



Image Steganography based on Fredkin gate and Improved path distribution with Quantum key exchange protocol

Project Thesis

Submitted By

17-33357-1	Morshed, Md. Niaz
16-32822-3	Sunny, Fazla Rabby
16-32768-3	Robin, Md. Mehedi Hasan

Department of Computer Science

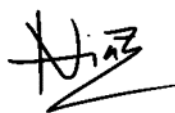
Faculty of Science & Technology

American International University Bangladesh

November, 2020

Declaration

We declare that this thesis is our original work and has not been submitted in any form for another degree or diploma at any university or other institute of tertiary education. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.



Morshed, Md. Niaz
17-33357-1
CSSE



Sunny, Fazla Rabby
16-32822-3
CSSE



Robin, Md. Mehedi Hasan
16-32768-3
CSSE

Approval

The thesis titled “Image steganography based on Fredkin gate and Improved path distribution with Quantum key exchange protocol” has been submitted to the following respected members of the board of examiners of the department of computer science in partial fulfilment of the requirements for the degree of Bachelor of Science in Computer Science on 8th November and has been accepted as satisfactory.

MSS

DR. A.F.M. Saifuddin Saif

Sr Assistant Professor & Supervisor
Department of Computer Science
American International University-Bangladesh

MD. Anwarul Kabir

Sr Assistant Professor & External
Department of Computer Science
American International University-Bangladesh

DR. MD. Mahbub Chowdhury Mishu

Assistant Professor & Head (Undergraduate)
Department of Computer Science
American International University-Bangladesh

Professor Dr. Tafazzal Hossain

Dean
Faculty of Science & Technology
American International University-Bangladesh

Dr. Carmen Z. Lamagna

Vice Chancellor
American International University-Bangladesh

Acknowledgment

First of all, we would like to be grateful to the Almighty ALLAH, who gives us the effort to work on this very thesis. We want to especially thank our honorable supervisor DR. AFM Saifuddin Saif, Sr Assistant Professor, American International University-Bangladesh [AIUB] for his consistent support and great supervision to make this thesis possible. We also want to thank our Vice Chancellor Dr. Carmen Z. Lamagna, our Dean Prof. Dr. Tafazzal Hossain, our Associate Dean in Charge Mashioor Rahman, our Director of Department Dr. Dip Nandi, and our head of the department Dr. Md. Mahbub Chowdhury Mishu for their constant motivation and support. This project is the outcome of our relentless work and our supervisor's initiative and constant motivation.

Abstract

Steganography is the art of hiding secret data into an innocent carrier data for secure communication. There are so many researches on this technique with image, video, text, and other medium but image is the most popular among them. Steganography shines in the classical system, but some people also trying to achieve the quantum steganography method for future systems. In our research, we tried to develop a method that can merge the quantum system tools into the classical system implementation to create room for quantum steganographic possibilities in the future. We used Fredkin gate's classical representation which is a Quantum gate with Quantum key exchange protocol I: BB84 for better path redistribution and security measure. We used the Canny algorithm for image segmentation and applied an advanced sorting algorithm to get dense area pixels. The results show that we achieved a highly balanced quality measure with high payload capacity, greater invisibility, and robustness with better security than many current methods.

Table of Contents

Chapter 1: Introduction	1
1.1 Introduction	1
1.2 Research Background	1
1.3 Problem Statement	2
1.4 Scope of the Research	2
1.5 Objectives	2
1.6 Significance of the Research	3
1.7 Research Outlines	3
1.8 Conclusion	4
Chapter 2: Literature Review	5
2.1 Introduction	5
2.2 Existing Research Methods	5
2.3 Observation and Discussion	8
2.4 Conclusion	10
Chapter 3: Research Methodology	11
3.1 Introduction	11
3.2 Proposed Method	11
3.3 Conclusion	18
Chapter 4: Experimental Research	19
4.1 Introduction	19
4.2 Experimental Results	19
4.3 Conclusion	28
Chapter 5: Conclusion and Future Work	29
5.1 Introduction	29
5.2 Contribution of the Research	29
5.3 Future Work	30
5.4 Conclusion	31
References	32

List of Tables

Table 1-A	Relative capacity of different datasets	20
Table 1-B	Relative capacity comparison with previous Research	20
Table 2-A	Average PSNR for in different Datasets each consists of 10 thousand images	22
Table 2-B	Comparison of PSNR values with previous research	22
Table 3-A	SSIM index on multiple datasets	25
Table 3-B	Comparison of the SSIM index with previous research	25
Table 4	SSIM results for datasets with noise and very low size	27
Table 5	Table 8: PSNR results for datasets with noise and very low size	28
Table 6	Computation time per image on all datasets	28

List of Figures

Fig. 1.1	Fredkin Gate Representation	12
Fig. 1.2	Two bases used for BB84 (“Plus” and “Times” respectively)	13
Fig. 1.3	Embedding diagram for the classical system	16
Fig. 1.4	Extracting diagram for the classical system	17
Fig. 2.1	PSNR values of 10100 images	21
Fig. 2.2	SSIM index of 10100 images	24
Fig. 2.3	Circuit diagram of Two Qubits entanglement	26
Fig. 2.4	Results of the Entangled Qubits	27

Chapter 1: Introduction

1.1 Introduction

In this modern era, the world dynamics are severely dependent on the Internet and digital data and confidentiality has increasingly emerged as a top priority, and one of the major concerns. Data hiding facilitates covert communications. Steganography is the art of hiding secret data in carrier data to outplay the middle guy who tries various algorithms to crack the encryption of a file when he/she gets suspicious as the file is encrypted. Encryption always creates suspicion about the file and no matter how complex the encryption is, it can be cracked at some point with the right tools. So, steganography tries hiding the important data into a general cover file which won't reveal anything and looks like a normal image. So, the chance of suspicion gets lower and thus the security of the main file is improved. There are two types of data hiding which are watermarking and steganography which are used for protecting sensitive data from unauthorized access. In the encryption and watermarking technologies, there are so many types and their pros and cons. They help to improve security and for that reason, many steganography methods use cryptography into the framework to make the whole method so much secure. We believe that, with improved steganography methods, digital data communications, and information technology will get so many new possibilities.

1.2 Research Background

Steganography is the art of hiding information into a piece of cover information. In this modern era of world wide web and high-speed internet, data communication security and privacy become one of the most concerned necessities which are a never-ending and forever developing area. The more secure way is found the more vulnerabilities take place founded by hackers and unauthorized persons. In the area of steganography, there is Steganalysis which is the opposite of steganography where we look for hidden information in a suspected file. So, the improvement of steganography drives the improvement of Steganalysis and vice versa. There are so many types of steganography but we will divide it into two major types which are classical steganography and quantum steganography. Each type has all other types as image, audio, video, text, and even very unconventional like DNA or MS excel cell steganography. In this research, we will be discussing Image steganography and may review some others. many researchers tried different quantum image steganography methods and frameworks. The actual embedding procedure may get similar to the classical methods but all the operations and logics must

be performed through the quantum circuits and thus the whole process gets changed and often results in much complex experiments and frameworks.

1.3 Problem Statement

We are living in an era of digital technology where fast and secure communication is a big concern where privacy matters most and security is a top priority. Data hiding facilitates covert communications. Steganography makes it easier with so many data hiding techniques. So many researchers are working on new methods to improve the efficiency and overall qualities to create a safer digital communication area. The main key qualities of steganography have been capacity, invisibility, and security. Researchers are trying to improve these qualities with new methods or improving the older methods, some researchers invented quantum steganography methods. Quantum steganography methods are necessary for the near future when quantum computation will be available for more people. But the methods are not practical for the current classical systems. Many of the classical steganography methods have the high capacity or high invisibility or high security but they all lack one of the key features to improve another. In this research, we will try to develop a method where all the qualities will be improved in a balanced way and rooms for quantum systems so that the method can work in the quantum system as well.

1.4 Scope of the Research

This research is based on the Quantum gate, Canny edge detection and Quantum key exchange algorithm where the used gates were Fredkin gate and CNOT gate and the protocol name is BB84. The research used RGB images of various size and quality as the communication method. So, the scope of this research is limited to Fredkin gate, CNOT gate, canny edge detection algorithm, Quantum key exchange protocol I: BB84, and any RGB images.

1.5 Objectives

The main objectives of this research are to:

- Develop a method with Quantum system possibilities
- Improve Payload capacity
- Improve imperceptibility
- Improve data security

- Create a balance between all quality factors
- Merge Quantum gates into the classical system

1.6 Significance of the Research

This research is focused on data security and developed a new method of steganography with more payload capacity and better imperceptibility. It can be used in any type of digital communication for higher privacy and secure communications. Any researcher can develop it further to improve certain areas and efficiency.

1.7 Research Outlines

The research outlines of the following research paper are shown below:

1. Introduction
 - 1.1 Introduction
 - 1.2 Research Background
 - 1.3 Problem Statement
 - 1.4 Scope of the Research
 - 1.5 Objectives
 - 1.6 Significance of the Research
 - 1.7 Research Outlines
 - 1.8 Conclusion
2. Literature Review
 - 2.1 Introduction
 - 2.2 Existing Research Methods
 - 2.3 Observation and Discussion
 - 2.4 Conclusion
3. Research Methodology
 - 3.1 Introduction
 - 3.2 Proposed Method

3.3 Conclusion

4. Experimental Results

4.1 Introduction

4.2 Experimental Results

4.3 Conclusion

5. Conclusion and Future Work

5.1 Introduction

5.2 Contribution of the Research

5.3 Future work

5.4 Conclusion

Bibliography

1.8 Conclusion

In digital communication, fast and secure communication is the highest priority. Steganography improves security by hiding the main secret data into carrier data. Many methods have been developed with various frameworks and approaches but there is no end for improvements in this domain. Better capacity, higher security, and better imperceptibility is an endless necessity for these communication techniques. Many methods have improved these quality factors but they all lack in some areas. After the evolution of cryptography, there was a necessity for a new method which will not have the problems in cryptography but help in secure communication where steganography stands out because of less suspicion which leads us to more secure communication where hackers will have to check endless possibilities to know if a data is hidden or not as the carriers are innocent. Steganography shines in the classical system with so many methods and approaches in various spaces. People are now upgrading it to use it in the Quantum system as well. We tried to merge the possibilities to create a system that is usable in the present classical system as well as in the Quantum system soon. Our method used Quantum gates and key exchange protocol which motivates us to use it in quantum systems. To conclude, we believe in more improvements in steganography which will create such secure digital communication where people can share information more safely.

Chapter 2: Literature Review

2.1 Introduction

Image-based steganography means the cover file is an image. Here the image gets manipulated and the secret information gets hidden in the pixels of the image with different methods. The secret information can be another image or text, some binary bits, audio, GIF, or even quantum bits. The secret information gets encoded to embed it in the cover image. One of the very first and most popular methods for image steganography is the LSB method where the LSB of the pixels of the cover image gets replaced by the secret message bits. Quantum steganography is the area where quantum bits are used in the process of steganography. From the QIP (Quantum image processing) and Quantum computing evolution using quantum bits in the method and securing the process for upcoming quantum computers is essential for advanced security. Quantum computers have parallel computing powers that enable the possibilities of destroying most of the classical data security and that is the reason we will be focusing on that though the resources are very limited and not feasible with the current computing and communicating devices. What will be trying to find is that if there's a way of merging both systems and develop a new method which will be feasible with general communicating and computing devices reserving the advanced security for upcoming quantum computing and QIP evolution.

