steganography can be defined as a method of hiding data in cover media so that others are not aware of its existence. Quantum computers, built on the principles of quantum physics, have introduced new possibilities for researchers in security and computer science. This paper explores the fundamentals of quantum computing, its achievements, and the challenges and future prospects it presents in the field of cryptography and steganography. Quantum computers give us a new approach to different kinds of complicated problems in security fields by creating multi-state computing spaces. The article deals with the steganography system which hides text inside images and after that realize quantum communication. The secret message is hidden in the cover image using Least Significant Bit (LSB) algorithm. The paper proposes an information transmission scheme with a quantum channel enabled. Quantum key distribution (QKD) is a secure communication method that implements a cryptographic protocol involving components of quantum mechanics**

Keywords*— *Quantum Key Distribution, Quantum Steganography, Qubits, Security.

I. Introduction

Nowadays in the world of information technologies, unprotected and obviously data transmission is tantamount to suicide. The use of steganography, in close connection with cryptography and securing with static passwords in the authentication process protects against the high risk of information security.

Quantum computers give us a new approach to different kinds of complicated problems in security fields by creating multi-state computing spaces.

In classical computing, the basic unit of information is the bit, which can be either a 0 or a 1. In contrast, quantum computing uses qubits, or quantum bits, which can exist in a state of 0, 1, or both simultaneously, thanks to a property called superposition. This allows quantum computers to perform many calculations at once, making them potentially much more powerful for certain tasks compared to classical computers. [1] told us that we can imagine a spinning coin, representing both heads and tails until it lands – that's the essence of superposition, a quantum phenomenon defying classical logic yet unlocking immense computational potential.

Computer steganography conceals the existence of secret information in the cover carrier [2], [3], [4] and [5].

The study aimed to analyze the possibility of secure use of steganography in the implementation of quantum communication.

Quantum steganography leverages the principles of quantum mechanics, such as superposition and entanglement, to hide information within quantum states [6]. This makes it even more secure compared to classical steganography, as any attempt to intercept the hidden information would disturb the quantum state and reveal the presence of eavesdropping [7].

The quantum steganography can indeed be used in quantum communication [8]. The firewall works based on the consistent application of rules that are divided into two parts [9], [10].

In figure 1 we can see the potential of quantum steganography, which could to address various security and privacy challenges. It is extremely interesting that these areas could expand and almost no area of people's public life would be untouched. A wide field for research opens up. Quantum steganography will strengthen the resilience of quantum cryptography, due to the fact of absolute imperceptibility.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8485

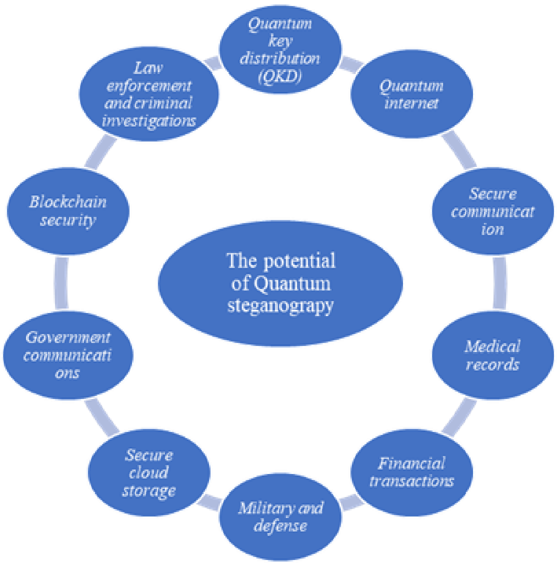
The potential of Quantum steganograpy
Quantum key distribution (QKD)
Quantum internet
Secure communicat ion
Medical records
Financial transactions
Military and defense
Secure cloud storage
Government communicati ons
Blockchain security
Law enforcement and criminal investigations

Fig. 1. Applications of quantum steganography

II. MATERIALS AND METHODS

A. Basic characteristics of Quantum steganography algorithms evaluation.

Least Significant Bit (LSB) replacement is the process of adjusting the most significant bits of the pixels of the cover image [11]. More details about how work LSB could be found in [12-15]. Steganography provides a way to transfer this information via ordinary files, thus reducing the risk of disclosure [16].

Least Significant Bit Qubits (LSBq) is presented in [17], [18] and [19]. In this case, embeds the secret message's qubits to the carrier image's least significant qubits, researchers increased *LSB's* security by embedding it by a modulo value rather than in order. However, there have the limitations: using primarily *LSBq* makes it easy for intruders to detect and extract the steganographic image and can result in low imperceptibility.