2.2 Existing Research Methods

There have been many methods that are introduced to steganography techniques. All the methods improve one or more parts of the system but can't improve the whole as the constraints are there. The most popular is the simple LSB method which is the most basic approach where the LSBs (Least Significant Bit) are replaced with the secret information bit. But as being simple its security is low and integrity is much lower than all the modern frameworks [7]. Capacity is a big issue for steganography. Multiple embedding [30] tried to solve the capacity issue where the pixels are divided into blocks and these blocks help multiple embedding which improves the embedding capacity, PSNR value, and error correction capability. But the method has higher complexity issues and it is based on attacking where steganography is mainly for lessening the attacks. To solve this, we can use pure LSB but it led us to a less secured framework. But LSB and secret map techniques tried to solve this issue [6].

In LSB and secret map techniques-based approach, the secret information bit length is set to the very first two pixels and a random key is generated from the 3D Chebyshev map.

This method has higher and improved results in terms of key sensitivity, hiding capacity, quality index, MSE, PSNR, and image fidelity. But too many keys and mappings make this method too much complex. Xintao Duan and others tried a different approach with an image elliptic curve and deep neural network which is highly efficient and provides great capacity [16]. The semantic segmentation method was used by Nan Pan and others in their research which is based on video steganography [18]. The experiments show that it has a large capacity and a certain resistance to noise attacks. A very different and unconventional approach was made by Chin-Feng Lee and others where they used the 3D magic cube and magic matrix for data hiding with ensuring very high capacity [21]. From QIP (Quantum Image Processing) research area some researchers tried to solve the capacity issues. Ahmed A. Abd El-Latif and others tried QIP, Arnold's cat map and controlled-NOT gate for their research and the results show excellent visual quality and high embedding capacity and security [34]. Another research-based on Least significant Qubit has also a higher capacity as it utilized NEQR for quantum representation [51]. They used Hadamard transformation in another research on a new Quantum Image steganography scheme [49]. The method has a higher hidden capacity and efficiency. But it creates a security vulnerability.

To solve the issue Ahmad Fashiha and others tried hiding multiple secret messages where they used dynamic image bit manipulation which is another form of LSB method where the LSB has been chosen dynamically [35]. Some researchers are dedicated to increasing the capacity of the system. Jung-Yao Yeh and others Focused on a high-payload-based hiding method which is for AMBTC decompressed images [31]. They start with finding a unique decodable dictionary. After that, they start an embedding stage and complete it with the extraction stage. Yu Zhang and others tried the MOPNA method. MOPNA (Modulus Calculations on Prime Number Algorithm) divides the cover- image into pixel groups that include two pixels [41]. Ningwu used state transition-binary sequence in their research on coverless text steganography. They sorted out the frequency and added information matching rules [26]. Various GAN (Generative adversarial network) based approaches have been taken in Steganography. Xintao Duan and others used it in their research on a coverless steganography method [12].

One of the new major problems that arise in these methods is the lack of robustness. Zhang, Yang, and others have tried a generative method to solve the robustness issues and other problems by covering synthesis with auxiliary semantics [8]. Some researchers tried different segmentation methods for increasing robustness. Ruohan Meng and others used instance segmentation and Mask R-CNN in their research which shows greater robustness in the experimental results [11]. A novel approach was taken by P.G. Kuppusamy and others which is based on modified cycle generative adversarial networks. They used seven steps where they used discriminators and neural networks [14]. The results show high robustness. Ki-Hyun Jung and others used a dedicated method for improving the robustness of the system. In their research, they used a two-layer embedding strategy for robust reversible data hiding scheme [25].

Now that some improved capacity and some improved robustness, some research has been done where capacity and robustness both were focused. Heng Yao and others used prediction error shifts for their research which is based on high-fidelity dual-image reversible data hiding [38]. In another field, Po-Yeuh Chen and Hung-Ju Lin used A DWT based approach for their Image steganography scheme and the results show that they improved both robustness and capacity [45]. Then from the QIP area, Zhiguo Qu and others used quantum image expansion and Grover search algorithm in their research on the Quantum Image steganography protocol. The experiments show that it can achieve good imperceptibility, security, and large capacity by quantum uncertainty and quantum non-cloning theorems [54].

There are so much researches that have been done on other areas of steganography and unconventional approaches were taken. Nan Jiang proposed a Control Value of the Control Quantum circuit phase before the Image partition [15]. Chris did their research on Quantum steganography over Noiseless Channels. The results show high efficiency and good quality [22]. Zaynalov used MS excel cells in steganography which ensured very high capacity but with a more suspectable file system the method lacks security [32] and Xiaofeng used structured medical pathology on an optimized convolutional Neural network where the method has very high complexity [24]. In the same area, Zhijun used K-means for their research which provides better speech quality but the system is very unconventional, it is rare to be used, [17] and Esra used a compression-based approach but not highly secured as the data compression is much popular [13]. Mingji Yu used an adaptive and separable based approach in the encryption domain which is very efficient but not highly secured [9].

In terms of video steganography, Bo Guan proposed selective encryption of HEVC video along with various sign encryption process which maintain both high capacity and robustness [10]. Devishree proposed meaningful encryption on their research which lacks both robustness and capacity [41] and in the other area, Dokyun Na proposed an unconventional and a new method for DNA steganography which may get very useful in the medical industry but not for general use as it is risky for health [20]. Haval and others proposed an efficient multi-secret approach which includes real and false data and causes low capacity [39]. Shailender used the most basic method which is LSB which is highly insecure [23] and keeping the simplicity and speed Piotr used the indiscernibility mask key but it is not focused on capacity or robustness [40]. Speaking of efficiency Zhenyu proposed 3D wavelet multiresolution analysis but with high complexity maintained high efficiency in detecting the hidden message. [33] Nan Wei also proposed generative adversarial networks that result as highly efficient but not focused on capacity [36]. Jia Liu also described advancements through GAN but did not propose any new methods or framework [37]. Zhe Liu proposed a Chaotic map in the DCT domain which improved the security of video steganography [29]. Nada Abdul proposed inserting invisible character to ensure multi-level complexity to avoid attackers but not focused on robustness and capacity [28] and Manuilova proposed a wavelet method on audio

steganography which improved robustness and extra security but not focused on capacity [27]. Ahmed proposed substitution boxes based on quantum walks in their method which is highly efficient but is limited to the usage in terms of devices [43] and Suzhen proposed quantum digital image processing consists of quantum image edge detection algorithm and quantum adaptive median filtering algorithm where adaptive median filtering can suppress pulse noise and edge detection handles the image segmentation and mode recognition [46]. Shen used the concrete least significant qubit information hiding algorithm for quantum image and about the frequency domain LSQb information hiding algorithm for quantum image [47] and Yahya proposed LSQu- block image information concealing algorithm but the study of quantum image LSB information hiding is still in its infancy [50]. Jia Luo proposed American Standard Code for Information Interchange (ASCII) but the method has low security and robustness issues [51] and the same happened with Shahrokh with their Quantum red-green-blue steganography research where the method is highly efficient but not focused on security and robustness [55]. Gyan proposed Hamilton Path in their research. Due to the complexity of Hamiltonian path generation, the embedding patterns become almost impossible to guess, even if the presence of secret data is observed using steganographic attacks. [53]. Sanjeev proposed novel fuzzy edge identification and adaptive steganography. It ensures the exact edge location after embedding the message and correctly extracts the concealed information from the stego image but it is not highly secured and it has a low capacity [48]. Joachim used the investigation of the steganographic communication approach which is not focused on security issues but measures which communication approach works better than others [44]. Mohanad and others proposed two random functions with Fibonacci decomposition along with the chaotic map on their research [19]. It provides one of the highest levels of security where four consecutive levels of security are added but too much security makes it too much complex and PSNR values show that it has low robustness.

2.3 Observation and Discussion

Steganography is the art of hiding the main data into fake data. There have been many methods and frameworks proposed in this technology and it has been improved many times. The most popular method is a simple LSB method which is the most basic approach where the LSB bits are replaced with the secret information bit. But as being simple its security is low and integrity is much lower than all the modern methods. This method is easily detectable and has no extra security to it. It doesn't have high capacity embedding and capacity is a big issue for steganography. Through multiple embedding, some tried to solve the capacity issue where the pixels are divided into blocks and these blocks help multiple embedding which improves the embedding capacity, PSNR value, and error correction capability. But the framework has higher complexity issues and it is based on attacking where steganography is mainly for lessening the attacks. To solve this, we can use pure LSB but it led us to a less secured framework. In LSB and secret map

techniques-based framework they had higher and improved results in terms of key sensitivity, hiding capacity, quality index, MSE, PSNR, and image fidelity. But too many keys and mappings make this framework too much complex. With an image elliptic curve and deep neural network which we can achieve high quality and capacity embedding. The framework has a higher complexity. A very different and unconventional approach ensured a very high capacity with a 3D magic cube. From QIP (Quantum Image Processing) research area some researchers tried to solve the capacity issues. Arnold's cat map and controlled-NOT gate in their research show excellent visual quality and high embedding capacity and security. Their Another research based on Least significant Qubit has also higher capacity as it utilized NEQR for quantum representation.

The new problem that arises in many of those researches is the lack of robustness. A generative method to solve the robustness issues and other problems by covering synthesis with auxiliary semantics. The results show higher robustness parameters but had some security vulnerability left. Some researchers tried different segmentation methods for increasing robustness. Instance segmentation and Mask R-CNN was tried and which shows greater robustness in the experimental results. A novel approach which is based on modified cycle generative adversarial networks where the results show high robustness and security. We have seen using a two-layer embedding strategy for robust reversible data hiding scheme. The experiment shows that the robustness is improved higher than many other approaches. In looking for solving the robustness and capacity many didn't come up with research for solving both. Then some researches have been done where capacity and robustness both were focused. Some achieved improvements in terms of both capacity and robustness. In another field, A DWT based approach for Image steganography scheme was used and the results show that they improved both robustness and capacity. Then from the QIP area, some used quantum image expansion and Grover search algorithms in their research as well as red-green-blue image steganography, and the experiments show that it can achieve good imperceptibility, security, and large capacity under quantum uncertainty and quantum non-cloning theorems. All these have a high level of complexity which is another problem. If the system complexity is too high then, the usage of the system will be difficult for general people and in emergency cases. So, keeping the system simple and easy to use is a necessary item and the system runtime is also a big issue.

With higher robustness and capacity security of the system are mostly ignore though in steganography the main focus is hiding efficiency and quality yet some research shows that the system gets highly secured as many layers of cryptography and watermarking are added to the framework. These extra layers make the whole framework too much complex and we should not create higher complexity when the main idea is not leading to it and the opposite. There have been many types of research which has higher complexity issues which are very good for security purposes but passively contradict the steganography idea. So, we should try to come up with a system where capacity, robustness, and efficiency will be improved and the framework should not have higher

complexity. But not as simple that anyone can break it without trying to. As the future is quantum computation, we should be aware of that and the framework should handle that, as quantum computers have the ability of parallel computing which can destroy some high-security frameworks in the classical computers in no time. The issue with the researches from the quantum image processing domain is mainly usage and complexity. Though it may not exist in the future when the hardware will be ready that creates uncertainty which we can't accept. Many of the QIP researches included quantum circuits and other high-level algorithms made for quantum computers which can be simulated in the classical computer but that is not the way. So, we should try quantum image processing as it is future proof but in such a way that it can be handled from classical computers even with some quantum circuits here and there. The technology is developing at a high pace so, we should improve the approaches in high efficiency.

2.4 Conclusion

It can be concluded after reviewing all the papers on steganography that, a lot of improvements have been done to steganography techniques for higher payload, message capacity, security, imperceptibility, and efficiency. There are Classical methods along with Quantum steganography techniques where various types were seen. There was audio steganography, video steganography, DNA steganography, and even MS excel cell steganography. Researchers are trying to use steganography idea to the areas which were never imagined before. From simple LSB to high complex Quantum channel methods there are so many types of methods that have been used and could be improved in the future. As the very research area is ever-evolving, the necessity of improvements will be never-ending in the future. Due to high necessity, steganography is becoming popular and evolving vastly. Now the researchers have the responsibility to take it to the next level where people can enjoy an easy simple life of no unauthorized access and data lost due to security vulnerabilities. There could be new possibilities with advanced AI and machine learning algorithms. Deep neural networks are already been used in this technology and we may see further improvements through it. With new technologies combined, we can achieve something that was never imagined before. The bridge between Quantum computing and classical computing where we can use quantum computing techniques without the pressure of actual hardware implementations in the general user side could be one of the breakthroughs in modern technologies. The number of new possibilities is undefined and it is a great motivation that we have to keep improving things forever and as efficiently as possible no matter how much improved the system already is. There is no end to improvements in this world. Improved Steganography will bring true secret communicating ways in the upcoming days and we hope, with new methods and frameworks the quality will be satisfactory.

Chapter 3: Research Methodology

3.1 Introduction

There are so many methods in the steganography area which include various types of communication media. We used the RGB image as the carried data. Our method is based on the Quantum gate for path redistribution and orthogonal base distribution named Fredkin Gate. Our method needs a Canny edge detection algorithm for image segmentation and Quantum key exchange protocol I: BB84 for our full implementation. Many methods have tried to improve the three quality factors of steganography techniques which are payload capacity, imperceptibility, and data security. Capacity means a lot in steganography as we are trying to hide data into data with higher robustness. A cover image should be robust and the framework should enable enough space to hide the data. To match these all three parts in a method, many researchers are trying novel schemes. As they improved one of the quality factors, other qualities were lacking and should be improved. This research is focused on creating a balanced state where all three factors are improved higher. Our method merges quantum gates and protocols to create such balance and used advanced sorting for better efficiency. The experiments show that this method can achieve very high robustness reserving high capacity. The security issue is covered by quantum gates that keep the encrypted secret message in safe positions.

3.2 Proposed Method

Our methodology is based upon the Quantum gate, and Quantum Key Exchange Protocol BB84 [56]. Our main focus is to use these gate and protocol in such a way that we can use in a classical system in the present world and immediately transform it into a Quantum system in the future.

Quantum gate: A Quantum gate is an operator that can act on Qubits. Qubit means a unit of information describing a two-dimensional quantum system.

We shall represent a Qubit with complex numbers as a 2-by-1 matrix:

$$\begin{matrix} 0 \\ 1 \end{matrix} \begin{pmatrix} C_0 \\ C_1 \end{pmatrix}$$

Where $|C_0|^2 + |C_1|^2 = 1$.

We won't go through Quantum systems as it is a very big topic, which can be found in [56].

There are a few quantum gates, such as identity operator I, the Hadamard Gate, the C NOT gate, the NOT gate, the Toffoli gate, Pauli matrices, Fredkin Gate, etc. But we will be using the Fredkin gate in our proposed method, which has three inputs and three outputs. All quantum gates are reversible as A Quantum system is reversible as a whole. The Fredkin gate is its own inverse.

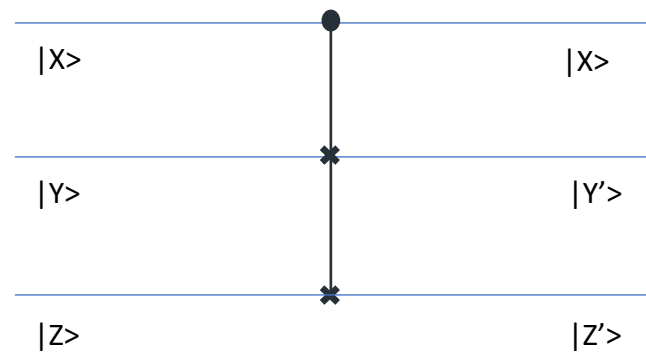


Fig. 1.1: Fredkin Gate Representation

The top $|X\rangle$ input is the control input. The output is always the same as input $|X\rangle$. The main changes happen when the control bit changes. If $|X\rangle$ is set to $|0\rangle$ then $|Y'\rangle = |Y\rangle$ and $|Z'\rangle = |Z\rangle$, i.e., the values stay the same. If, on the contrary, the control bit $|X\rangle$ is set to $|1\rangle$, then the outputs are reversed:

$$|Y'\rangle = |Z\rangle$$

And

$$|Z'\rangle = |Y\rangle.$$

In short,

$$|0, Y, Z\rangle = |0, Y, Z\rangle$$

And

$$|1, Y, Z\rangle = |1, Z, Y\rangle.$$

The Fredkin gate is also universal.

Quantum Key Exchange I: Protocol BB84 – In the 1980s two authors introduces an idea that exploits quantum mechanics. Charles Bennet and Gilles Brassard introduced it in 1984, and hence the name BB84.

In this, protocol two users (sender and receiver) will use orthogonal bases [56], where both of them use two different orthogonal bases which are called “Plus” and “Times” bases.

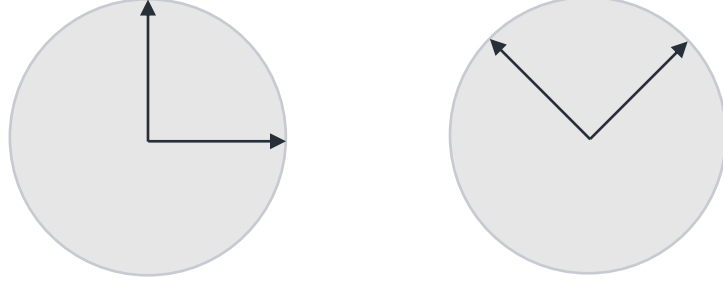


Fig. 1.2: Two bases used for BB84 (“Plus” and “Times” respectively)

Here “Plus” stands for: $+$ = $\{|\rightarrow\rangle, |\uparrow\rangle\} = \{[1, 0]^T, [0, 1]^T\}$

And “Times” stands for: \times = $\{|\nwarrow\rangle, |\nearrow\rangle\} = \{1/\sqrt{2}[-1, 1]^T, 1/\sqrt{2}[1, 1]^T\}$

The sender will use one of the two bases randomly for each classical bit and send the sequence to the receiver through a quantum channel. The receiver will also randomly choose an orthogonal base out of the two and measure it. The output bitstream will not be perfectly matching as the bases are chosen randomly. So, the sender and receiver will share half of their bits in the public channel to check and detect any anomalies. The sender will tell the sequence used, and the receiver will reply as of right or wrong.

With this protocol we can ensure two major solutions:

1: No one can make perfect copies of the sequence because of the no-cloning theorem [56].

2: No one can listen to the stream without traces as the very act of measuring the qubit alters it.

As this protocol is based on the quantum system, we have to make some adjustments to use it in the classical deterministic system.

Proposed Method: At the beginning of our approach, to store the hidden encrypted data into an image, we need to choose the pixels. We tried an image detection algorithm to detect the edge pixels where we can hide the encrypted secret data. Edge pixels are the less noticeable pixels in an image and could be found in a large amount in an image. We used canny edge detection which is superior to others. After getting the edge pixels list, we sort the columns starting with the one which has maximum row values. By such a sorting technique we get the dense areas where we will try to store first. When the pixels are ready to be embedded, we need to start our embedding approach, and we start with quantum entanglement.

The starting of the Fredkin gate needs a control bit. The control bit will decide the other two outputs value. The other output $|Y\rangle$ and $|Z\rangle$ will be the deciding factor whether to embed it to the very next pixel or not and which orthogonal base we will use. Now for using the orthogonal base and sending the sequence through a quantum channel, we need to represent the classical image into a Quantum image. We will use RGB image representation which is based on The Novel Enhanced Quantum Representation (NEQR) [55]. The presentation of a $2n \times 2n$ RGB image can be shown as:

$$|I\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \cdot \sum_{x=0}^{2^n-1} |C_{RGB_{yx}}\rangle \otimes |yx\rangle,$$

Where \otimes represents the tensor product and the state, $|C_{RGB_{yx}}\rangle$ is used to encode the Red, Green, and Blue channels information of the yx pixel.

As we will be working on RGB images, we will be embedding on three LSB values of a selected pixel. In such a way we will get 9 bits per pixel where we will be embedding 1 byte and one bit will be left which will be the control bit of the Fredkin gate. When the Fredkin gate will read the 9th bit it will decide the next pixel and the orthogonal base. But we need a control bit to start with the very 1st pixel from the selected sorted list, where we will decide which base, we will be using. For the starting bit, we will use two entangled qubits in the quantum system. Quantum entangled Qubits does not have any values of their own but respect to each other [56]. Whenever one bit is measured, the other one will collapse and show the measurement instantly. It happens with no time, faster than light. So, these entangled qubits will give us a control value to start the embedding process and the integrity of the image as the measuring of them will trigger the users about anomalies.

The sender will send an entangled qubit to the receiver. When the receiver gets the qubit, he will measure it safely as it cannot be cloned, and measuring it will let the sender know about the breach. When reliever measures it, they will share the measurement in a public channel to know if it's right or not and know where to start the extracting. In the BB84 users had to share actual bits and, in our method, users need to share only the measurement.

The Embedding process:

As the implementation of the Quantum system is not yet possible, we will discuss the classical system implementation with the equivalent classical gate.

Step 1: Read an RGB image (represent it as Quantum RGB image in Quantum system);

Step 2: Apply Canny Edge detection and get Edge values;

Step 3: Apply advance sorting and make a list of selected pixels in descending order;

Step 4: Set Fredkin gate inputs as 0, 1, 0 respectively, and change the 1st one as the senders own random selection and it will be the main key value of the entangled qubits. If the sender uses 0, and the receiver measures the entangled bits as 00, in the public channel, the sender only replies as right and if the receiver measures 11, the sender will reply wrong. The same happens for alternative usage. As it won't happen in the Classical system, the sender will decide the 9th LSB bit value of the 1st pixel as well as the receiver. The Fredkin gate results will decide the orthogonal base and whether to use the next pixel or not in the Quantum system. In the classical system, its second output $|Y'\rangle$ will decide only the next pixel selection. If the output remains the same, the next pixel will be used and if the outputs alter, the very next pixel will be skipped. The operation is:

$$C_{out} = C_{in};$$

$$Out_1 = In_1 (XOR) S;$$

$$Out_2 = In_2 (XOR) S;$$

$$\text{Where } S = (In_1 (XOR) In_2 (AND) C_{in});$$

Here

$C_{out}, C_{in}, Out_1, Out_2, In_1, In_2$ are $|X'\rangle, |X\rangle, |Y'\rangle, |Z'\rangle, |Y\rangle, |Z\rangle$ respectively.

In the Quantum system:

If the $|Z'\rangle = |0\rangle$ then,

the “Plus” orthogonal base will be used.

If $|Z'\rangle = |1\rangle$ then,

the “Times” orthogonal base will be used.

Step 5: Encrypt the secret message binary values with a CNOT gate which is also a reversible and Quantum gate.

Step 6: Get 1st byte from the encrypted message, slice it into 3-3-2 bits tuple.

Step 7: Get binary values of 1st selected edge pixel value.

Step 8: Embed 1st 6 bits into R and G channel's LSB values (6th, 7th, and 8th bits) by Sliced out 1st 6 bits and then embed the last 2 sliced out bits into B channel's 6th and 7th LSB values. The 8th value of the B channel will be the Control bit for the Fredkin gate for next byte embedding.

Follow steps 5 – 8 for each byte from the encrypted message.