When comparing two images four major statistical properties which describe the degree of similarity between the images are calculated: *MSE* (Mean Squared Error), *PSNR* (Peak Signal-to-Noise Ratio) and images entropy.

The characteristics studied are represented by formulas (1) and (2), the PSNR is based on values obtained for the MSE:

$$MSE \ = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,\ j)-K(i,\ j)]^2, \qquad (1)$$

where m and n are the width and height of the image; I (i, j) and K (i, j) are relevant pixels with coordinates (i, j) in the original stego-image.

$$PSNR\ = 10.log_{10}(\frac{max^2}{MSE}) = 10.log_{10}(\frac{max}{\sqrt{MSE}}), \qquad (2)$$

where MAX = 255 for 8 bit images.

Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. The entropy of an image can be calculated by calculating at each pixel position *(i, j)* the entropy of the pixel-values within a 2-dim region centered at *(i, j)*.

$$entropy = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} p(i,\ j)log\log_b p(i,j) \qquad (3),$$

where n and b are again the number of gray levels and the base of the logarithm function, respectively, and *p(i, j)* stands for the probability of two pixels separated by the specified offset having intensities *i* and j.

Quantum Mean Squared Error (QMSE) is typically used to quantify the difference between a target quantum state and an estimated quantum state. The calculation depends on the context, but here are the common approaches

QMSE-One approach uses fidelity

$$F(\rho,\sigma) = Tr\left(\sqrt{\sqrt{\sigma}\sqrt{\rho\sigma}}\right)^2 \qquad (3)$$

to compare two quantum states ρ and σ, where ρ is the target state and σ is the estimated state. A common definition of QMSE in this context is (4):

$$QMSE=1-F(\rho,\sigma) \qquad (4)$$

where *F(ρ,σ)* is the fidelity between the density matrices.

The formula for QPSNR (5) is derived from the traditional PSNR formula and is expressed as:

$$QPSNR\ = 10.log_{10}(\frac{max^2}{MSE}), \qquad (5)$$

where MAX is the maximum possible pixel value (for example, 255 for an 8-bit image).

In [20] proposed a new model based on *log-polar* coordinates (quantum log-polar image, *QUALPI*). A log polar image with a resolution *of* 2^mX2^n and a gray level of *q2* can be represented by the following equations.

$$|I\rangle = \frac{1}{\sqrt{2^{m+n}}}\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}(|g(\rho,\theta)\rangle \otimes |\rho\rangle \otimes |\theta\rangle \quad ($$

$$g\,(\rho,\theta) = C_0C_1\cdots C_{q-2}C_{q-1},\ g\,(\rho,\theta) \in \left[0, 2^q-1\right]$$

([20]

Here, *p* represents information of the image in the radial direction, *Θ* represents information of the image in the axial direction, and *(p, Θ)* represents the position information of the image pixels. *g (p, Θ)* represents the gray value of the pixel. In addition, the preparation process of quantum images is given in detail in [20].

III. RESULTS AND DISCUSSION

A. Quantum steganography protocol.

The quantum analogue of the *classical binary symmetric channel* (BSC) is the *depolarizing channel* (DC) which is one of the most widely used quantum channel models:

$$\rho \rightarrow N\rho = (1-p)\rho + \frac{p}{3}\, X\rho X + \frac{p}{3}\, Y\rho Y + \frac{p}{3}\, Z\rho Z \quad (6)$$

That is, each qubit has an equal probability of undergoing an X, Y or Z error. Applying this channel repeatedly to a qubit will map it eventually to the maximally mixed *state* $\frac{I}{2}$.

It is possible to rewrite this channel in a different but equivalent form:

$$N = \left(1 - \frac{4p}{3}\right) I\rho + \left(\frac{4p}{3}\right) T\rho \qquad (7)$$

where $I\rho = \rho$ and

$$T\rho = \left(\frac{1}{4}\right)(\rho + X\rho X + Y\rho Y + Z\rho Z) \quad (8)$$

The operation $T\rho$ is twirling: it takes a qubit in any state ρ to the maximally mixed state $\frac{I}{2}$. If was rewritten the channel in this way, instead of applying *X, Y, or Z* errors with probability $\frac{p}{3}$, we can think of removing the qubit with probability $\frac{4p}{3}$, and replacing it with a maximally mixed state.

The figure 2 makes the steganographic protocol more transparent. It will possible at first assume the actual physical channel between Alice and Bob is noiseless. All the noise that Eve sees is due to deliberate errors that Alice applies to her codewords.