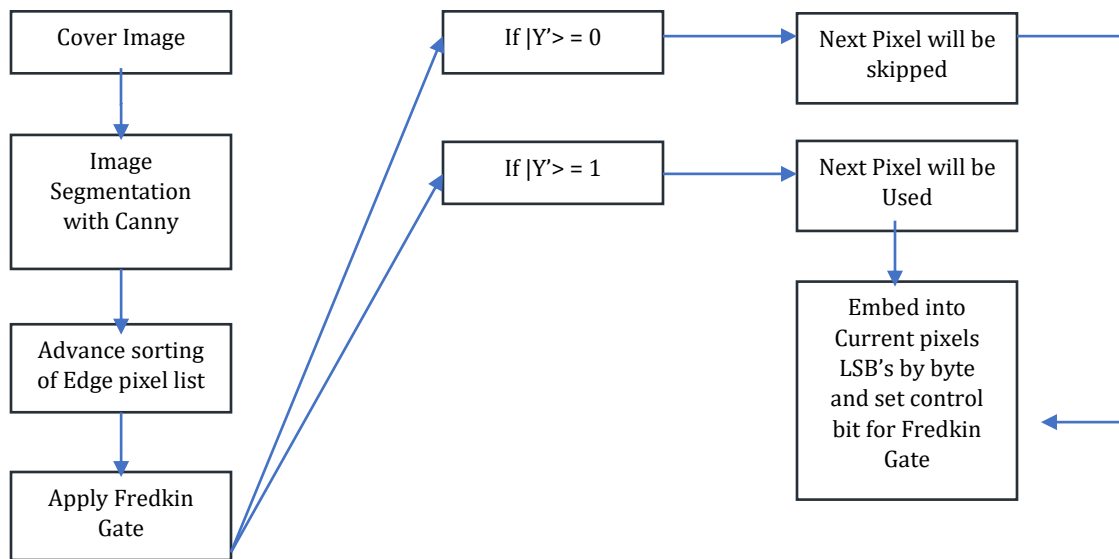


Fig. 1.3: Embedding diagram for the classical system

The Extraction Process:

The extraction process is the reverse process of the embedding procedure.

Step 1: Read the stego image;

Step 2: Apply Canny edge detection and get edge values;

Step 3: Apply advance sorting and makes a list of dense area pixels in descending order;

Step 4: Set Fredkin gate inputs as 0, 1, 0 respectively, and change the 1st one as the senders own random selection and it will be the main key value of the entangled qubits. If the sender uses 0, and the receiver measures the entangled bits as 00, in the public channel, the sender only replies as right and if the receiver measures 11, the sender will reply wrong. The same happens for alternative usage. As it won't happen in the Classical system, the sender will decide the 9th LSB bit value of the 1st pixel as well as the receiver. The Fredkin gate results will decide the orthogonal base and whether to use the next pixel or not in the Quantum system. In the classical system, its second output $|Y'\rangle$ will decide only the next pixel selection. If the output remains the same, the next pixel will be used and if the outputs alter, the very next pixel will be skipped. The operation is:

$$C_{out} = C_{in};$$

$$Out_1 = In_1 (XOR) S;$$

$$Out_2 = In_2 (XOR) S;$$

$$\text{Where } S = (In_1 (XOR) In_2 (AND) C_{in});$$

Here $C_{out}, C_{in}, Out_1, Out_2, In_1, In_2$ are $|X'\rangle, |X\rangle, |Y'\rangle, |Z'\rangle, |Y\rangle, |Z\rangle$ respectively. In the Quantum system if the $|Z'\rangle = |0\rangle$ then the “Plus” orthogonal base will be used. If $|Z'\rangle = |1\rangle$ then, “Times” orthogonal base will be used. This step will follow Quantum key Exchange Protocol I: BB84.

Step 5: Get the encrypted binary values from the RGB channel where, 1st 3 bits will come from the R channel, 2nd 3 bits will come from the G channel and the last 2 bits will come from the B channel for each byte.

Step 6: Decrypt the secret message from the encrypted binary values by using the CNOT gate and converting them to main character values.

Step 7: Last LSB of the B channel will be used for the next iteration step 4-6.

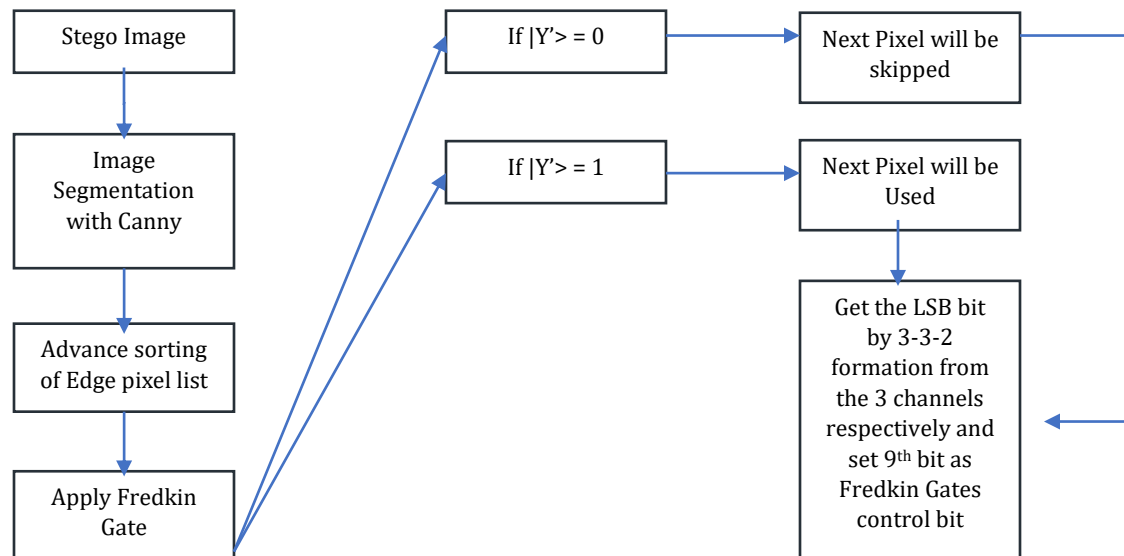


Fig. 1.4: Extracting diagram for the classical system

3.3 Conclusion

Steganography stands out because of less suspicion which leads us to more secure communication where hackers will have to check endless possibilities to know if data is hidden or not as the carriers are innocent. Steganography shines in the classical system with so many methods and approaches in various spaces. People are now upgrading it to use it in the Quantum system as well. We tried to merge the possibilities to create a system that is usable in the present classical system as well as in the Quantum system soon. Our method used Quantum gates and key exchange protocol which motivates us to use it in quantum systems. Even in the classical system, our experiments show that we can achieve a high capacity with great invisibility and robustness. In steganography, the main quality parameter is invisibility which will keep hackers away and hide the main data through the carrier and our method achieved a decent index which ensures the stego image cannot be identified by both human eyes and cyber-attacks. We hope to improve our algorithm with better image segmentation as no methods are complete and undetectable. There are so many methods and all of them have issues in different criteria. We tried to achieve a better balance with our method of the important quality factors and we hope we managed to create a good balance.

Chapter 4: Experimental Research

4.1 Introduction

In this chapter, we will discuss the experimental results and the overall observation of our method. There are many types of steganography techniques. But the most popular is Image steganography where the carrier file is an image file. The main file can be text, image, or other files that can be hidden in the cover image. There other techniques for text-based steganography, audio and video steganography, MS Excel files-based steganography, Quantum steganography, and many more. The main goal here has remained the same that the main secret information should be hidden in another cover public information so that the secret information does not attract attention to itself as an object of security. In this paper, we will focus on Image-based steganography and Quantum steganography as the Images are the most used media in digital communications and has fewer possibilities of getting suspicion. Even it is most popular in the research articles and thus it has been improved many times and more mature areas than others. Quantum steganography is the most advanced technology which ensures promising security in the near future of quantum computing evolution. Our results show that we developed a method that can achieve better qualities while merging the quantum system possibilities into the current classical system which is implantable now and in the quantum system as well.

4.2 Experimental Results

Operating Environment: All the experiments were done in a Linux Manjaro KDE 20.3 64-bit PC equipped with a Core i5 7th generation CPU, 8GB of Ram, and 2GB AMD RX 550 GPU. The programming language used for these experiments is Python 3.8 with its various image processing libraries. For the Quantum gates simulation, we used the IBM quantum experience program. For the datasets, we used multiple datasets for image processing where some of them were already funneled and noisy (CIFAR 10 and CIFAR 100[3]) which helped us to determine the robustness of the method better.

Capacity: Capacity is one of the main quality parameters of any steganography which interprets how much secret message we can embed to the carrier. The capacity always changes as the carrier is different in sizes each time and that is where relative capacity comes in. In relative capacity, we find out, how many bits can be embedded into a pixel. We can express it as:

$$\text{Relative capacity} = \frac{\text{Absolute Capacity}}{\text{Number of Pixel in Image}}$$

In our method, we select an RGB image and when we get the pixel for embedding, we divide it into three-channel which are R, G, and B. In three-channel, we get 1 byte or 8 bits each, where we put 3 bits from the encrypted secret message and we use last channel's last bit as the control bit of the Fredkin gate. So, we get a total of 8 bits embedded into one pixel which means 1 byte per pixel. This amount is currently the highest relative capacity which is similar to some of the previous research.

Table 1-A: Relative capacity through different datasets.

	Datasets	Relative Capacity
1	CIFAR-10 dataset [3]	1 byte per Pixel
2	CIFAR-100 dataset [3]	1 byte per Pixel
3	BOWS2 database [4]	1 byte per Pixel

Table 1-B: Relative capacity comparison with previous research.

Methods	Relative Capacity
Our Method	1 byte per pixel
Generative adversarial Network [12]	1 byte per pixel
Adaptive and separable multiary RDHEI method [9]	0.2 bits per pixel
Image Elliptic Curve and Deep Neural Network [16]	1 byte per pixel
Cycle generative adversarial Network [14]	1.34E-05 byte per pixel
Semantic segmentation [18]	8 bits per frame
Modulus Calculations on Prime Number Algorithm, MOPNA [41]	3.5 bits per pixel
Generative Adversarial Networks, GAN [37]	0.4 bit per pixel
Novel image steganography technique [43]	6 bits per pixel
Adaptive steganography [48]	2 bits per pixel
Hadamard Transformation [49]	2 bits per pixel
LSB (2 LSBq) [52]	2 bits per pixel
Quantum RGB method [55]	2 bits per pixel

Invisibility: The peak-signal-to-noise ratio (PSNR) is one of the most used quantities for comparing the fidelity of a stego image with its original version. We get the value easily from mean square error (MSE), which for two $m \times n$ images I and J is defined as:

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

PSNR is defined as:

$$PSNR = 20 \log_{10} \left(\frac{MAX_1}{\sqrt{MSE}} \right)$$

Where MAX_1 is the maximum pixel value of the image I.

In our method, I and J corresponds to the original image and the stego image respectively.

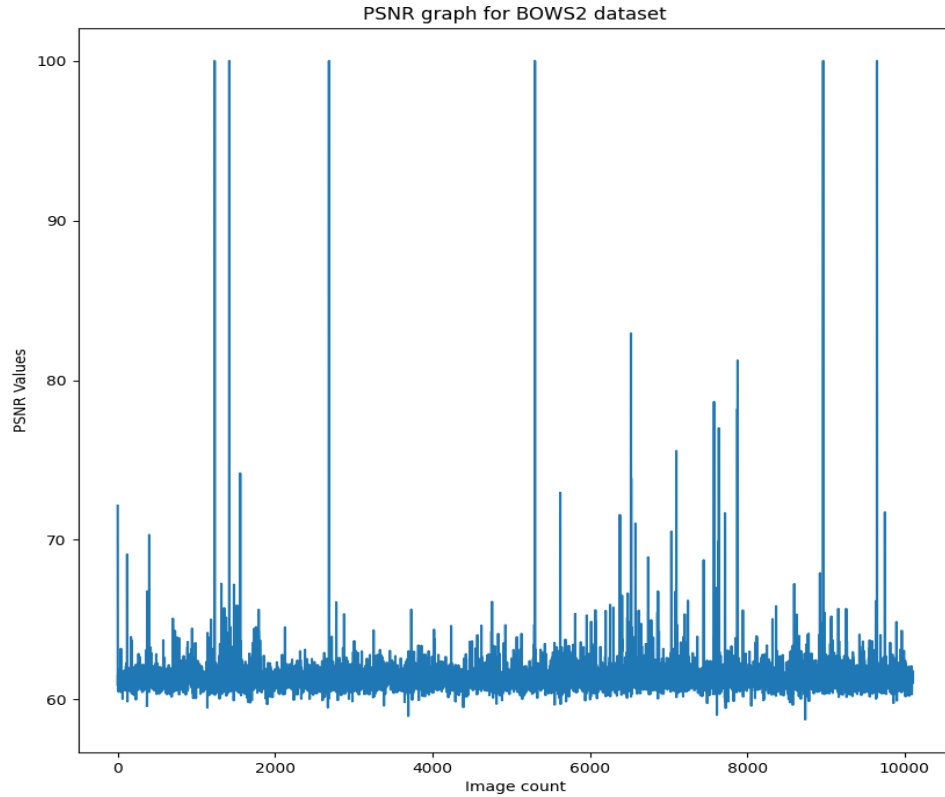


Fig. 2.1: PSNR values of 10100 images

Table 2-A: Average PSNR for in different Datasets each consists of 10 thousand images

	Datasets	Average PSNR
3	CIFAR-10 dataset [3]	46.42906
4	CIFAR-100 dataset [3]	46.50901
5	BOWS2 database [4]	61.4005

Table 2-B: Comparison of PSNR values with previous research

Methods	Average PSNR
Our Method	61.4005
Coding Theory [30]	52.09
LSB (Plain + Block) [15]	51.1411
Chaotic Function and Random map with Fibonacci decomposition [19]	61.14
LSB + MAP Technique [6]	45.8661
adaptive and separable multiary RDHEI method [9]	49.59
Video encryption and video data hiding in HEVC format [10]	37.5068
Image Elliptic Curve and Deep Neural Network [16]	41.7673
Cycle generative adversarial Network [14]	61.033
Instance Segmentation, Mask R-CNN [11]	59
3D magic cube, magic matrix [21]	44
Quantum Image Processing, Arnold's cat map, controlled-NOT gate [34]	47.1785
Dynamic image bit manipulation [35]	62.5081
Prediction Error shift, dual image reversible data hiding [38]	65.28

Unique encoding and decoding dictionary search [31]	32.0908
Modulus Calculations on Prime Number Algorithm, MOPNA [41]	37.93
Generative Adversarial Networks, GAN [37]	38
Chaotic mapping in DCT Domain [29]	39
Two Layer embedding strategy [25]	46
Wavelet [27]	36.67
Novel image steganography technique [43]	44.375
Investigation of steganographic communication approach [44]	36.42
DWT Based Approach [45]	46
Quantum digital image processing consists of quantum image edge detection algorithm and quantum adaptive median filtering algorithm [46]	36.5379
LSQb information hiding algorithm for quantum image [47]	65
Adaptive steganography [48]	51
Hadamard Transformation [49]	73.27
LSQu-Blocks Image Information Concealing Algorithm [50]	67.1
LSB (2 LSBq) [52]	43.16
Hamilton Path (two-fold objective: ECO and HDM) [53]	39.2
Quantum image expansion with Grover search algorithm [54]	39
Quantum RGB method [55]	52.8

We used the BOWS2 dataset [4] as our main as it is made for specifically data encryption and hiding methods. There we will see in Fig 2.1 that, the average PSNR values are around 60 to 63 dB and the lowest is more than 57 dB which a very promising value for the invisibility of the stego image, and this quality is the most significant and signature parameter of steganography methods. We got more than 100 images with 70-85 dB and

some reached 100 dB for soft edges on the images. Overall, the invisibility of our method is good enough to overcome both the human eye and cyber-attacks.

The structural similarity index measure (**SSIM**) is another popular parameter that is used to evaluate image quality, similarity, and integrity. Its value range is -1 to 1 where 1 means the perfect structural similarity and 0 means no similarity at all. It is calculated using different sizes of block windows. It uses the original uncompressed image as the reference to evaluate the target image. It is used in many research experiments in the steganography and image processing domains to evaluate the method efficiency and robustness.

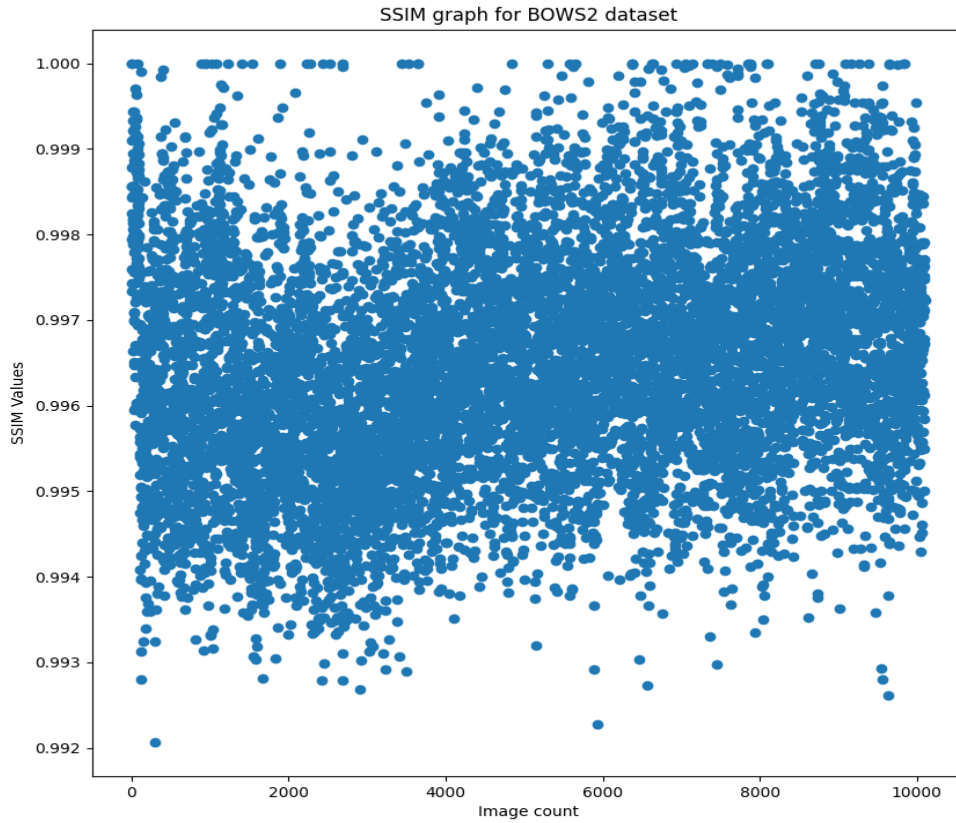


Fig. 2.2: SSIM index of 10100 images

As we see in Fig 2.2, the SSIM index for our method is very promising too. The main average value is around 0.996-0.997 where it goes higher to nearly 1.000 in soft-edged images. The values are most of the time between 0.995 to 0.998. No values were less than 0.992 which is a great result. Some of the values have gone so high like 0.999. But on average the value is 0.9965 which is promising for evaluating structural similarity.

Table 3-A: SSIM index on multiple datasets

	Datasets	Average SSIM
1	CIFAR-10 dataset [3]	0.94228
2	CIFAR-100 dataset [3]	0.9502
3	BOWS2 database [4]	0.9965

Table 3-B: Comparison of the SSIM index with previous research

Methods	Average SSIM
Our Method	0.9965
Chaotic Function and Random map with Fibonacci decomposition [19]	0.99
LSB + MAP Technique [6]	0.99
adaptive and separable multiary RDHEI method [9]	0.99
Video encryption and video data hiding in HEVC format [10]	0.94
Image Elliptic Curve and Deep Neural Network [16]	0.9717
Instance Segmentation, Mask R-CNN [11]	0.99
Semantic segmentation [18]	0.8833
unique encoding and decoding dictionary search [31]	0.915
Generative Adversarial Networks, GAN [37]	0.9
Chaotic mapping in DCT Domain [29]	0.95
Novel image steganography technique [43]	0.94
Adaptive steganography [48]	0.99
Hamilton Path (two-fold objective: ECO and HDM) [53]	0.98

Security: In terms of security with the classical system, we used edge detection algorithms to find edge pixels, and then advance sorting has been applied. To make them more secured we put them through the classical representation of the Fredkin gate which will use a control bit to pick the edges for embedding.

With the Quantum system, the no-cloning theorem [56] applies which will ensure that the data will not be copied in a middle way. About reading it in the network is very difficult due to the use of Entangled Qubits, which will determine 1st control bit value of the Fredkin gate. We have experimented with two Qubits to make them entangled through the IBM Quantum Experience program where we got the result that ran into an original Quantum Computer. Entangled qubits have no value of their own but with respect to each other. If one qubit collapses another one will automatically collapse instantly. This will let us know if anyone is trying to sniff the data in the network.

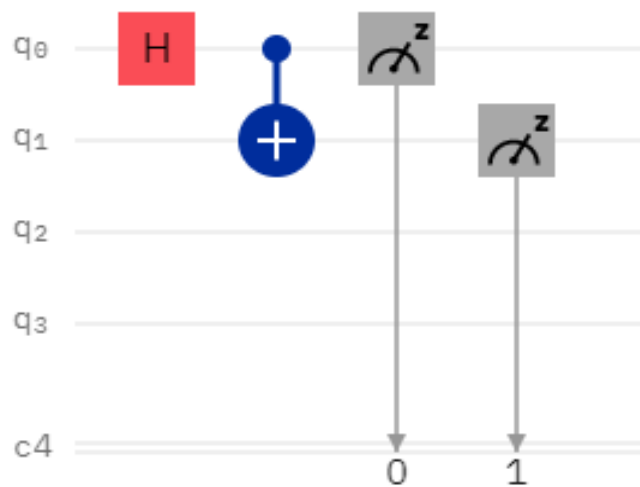


Fig. 2.3: Circuit diagram of Two Qubits entanglement

Figure 2.3 is a quantum circuit built with the IBM quantum experience program. Here we built a quantum entanglement circuit where the “red” block is a “Hadamard” Gate, the “plus” node is the “CNOT” gate, the other two are measurement nodes. The circuit ran into an actual quantum computer in the IBM lab and measured two qubits (Q_0 and Q_1) after the operation, The Hadamard gate makes the 1st qubit in superposition which gets controlled by the 2nd qubit through the CNOT gate and then we get two entangled qubits. Which means, these qubits have no values of their own but with respect to each other. If one of them gets affected, the other one gets the same effect in no time, doesn’t matter how far away they are. These topics are cover in “Quantum Computing for Computer Scientists”. Here, 1st measurement is introduced as 0 and 2nd one is introduced with 1.