Step 3 share with us how Alice chooses a random subset of *M* qubits out of the *N*, and swaps her *M* stego qubits for those qubits of the codeword. She also replaces a random number *m* of qubits outside this subset with maximally mixed qubits, so that the total *Q=M+m* matches the binomial distribution (6) to high accuracy.

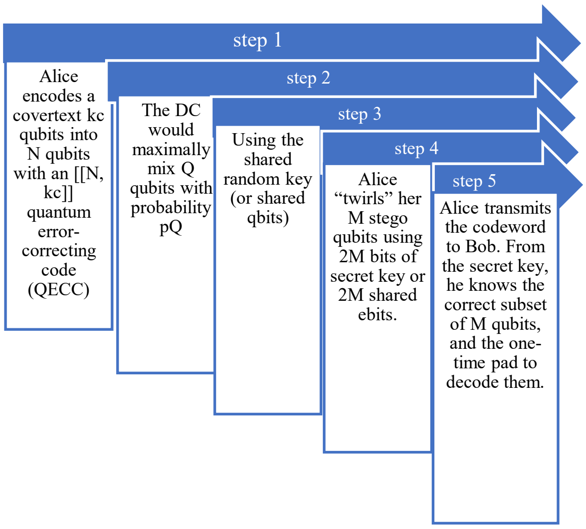
step 1
step 2
step 3
step 4
step 5
Alice encodes a covertext kc qubits into N qubits with an [[N, kc]] quantum error-correcting code (QECC)
The DC would maximally mix Q qubits with probability pQ
Using the shared random key (or shared qbits)
Alice "twirls" her M stego qubits using 2M bits of secret key or 2M shared ebits.
Alice transmits the codeword to Bob. From the secret key, he knows the correct subset of M qubits, and the one-time pad to decode them.

Fig. 2 Visualization quantum steganography protocol.

Generate two entangled qubits: *QubitA* and *QubitB*, such that their states are correlated. *QubitA* was prepared in a superposition state that will represent the hidden information. The specific state preparation depends on the encoding method chosen [1].

B. Simplified conceptual quantum algorithm.

The figure 3 provides and included a short description of scheme methodology of simplified conceptual quantum algorithm.

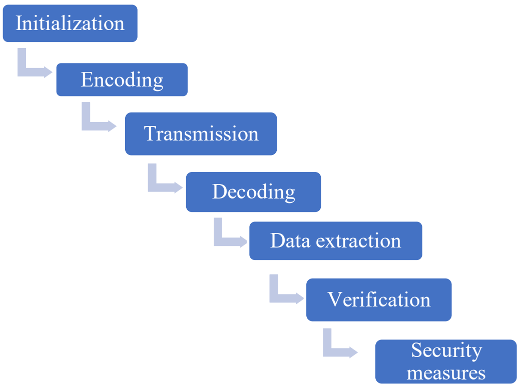

Fig. 3. Flowchart of simplified conceptual quantum algorithm for communication.

It's (9) to calculate the maximum number of secret information's bits transmitted per time.

$$[X]_{max} = log2\frac{360^{0}}{\theta} \qquad (9)$$

where, is θ smaller than the minimum rotation angle at which the image is expanded, and $[X]_{max}$ denotes the maximum number of secret information's bits by calculation.

Finally, quantum communication in free space involves many basic infrastructure elements that are extremely important for any quantum communication link. They are also critically important due to the direct impact on the reliability, security and efficiency of the quantum communication node.

IV. Other recommendations

A. The future of secure quantum communication

One of the main aims of the realized research of the steganography system is its practical applicability and evaluation in terms of the invisibility and size of the hidden data in the cover images.

Steganography algorithm for embedding information in images uses the *LSB* in each colour channel pixels and after that used quantum channel to send a key. How this works presented on figure 4, a stego image can use an opened communicate channel.

Thus, it is checked and ensured what operation will be implemented and the confidential information is preserved. This is the basic communication scheme with the steganographic environment included.

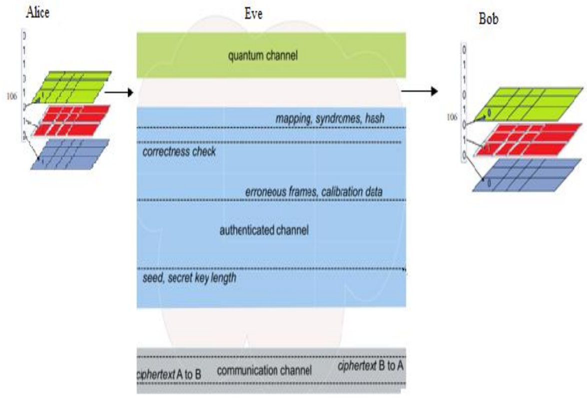

Fig.4. LSB Replacement embedding in colour image using quantum channel.