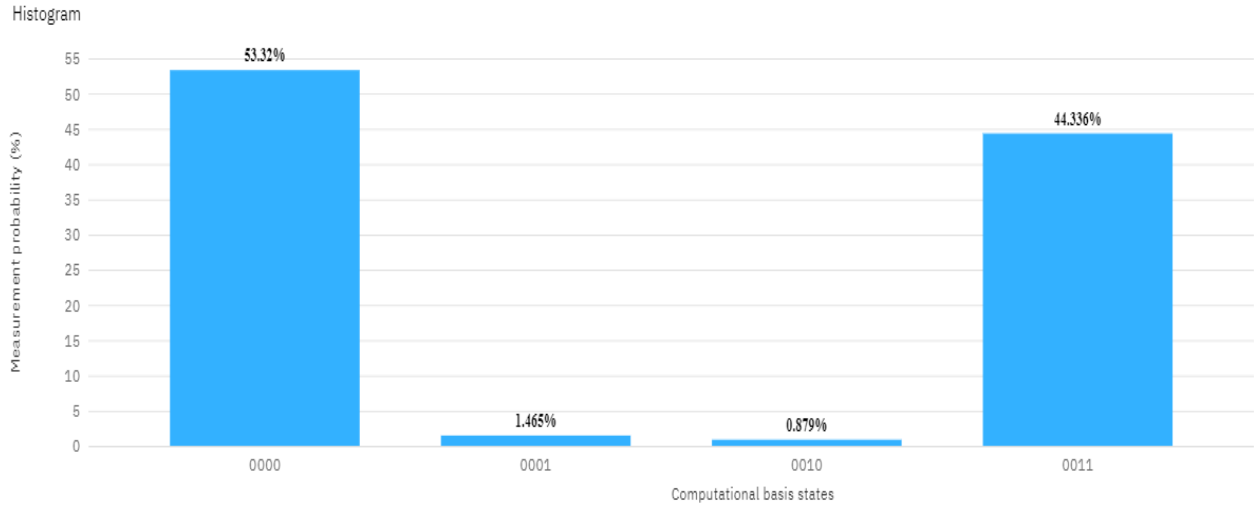


Fig. 2.4: Results of the Entangled Qubits

The circuit which ran into the IBM lab, through the IBM Quantum Experience program, showed the result in this chart. Here we can see that the qubits are entangled successfully. The probability of the same results of those qubits is near to same. The perfect result would be 50% for both 00 and 11, and 0% for both 01 and 10 but, as the quantum computer has a noise in the system, we get some errors in the probability. But this means, if we get 0 from the 1st qubit, we will also get 0 from the 2nd qubit and vice versa. If we measure one qubit, another qubit will also collapse from its superposition. We know that, when in superposition, qubits are not only 0 or 1, they are both at the same time. So, with entanglement, we can tell that whatever value it is, it's the same for them both, if one is giving 0 value, the other will also collapse in 0, if one is giving 1 as the value, the other will intravenously collapse to value 1.

We tested other datasets for noise and size loss understanding such as LFW [1], COCO 2017 [2], and USC-SIPI [5] datasets.

Table 4: SSIM results for datasets with noise and very low size

	Datasets	Average SSIM
1	LFW dataset [1]	0.9579
2	COCO 2017 dataset [2]	0.9079
3	Signal and Image Processing Institute (USC-SIPI) image database [5]	0.9412

Table 5: PSNR results for datasets with noise and very low size

	Datasets	Average PSNR
1	LFW dataset [1]	39.49

2	COCO 2017 dataset [2]	34.1538
3	Signal and Image Processing Institute (USC-SIPI) image database [5]	37.7570

Table 6: Computation time per image on all datasets

	Datasets	Computation Time *per image
1	LFW dataset [1]	.020 sec
2	COCO 2017 dataset [2]	.17 sec
3	CIFAR-10 dataset [3]	.08 sec
4	CIFAR-100 dataset [3]	.08 sec
5	BOWS2 database [4]	.20 sec
6	Signal and Image Processing Institute (USC-SIPI) image database [5]	.16 sec

4.3 Conclusion

The results show that the method has better or equivalent capacity than any other method that is 1 byte per pixel. It means we can embed 1 byte into a targeted pixel, but we will still have one bit left which will be used for Fredkin gate input bit and next pixel decision. We use all 3 channels of a pixel and thus we get 3 times bits from a single pixel. The PSNR value of our method is also decent compared to other methods which are on average 61.4005, that means it is indistinguishable by human eyes and also undetectable from various Steganalysis algorithm where we also have advance sorting algorithm and Fredkin gate to bypass the Steganalysis process on the Stego image. In terms of integrity and structural similarity, the SSIM value is also promising which is on average 0.9965. It means the integrity and structural similarity is high and also better than many other methods. In the IBM quantum experience, we tried the Entanglement circuit which was also successful. The overall experimental results of our method are better than many other methods and promising to our goal where we can merge classical computation with quantum computation for future implementations and get a balanced quality of all 3 key quality factors.

Chapter 5: Conclusion and Future Work

5.1 Introduction

Throughout this chapter, the contribution of the research and the future work of the research will be discussed with concluding the whole research. Steganography is the art of hiding secret data in carrier data to outplay the middle guy who tries various algorithms to crack the encryption of a file when he/she gets suspicious as the file is encrypted. Encryption always creates suspicion about the file and no matter how complex the encryption is, it can be cracked at some point with the right tools. So, steganography tries hiding the important data into a general cover file which won't reveal anything and looks like a normal image. So, the chance of suspicion gets lower and thus the security of the main file is improved. We tried to merge the possibilities to create a system that is usable in the present classical system as well as in the Quantum system soon. Our method used Quantum gates and key exchange protocol which motivates us to use it in quantum systems. Even in the classical system, our experiments show that we can achieve a high capacity with great invisibility and robustness. In steganography, the main quality parameter is invisibility which will keep hackers away and hide the main data through the carrier and our method achieved a decent index which ensures the stego image cannot be identified by both human eyes and cyber-attacks. We hope to improve our algorithm with better image segmentation as no methods are complete and undetectable. There are so many methods and all of them have issues in different criteria. We tried to achieve a better balance with our method of the important quality factors and we hope we managed to create a good balance.

5.2 Contribution of the Research

We tried to use Quantum system advantages in classical form and reserve the instant evolution opportunity for future available quantum systems. The reason behind this is that many of the quantum system-based algorithm and approaches has been shown but we cannot use them in the current systems. So, we decided to use a merged system that will work now and then with reserving the quality parameters. We proposed a method with RGB images, where we proposed RGB quantum representation of the classical image and using image segmentation algorithms with Quantum gate we tried to achieve high capacity, robustness, and security at a balanced rate. We used the Fredkin gate and CNOT gate which are Quantum gates. We tried to use Canny edge detection for image segmentation. The experiments show that this method can achieve very high robustness reserving high capacity. The security issue is covered by quantum gates that keep the

encrypted secret message in safe positions. This may be the first approach to achieve merged classical and Quantum system tools in the same method.

Our research is in the Image steganography domain which is based on Fredkin gate and Improved path distribution with Quantum key exchange protocol. Many types of research can be found on Quantum steganography and QIP but their method is not affordable in current systems, we have to wait for the normalization of quantum computers to apply them in practice. In our research, we used the Quantum gates and protocols in such a way that we can apply them in the current system and future quantum systems as well. Our method has three main parts which are the Quantum gate, Path redistribution, Quantum key exchange protocol. We control the path with image segmentation and then filter them with the dense area. Then we control the distribution with Quantum gate and key exchange protocol. Our experiments included three main quality checks. Capacity, robustness, and security which was validated through PSNR, SSIM index, capacity check. The results show that we have a high capacity than many other methods, decent PSNR value, and SSIM index for robustness assurance, and for security, we used quantum gate and key exchange protocol. This research is one of the first to use quantum system advantages in the classical system and create an opportunity to use the method in quantum system reserving all the quality factors in balanced metric values.

5.3 Future Work

There is always room for improvement in researches like this where we try to improve a technique because there is no end to improvement in this world. Our method focuses on creating balance in the quality factors and improve them all. In the future, we want to try a better image segmentation technique to create better absolute capacity and overall capacity. We also want to try a new key exchange protocol to have a better path redistribution with a more scattered path. We worked only on the RGB images as the medium this time and we want to work on other file types such as CMYK images, Video, GIFs, text, etc. We only used text as the secret data and in the future, we want to use image data to be hidden into another image with better efficiency as that is already possible with some limitations. In the future, we want to add watermarking into our method and also add state of the art cryptographic encryption for high-level security measure. Including all of these will create higher complexity and we want to make the algorithm efficient to reduce the complexity. In terms of quantum system additions, we want to create a fully compatible merged system that can be implemented in the classical system and quantum system at the same time. We want to add quantum entanglement in further steps and we also want to try Quantum teleportation protocols where we can teleport hidden data into another carrier data which will create a spectacular security measure. We want to try new quantum gates into the method for creating better results and path redistribution and orthogonal base determination. We also want to try a new composition of orthogonal bases to see better quality achievements.

5.4 Conclusion

With new technologies combined, we can achieve something that was never imagined before. The bridge between Quantum computing and classical computing where we can use quantum computing techniques without the pressure of actual hardware implementations in the general user side could be one of the breakthroughs in modern technologies. The number of new possibilities is undefined and it is a great motivation that we have to keep improving things forever and as efficiently as possible no matter how much improved the system already is. Our method used Quantum gates and key exchange protocol which motivates us to use it in quantum systems. Even in the classical system, our experiments show that we can achieve a high capacity with great invisibility and robustness. In steganography, the main quality parameter is invisibility which will keep hackers away and hide the main data through the carrier and our method achieved a decent index which ensures the stego image cannot be identified by both human eyes and cyber-attacks. We hope to improve our algorithm with better image segmentation as no methods are complete and undetectable. There are so many methods and all of them have issues in different criteria. We tried to achieve a better balance with our method of the important quality factors and we hope we managed to create a good balance. There is no end to improvements in this world. Improved Steganography will bring true secret communicating ways in the upcoming days and we hope, with new methods and frameworks the quality will be satisfactory.

References

- [1] Gary B. Huang, Manu Ramesh, Tamara Berg, and Erik Learned-Miller. Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments. *University of Massachusetts, Amherst, Technical Report 07-49*, October, 2007.
- [2] COCO - Common Objects in Context, 2020.
- [3] Learning Multiple Layers of Features from Tiny Images, Alex Krizhevsky, 2009.
- [4] Bows2-original data-base (2011) <http://bows2.ec-lille.fr/BOWS2OrigEp3.tgz> , 2020.
- [5] USC-SIPI Image Database, University of Southern California. Available online at, <http://sipi.usc.edu/database> , 2020.
- [6] Alabaichi, A., Al-Dabbas, M., and Salih, A. 2020. Image steganography using least significant bit and secret map techniques. *International Journal of Electrical and Computer Engineering*, 10(1), p.935–946.
- [7] Rachael O., Misra S., Ahuja R., Adewumi A., Ayeni F., Mmaskeliunas R. (2020) Image Steganography and Steganalysis Based on Least Significant Bit (LSB). In: Singh P., Panigrahi B., Suryadevara N., Sharma S., Singh A. (eds) *Proceedings of ICETIT 2019. Lecture Notes in Electrical Engineering*, vol 605. Springer, Cham. https://doi.org/10.1007/978-3-030-30577-2_97
- [8] Zhang, Z., Fu, G., Ni, R., Liu, J., and Yang, X. 2020. A generative method for steganography by cover synthesis with auxiliary semantics. *Tsinghua Science and Technology*, 25(4), p.516–527.
- [9] Yu, M., Liu, Y., Sun, H., Yao, H., and Qiao, T. 2020. Adaptive and separable multiary reversible data hiding in encryption domain. *Eurasip Journal on Image and Video Processing*, 2020(1).
- [10] Guan, B., Xu, D., and Li, Q. 2020. An Efficient Commutative Encryption and Data Hiding Scheme for HEVC Video. *IEEE Access*, 8, p.60232–60245.