QKD is a part of quantum cryptography [21]. It is a secure communication method for exchanging encryption keys only known between shared parties. *QKD* network architecture can to be seen in figure 5:

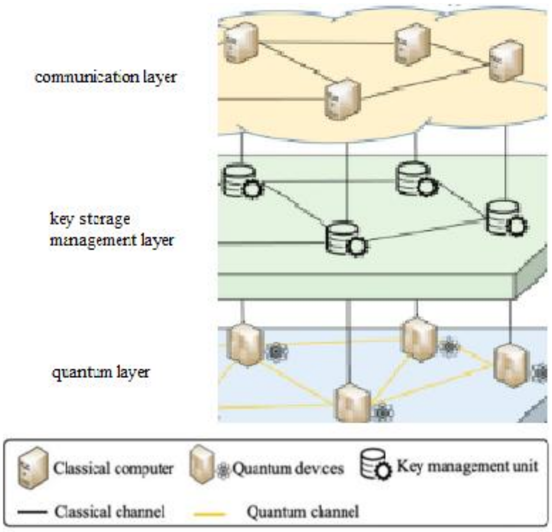

Fig.5. Communication scheme on layers on the QKD network.

A wide area *QKD* network is composed by a set of quantum, point to point, nodes linked by quantum channels. These links could also include information theoretic security (ITS) switched networks, like the access network depicted at the lower rigth corner. The set of quantum nodes and links form the quantum level. Many of the quantum nodes will act as classical repeaters by retransmitting the keys distilled from the signals of one of the quantum links using another quantum link connected to the same node [21]. In general scheme of the communication could establish three layers – communication layer (Key users, for example encryptors), key storage management layer (Protection of the encryption keys via using *QKD* keys for every hop) and quantum layer (Key Generation –symmetrically independent).

B. Quantum Key Distribution.

In general, *QKD* is combined with conventional encryption systems, such as AES, where the generated *QKD* key is used by Alice and Bob to generate a temporary session key with AES, to encrypt their messages over Ethernet until it expires, and *QKD* protocols require the ability to create, manipulate, transmit and detect signals at the quantum level.

When the cover protocol consists of communicating classically over a quantum channel, we show that, in addition to the cover classical message, entangled qubits can be generated [22]. Currently, the number of qubits that can be controlled and manipulated in a laboratory environment is still very small, limiting the potential of quantum computing. Another fundamental problem of a quantum computer is how to send and receive information from it. Some critics consider this problem insolvable. However, this appears to be less of a problem in optical quantum computers where qubits are defined in terms of photons [1]. In [23] is presented the hierarchical decision model of cybersecurity risk assessment.

V. CONCLUSIONS

In conclusion, this paper encompasses a discussion on the field of quantum steganography, which is a process of hiding information in existing content. Mostly images are used to hide the content. Unlike classical steganography, which hides information in plain sight, quantum steganography leverages quantum entanglement and superposition to encode data in quantum states, making it exceptionally resistant to unauthorized interception or decryption.

In the local way had have lack of understanding regarding the necessity of *QKD* implementation, the equipment has high prices and lack of standards, but QKD is likely the most advanced quantum technology currently accessible in use. With the increase in computing power, cyber security is getting complicated.

The importance of the use Quantum Steganography as a means to hide sensitive information through public channels by governments, companies and individuals are important. This is because countries exchange confidential information in their daily activities. Least significant qubit: uses the carrier image’s least significant qubits to embed the needed secret qubits.

ACKNOWLEDGEMENT

The author would like to thanks that paper was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022

REFERENCES

[1] M. Imanparast, “The prospect of cryptography and computing with quantum computers”, 8th International Conference on Combinatorics, Cryptography, Computer Science and Computation, pp.379-384, 2023.

[2] N. Subramanian, S. Al-maadeed, A. Bouridane, “Image Steganography: A Review of the Recent Advances”, IEEE Access, vol. 9, 2021, pp.23409-23423, doi:10.1109/ACCESS.2021.3053998.

[3] P. Mandal, I. Mukherjee, G. Paul, B. Chatterji, “Digital image steganography A literature survey”, Information Sciences,

Elsevier Inc, volume 609, 2021, pp. 1451–1488, ISSN: 0020-0255, [Online]. Available: doi.org/10.1016/j.ins.2022.07.120

[4] D. Artz, "Digital steganography: hiding data within data", in IEEE Internet Computing, vol. 5, no. 3, pp. 75-80, 2001, doi: 10.1109/4236.935180

[5] V. Stoyanova, "Research of the characteristics of a steganography algorithm in images when using different alphabet" Environment. Technologies. Resources. Proceedings of the International Scientific and Practical Conference. Vol. 4. 2024, https://doi.org/10.17770/etr2024vol4.8236.