- [11] Meng, R., Cui, Q., Zhou, Z., Yuan, C., and Sun, X. 2020. A novel steganography algorithm based on instance segmentation. *Computers, Materials and Continua*, 63(1), p.183–196.
- [12] Duan, X., Li, B., Guo, D., Zhang, Z., and Ma, Y. 2020. A coverless steganography method based on generative adversarial network. *Eurasip Journal on Image and Video Processing*, 2020(1).
- [13] Satir, E., and Isik, H. 2012. A compression-based text steganography method. *Journal of Systems and Software*, 85(10), p.2385–2394.
- [14] Peramandai Govindasamy, Kuppusamy & Ramya, K & Rani, S & Sivaram, M & D, Vigneswaran. (2020). A Novel Approach Based on Modified Cycle Generative Adversarial Networks for Image Steganography. *Scalable Computing: Practice and Experience*. 21. 63-72. 10.12694/scpe.v21i1.1613.
- [15] Jiang, N., Zhao, N., and Wang, L. 2016. LSB Based Quantum Image Steganography Algorithm. *International Journal of Theoretical Physics*, 55(1), p.107–123.
- [16] Duan, X., Guo, D., Liu, N., Li, B., Gou, M., and Qin, C. 2020. A New High Capacity Image Steganography Method Combined with Image Elliptic Curve Cryptography and Deep Neural Network. *IEEE Access*, 8, p.25777–25788.
- [17] Wu, Z., Li, R., and Li, C. 2020. Adaptive speech information hiding method based on K-means. *IEEE Access*, 8, p.23308–23316.
- [18] Pan, N., Qin, J., Tan, Y., Xiang, X., and Hou, G. 2020. A video coverless information hiding algorithm based on semantic segmentation. *Eurasip Journal on Image and Video Processing*, 2020(1).
- [19] Abdulwahed, M. 2020. An effective and secure digital image steganography scheme using two random function and chaotic map. *Journal of Theoretical and Applied Information Technology*, 98(1), p.78–91.
- [20] Na, D. 2020. DNA steganography: hiding undetectable secret messages within the single nucleotide polymorphisms of a genome and detecting mutation-induced errors. *Microbial cell factories*, 19(1), p.128.
- [21] Lee, C., Shen, J., Agrawal, S., Wang, Y., and Lee, Y. 2020. Data Hiding Method Based on 3D Magic Cube. *IEEE Access*, 8, p.39445–39453.

- [22] Sutherland, C., and Brun, T. 2020. Quantum steganography over noiseless channels: Achievability and bounds. *Physical Review A*, 101(5), p.1–9.
- [23] Gupta, S., and Bhushan, B. 2012. Information Hiding Using Least Significant Bit Steganography and Cryptography. *International Journal of Modern Education and Computer Science*, 4(6), p.27–34.
- [24] Li, X., Wang, Y., and Liu, G. 2020. Structured Medical Pathology Data Hiding Information Association Mining Algorithm Based on Optimized Convolutional Neural Network. *IEEE Access*, 8, p.1443–1452.
- [25] Kumar, R., and Jung, K. 2020. Robust reversible data hiding scheme based on two-layer embedding strategy. *Information Sciences*, 512(October), p.96–107.
- [26] Wu, N., Yang, Z., Yang, Y., Li, L., Shang, P., Ma, W., and Liu, Z. 2020. STBS-Stega: Coverless text steganography based on state transition-binary sequence. *International Journal of Distributed Sensor Networks*, 16(3).
- [27] Manuilova, N., Khairullina, L., Khabibullina, G., Minnegalieva, C., Makletsov, S., Bronskaya, V., and Kharitonova, O. 2020. Wavelet method of hiding text information in audio signals. *Journal of Physics: Conference Series*, 1515(3).
- [28] Mustafa, N. 2020. Text hiding in text using invisible character. *International Journal of Electrical and Computer Engineering*, 10(4), p.3550–3557.
- [29] Liu, Z., Chen, H., and Sun, S. 2020. Research on covert communication security based on screen content coding. *IEEE Access*, 8, p.22275–22280.
- [30] Kingsley, K., and Barmawi, A. 2020. Improving data hiding capacity in code-based steganography using multiple embedding. *Journal of Information Hiding and Multimedia Signal Processing*, 11(1), p.14–43.
- [31] Yeh, & Chen, Qiyang & Liu, Zishun & Huang, (2020). High-Payload Data-Hiding Method for AMBTC Decompressed Images. *Entropy*. 22. 145. 10.3390/e22020145.
- [32] Zaynalov, N., Narzullaev, U., Muhamadiev, A., Rahmatullaev, I., and Qilichev, D. 2020. Manipulating the rotation of Ms excel cells to hide information. *International Journal of Advanced Science and Technology*, 29(8 Special Issue), p.2270–2273.
- [33] Li, Z., and Bors, A. 2020. Steganalysis of meshes based on 3D wavelet multiresolution analysis. *Information Sciences*, 522, p.164–179.

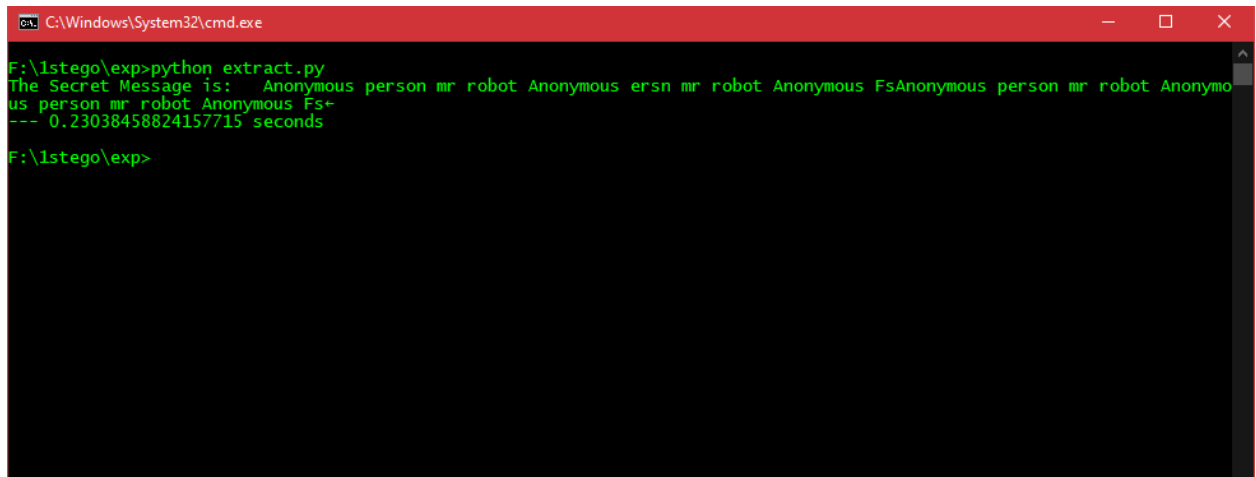
- [34] Abd El-Latif, A., Abd-El-Atty, B., Hossain, M., Rahman, M., Alamri, A., and Gupta, B. 2018. Efficient Quantum Information Hiding for Remote Medical Image Sharing. *IEEE Access*, 6, p.21075–21083.
- [35] Fashiha Hastawan, A., and Septiana, R. 2020. Hiding multiple secret information using dynamic image bit manipulation. *Journal of Physics: Conference Series*, 1444(1).
- [36] Yang, Z., Wei, N., Liu, Q., Huang, Y., and Zhang, Y. 2020. GAN-TStega: Text Steganography Based on Generative Adversarial Networks. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 12022 LNCS(March), p.18–31.
- [37] Liu, J., Ke, Y., Zhang, Z., Lei, Y., Li, J., Zhang, M., and Yang, X. 2020. Recent Advances of Image Steganography with Generative Adversarial Networks. *IEEE Access*, 8, p.60575–60597.
- [38] Yao, H., Mao, F., Tang, Z., and Qin, C. 2020. High-fidelity dual-image reversible data hiding via prediction-error shift. *Signal Processing*, 170(January), p.107447.
- [39] Sidqi, H. 2020. Efficient multi-secret digital images steganography. *Journal of Computer Science*, 16(2), p.249–256.
- [40] Artiemjew, P., and Kislak-Malinowska, A. 2020. Indiscernibility mask key for image steganography. *Computers*, 9(2).
- [41] Zhang, Y., Wang, S., Li, T., Liu, B., and Pan, D. 2020. Modulus Calculations on Prime Number Algorithm for Information Hiding with High Comprehensive Performance. *IEEE Access*, 8, p.85309–85320.
- [42] Naidu, D., Tirpude, S., Kalyani, K., Bongirwar, V., and Sharma, T. 2020. Data hiding using meaningful encryption algorithm to enhance data security. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(2), p.2408–2413.
- [43] Abd El-Latif, Ahmed & Abd-El-Atty, Bassem & Venegas-Andraca, Salvador. (2019). A novel image steganography technique based on quantum substitution boxes. *Optics & Laser Technology*. 116. 92-102. 10.1016/j.optlastec.2019.03.005.
- [44] Eggers, Joachim & Baeuml, Robert & Girod, Bernd. (2002). A Communications Approach to Image Steganography. *Proceedings of SPIE*. 10.1117/12.465284.

- [45] Chen, Po-Yueh & Lin, Hung-Ju. (2006). A DWT Based Approach for Image Steganography. *International Journal of Applied Science and Engineering*. 4.
- [46] Yuan, Suzhen & Mao, Xia & Chen, Lijiang & Xue, Yuli. (2013). Quantum digital image processing algorithms based on quantum measurement. *Optik*. 124. 6386-6390. 10.1016/j.ijleo.2013.05.063.
- [47] Wang, Shen & Sang, Jianzhi & Song, Xianhua & Niu, Xiamu. (2015). Least Significant Qubit (LSQb) Information Hiding Algorithm for Quantum Image. *Measurement*. 73. 10.1016/j.measurement.2015.05.038.
- [48] Kumar, Sanjeev & Singh, Amarpal & Kumar, Manoj. (2018). Information hiding with adaptive steganography based on novel fuzzy edge identification. *Defence Technology*. 15. 10.1016/j.dt.2018.08.003.
- [49] Abd-El-Atty, Bassem & Abd El-Latif, Ahmed & Amin, Mohamed. (2017). New Quantum Image Steganography Scheme with Hadamard Transformation. 10.1007/978-3-319-48308-5_33.
- [50] Alsalmi, Yahya & Lu, Songfeng. (2016). Quantum Image Steganography and Steganalysis Based On LSQu-Blocks Image Information Concealing Algorithm. *International Journal of Theoretical Physics*. 55. 10.1007/s10773-016-3001-3.
- [51] Luo, Jia & Zhou, Ri-Gui & Liu, XingAo & Hu, WenWen & Liu, GuangZhong. (2019). A novel quantum steganography scheme based on ASCII. *International Journal of Quantum Information*. 17. 1950033. 10.1142/S0219749919500333.
- [52] ZHANG, Tie-jun & Abd-El-Atty, Bassem & Amin, Mohamed & Abd El-Latif, Ahmed. (2017). QISLSQb: A Quantum Image Steganography Scheme Based on Least Significant Qubit. *DEStech Transactions on Computer Science and Engineering*. 10.12783/dtcse/mcsse2016/10934.
- [53] Yadav, Gyan & Ojha, Aparajita. (2018). Hamiltonian path-based image steganography scheme with improved imperceptibility and undetectability. *Applied Soft Computing*. 73. 10.1016/j.asoc.2018.08.034.
- [54] Qu, Zhiguo & Li, Zhengyan & Xu, Gang & Wu, Shengyao & Wang, Xiaojun. (2019). Quantum Image Steganography Protocol Based on Quantum Image Expansion and Grover Search Algorithm. *IEEE Access*. 7. 50849-50857. 10.1109/ACCESS.2019.2909906.

- [55] Heidari, Shahrokh & Pourarian, Mohammad Rasoul & Gheibi, Reza & Naseri, Mosayeb & Houshmand, Monireh. (2017). Quantum red–green–blue image steganography. *International Journal of Quantum Information*. 15. 1750039. 10.1142/S0219749917500393.
- [56] Yanofsky, N. S. and Mannucci, M. A. (2008) *Quantum Computing for Computer Scientists*. Cambridge: Cambridge University Press. doi: 10.1017/CBO9780511813887.

Appendix A

Screenshots after Extraction:

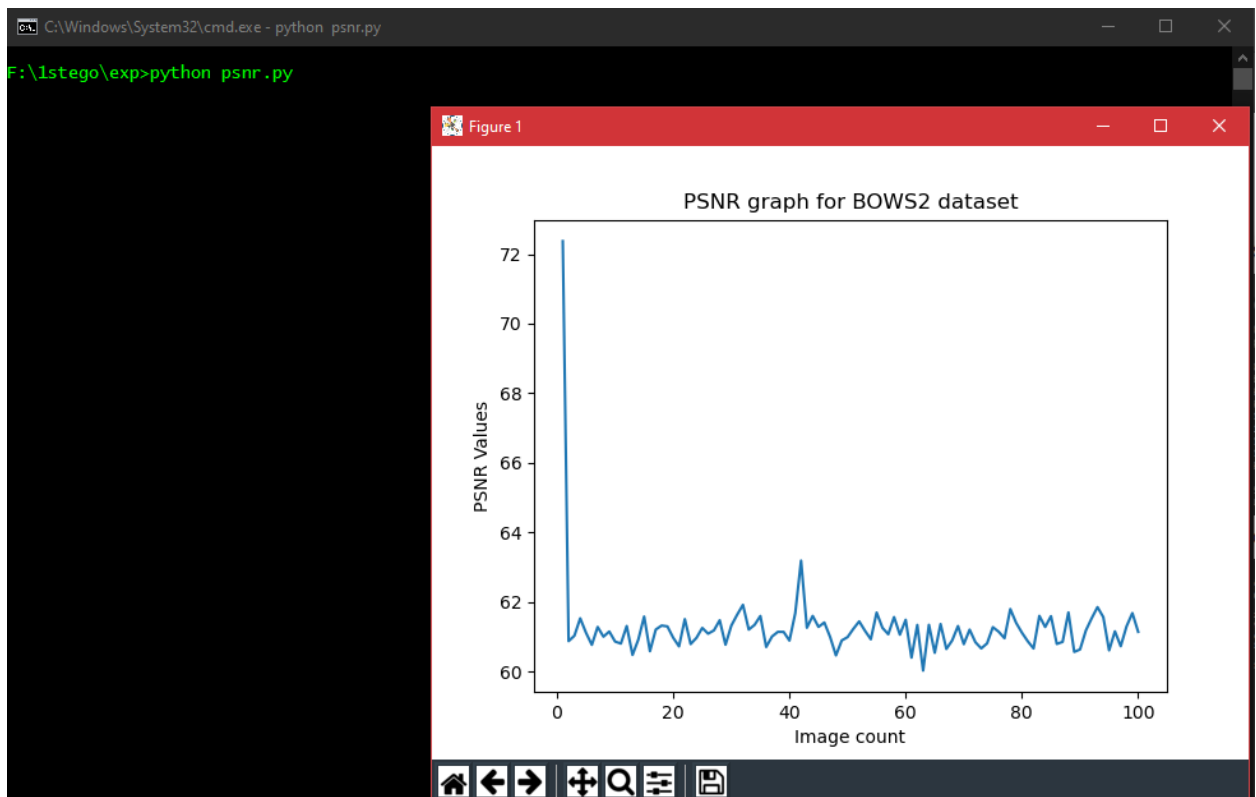


```
C:\Windows\System32\cmd.exe

F:\1stego\exp>python extract.py
The Secret Message is: Anonymous person mr robot Anonymous ersn mr robot Anonymous FsAnonymous person mr robot Anonymo
us person mr robot Anonymous Fs+
--- 0.23038458824157715 seconds

F:\1stego\exp>
```

Screenshots after PSNR Calculation:



Screenshots after SSIM results:



Appendix B

Embedding source code:

```
### the python script for embedding the text
```

```
import cv2
import numpy as np
from matplotlib import pyplot as plt
import operator
from operator import add
from PIL import Image
import time
```

```
start_time = time.time()
ecr = 0
startx = 0
stopx = 8
#fredkin gate operators
cOut = 0
inPx = 1
inPy = 0
outPx = 1
outPy = 0
```

```
def FREDKIN(c):
    cOut = c
    s = XOR(inPx,inPy)
```



```

rs = AND(s,cOut)
outPx = XOR(inPx,rs)
outPy = XOR(inPy,rs)
return 0

```

```

def AND (a,b):
    if a == 1 and b == 1:
        return 1
    else:
        return 0

```

```

def XOR(a,b):
    if a != b:
        return 1
    else:
        return 0

```

#binary conversion

```

def tobits(s):
    result = []
    for c in s:
        bits = bin(ord(c))[2:]
        bits = '00000000'[len(bits):] + bits
        result.extend([int(b) for b in bits])
    return result

```

```

def frombits(bits):
    chars = []
    for b in range(len(bits) / 8):
        byte = bits[b*8:(b+1)*8]
        chars.append(chr(int(''.join([str(bit) for bit in byte]), 2)))
    return ''.join(chars)

```

```

#making equal length binary string
def makeEqLen(a):
    len_a = len(a)
    len_b = 8

    num_zeros = abs(len_a - len_b)
    if (len_a < len_b):
        for i in range(num_zeros):
            a = '0' + a
        return a
    else:
        return a

#secret text
st = "Anonymous person mr robot Anonymous person mr robot Anonymous FsAnonymous person
mr robot Anonymous person mr robot Anonymous Fs"

for i in range(1):
    j=str(i)

    img = cv2.imread('bowsx/image-'+j+'.png',0) #input file reading
    edges = cv2.Canny(img,50,100)
    width = img.shape[0]

    #loading test image
    testImage = Image.open("bowsx/image-"+j+".png") #input file reading
    pixelXY = testImage.load()

    edgedic = {}

```

```

pixValX = []
pixValY = []
finalkeylist = []

addup = 0

pin = 0

#binary secret msg
sms = tobits(st)

sm = []
for sb in sms:
    if(sb == 0):
        sm.append(1)
    elif(sb == 1):
        sm.append(0)

counterBin = len(sm)
loopen = counterBin/8
smx = ''.join(str(sxyz) for sxyz in sm)

#sorting the edge pixels
for xval in range(width):
    edgedic[xval] = np.count_nonzero(edges[xval])

```

```
sorted_d = dict(sorted(edges.items(), key=operator.itemgetter(1), reverse = True))
```

```
keylist = list(sorted_d.keys())
```

```
#creating two list for embedding
```

```
for pixvalfinalx in keylist:
```

```
    midlist = np.transpose(np.nonzero(edges[pixvalfinalx]))
```

```
    finlist= np.ndarray.flatten(midlist)
```

```
    for pixvalfinaly in finlist:
```

```
        pixValX.append(pixvalfinalx)
```

```
        pixValY.append(pixvalfinaly)
```

```
print(len(pixValX))
```

```
ecr += len(pixValX)
```

```
#embedding
```

```
#main loop: iterate secret msg
```

```
for msgbit in range(int(loopleften)):
```

```
    pix = pixelXY[int(pixValY[pin+0]), int(pixValX[pin+0])]
```

```
    if(outPx==1):
```

```
        pixR = makeEqLen(bin(pix[0])[2:])
```

```
        pixG = makeEqLen(bin(pix[1])[2:])
```

```
        pixB = makeEqLen(bin(pix[2])[2:])
```

```
        pixR = pixR[:5]+ smx[startx:startx+3]
```

```
        startx +=3
```

```
        embdR = int(pixR,2)
```

```
        pixG = pixG[:5]+ smx[startx:startx+3]
```

```
        startx+=3
```

```
        embdG = int(pixG,2)
```

```

        pixB = pixB[:5]+ smx[startx:startx+2] + pixB[7:]
        startx+=2
        embdB = int(pixB,2)
        pixelXY[int(pixValY[pin]), int(pixValX[pin])] = tuple([embdR, embdG,
embdB])

        cOutx = pixB[7:]
        FREDKIN(cOutx)
        pin+=1
    elif(outPx==0):
        outPy = 1
        outPy = 0
        pin+=1

#saving stego image
testImage.save('bowsy/image-'+j+'.png', format = 'PNG') #output file reading
print("Success-"+j+"")
print("--- %s seconds" % (time.time() - start_time))

```

Exctraction Code:

```

### the python script for extracting the text

import cv2
import numpy as np
from matplotlib import pyplot as plt
import operator

```

```

from operator import add
from PIL import Image
import time

start_time = time.time()

ecr = 0
startx = 0
stopx = 8
#fredkin gate operators
cOut = 0
inPx = 1
inPy = 0
outPx = 1
outPy = 0
secretmsg = []

def FREDKIN(c):
    cOut = c
    s = XOR(inPx,inPy)
    rs = AND(s,cOut)
    outPx = XOR(inPx,rs)
    outPy = XOR(inPy,rs)
    return 0

def AND (a,b):
    if a == 1 and b == 1:
        return 1
    else:
        return 0

def XOR(a,b):
    if a != b:

```

```

        return 1
    else:
        return 0

```

#making equal length binary string

```

def makeEqLen(a):
    len_a = len(a)
    len_b = 8

    num_zeros = abs(len_a - len_b)
    if (len_a < len_b):
        for i in range(num_zeros):
            a = '0' + a
        return a
    else:
        return a

```

```

for i in range(1):
    j=str(i)

```

```

img = cv2.imread('bowsy/image-'+j+'.png',0) #input file reading
edges = cv2.Canny(img,50,100)
width = img.shape[0]

```

#loading test image

```

testImage = Image.open("bowsy/image-"+j+".png") #input file reading
pixelXY = testImage.load()

```

```
edgedic = {}
```

```
pixValX = []
```

```
pixValY = []
```

```
finalkeylist = []
```

```
addup = 0
```

```
pin = 0
```

```
#sorting the edge pixels
```

```
for xval in range(width):
```

```
    edgedic[xval] = np.count_nonzero(edges[xval])
```

```
sorted_d = dict(sorted(edgedic.items(), key=operator.itemgetter(1), reverse = True))
```

```
keylist = list(sorted_d.keys())
```

```
#creating two list for embedding
```

```
for pixvalfinalx in keylist:
```

```
    midlist = np.transpose(np.nonzero(edges[pixvalfinalx]))
```

```
    finlist= np.ndarray.flatten(midlist)
```

```
    for pixvalfinaly in finlist:
```

```
        pixValX.append(pixvalfinalx)
```



```

        pixValY.append(pixvalfinaly)

    ecr += len(pixValX)

    #main loop: iterate stego Image
    for iterx in range(int(len(pixValX))):
        pix = pixelXY[int(pixValY[pin+0]), int(pixValX[pin+0])]
        if(outPx==1):
            pixR = makeEqLen(bin(pix[0])[2:])
            pixG = makeEqLen(bin(pix[1])[2:])
            pixB = makeEqLen(bin(pix[2])[2:])
            pixRx = pixR[5:]
            secretmsg.append(pixRx)
            pixGx = pixG[5:]
            secretmsg.append(pixGx)
            pixBx = pixB[5:7]
            secretmsg.append(pixBx)
            cOutx = pixB[7:]
            FREDKIN(cOutx)
            pin+=1
        elif(outPx==0):
            outPy = 1
            outPy = 0
            pin+=1

    #saving secret message
    scrt = "".join(secretmsg)

    def Convert(string):
        list1=[]
        list1[:0]=string
        return list1

    scrt = Convert(scrt[:1014])

```

```
ensm = []  
for enx in scrt:  
    if enx == "0":  
        ensm.append("1")  
    elif enx == "1":  
        ensm.append("0")  
ensm = "".join(ensm)  
  
def BinToDec(binary):  
    string = int(binary, 2)  
    return string  
str_data = ''  
for i in range(0, len(ensm), 8):  
    temp_data = ensm[i:i+8]  
    decimal_data = BinToDec(temp_data)  
    str_data = str_data + chr(decimal_data)  
print("The Secret Message is: ", str_data)  
  
print("--- %s seconds" % (time.time() - start_time))
```