[6] A. Agrawal, R. Soni, and A. Tomar, "Perspective Chapter: Quantum Steganography – Encoding Secrets in the Quantum Domain" in Steganography - The Art of Hiding Information. IntechOpen, Apr. 19, 2024, doi: 10.5772/intechopen.1004597.

[7] B. A. Shaw, T. A. Brun, "Quantum Steganography", arXiv:1006.1934, 10 Jun 2010, https://doi.org/10.48550/arXiv.1006.1934

[8] N. Min-Allah, N. Nagy, M. Aljabri, M. Alkharraa, M. Alqahtani, D. Alghamdi, R. Sabri and R. Alshaikh, "Quantum Image Steganography Schemes for Data Hiding: A Survey", Applied Sciences, 12(20), 2022, 10294. https://doi.org/10.3390/app122010294

[9] Ts.Tsankov, L.Staneva, I.Vardeva and D.Iliev, "Generalized net model of a communication network using the Port Knocking method", Scientific Conference with international participation MATTEH 2022, Conference proceeding, Vol. 2, Shumen, 2022, ISSN 1314-3921, pp. 29-34

[10] Ts.Tsankov, T.Trifonov and L.Staneva, "A survey of phase manipulated signals with high structural complexity and small loses after processing with mismatched filters", Konstantin Preslavski University Of Shumen, Jornal Scientific and applid reserch, 2013, https://jsar.ftn.shu.bg › jsar › article › download, [Accessed Yan 24, 2025].

[11] V.Stoyanova, "Steganography System Using LSB Methods", Proceedings of the ENTRENOVA. ENTerprise REsearch InNOVAtion Conference, Split. Croatia, IRENET – Society for Advancing Innovation and Research in Economy, Zagreb. 6–8 .09.2018. Vol. 4. P. 381–387

[12] M.Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, vol. 6, no. 79, pp. 3907 – 3915, 2012.

[13] C. K.Chan and L. M.Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition, vol. 37, pp. 469-474, 2004.

[14] C. C. Chang, J. Y. Hsiao and C. S. Chan, "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy", Pattern Recognition, vol. 36, pp. 1583-1595, 2003.

[15] C. H.Yang and S.-J.Wang, "Transforming LSB Substitution for Image-based Steganography in Matching Algorithms", Journal of Information Science and Engineering, vol. 26, pp. 1199-1212, 2010. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=fe144037adc9e934a44cb1f31aaee4ed5cb4cd2e, [Accessed Yan 24, 2025].

[16] G. A. Kozarev and St. H. Parvanov, "Research opportunities for using steganographic methods in the field of defense", Proceedings of International Scientific Conference-Defense Technologies‖ DefTech 2024, Shumen, pp.637-642, ISSN 2367-7902.

[17] R.G.Zhou, J.Luo, X.Liu, C.Zhu, L.Wei and X.Zhang, "A novel quantum image steganography scheme based on LSB", International Journal of Theoretical Physics, June 2018, 57, 1848–1863, DOI: 10.1007/s10773-018-3710-x.

[18] A.G.Tudorache, V.Manta and S.Caraiman, "Quantum Steganography Using Two Hidden Thresholds", Adv. Electr. Comput. Eng. 2021, 21, 79–88.

[19] E. Şahin, I.Yilmaz "QRMW:Quantum representation of multi wavelength images", Turk. J. Electr. Eng. Comput. Sci., 7, 2018, pp.68–779.

[20] Y. Zhang, K. Lu, Y. Gao, and K. Xu, "A novel quantum representation for log-polar images," Quantum Inf. Process., vol. 12, no. 9, pp. 3103_3126, Sep. 2013.

[21] V. Martin, M.J.Martinez and M.Peev, "Introduction to Quantum Key Distribution", 2016, http://www.gcc.fi.upm.es/publications/qkd_intro.pdf

[22] M. Tahmasbi and M. R. Bloch, "Steganography protocols for quantum channels", Journal of Mathematical Physics, vol.61, issue 8, August 2020;082201. https://doi.org/10.1063/5.0004731

[23] V. Petrova, "The Hierarchical Decision Model of cybersecurity risk assessment", 12th National Conference with International Participation (Electronica), vol. 1, 2021, pp. 1-4, doi:10.1109/ELECTRONICA52725.2021.9513722. 978-1-66544061-5.