Performance Analysis for Secure Quantum Image Transmission Using BB84 Protocol

J. Vijayakumar*, L. Jeganson Durai**
*(Department of Electronics and Instrumentation, Bharathiar University, Coimbatore, Tamilnadu, India
Email: vijayakumar@buc.edu.in)
** (Department of Electronics and Instrumentation, Bharathiar University, Coimbatore, Tamilnadu, India
Email: jegansondurai@gmail.com)

ABSTRACT

Nowadays Quantum mechanical systems promise a secure transmission of information from one to others. But, it is also attacked by many eavesdroppers and the information will be stolen by the third parties. So, the security level of transmission of quantum information is the important one to make the secured system. This research paper provides the performance analysis of the transmission of quantum images by using the QKD-BB84 protocol, which speculation will prove the sharing of the image is secured or notby using the quantum computational properties. Finally, calculation of QBER value between sender and receiver, the measurement of security level and the mismatch frequency are presented by using mathematical descriptions.

Keywords *-BB84 Protocol, Quantum Computation, Quantum Images, X-Ray images*

1. Introduction

In this present time, secret sharing of data is the fundamental one and its protection has been more important in the field of cryptography and secured data communication environment [1, 2]. The transmission of information in the open nature, which makes the data is unguarded by the various eavesdropper's attacks and hence the multimedia contents (Data, Image, Audio, Video, etc.) security has become a crucial requirement. Many approaches are proposed by many researchers, which had been expanded in multimedia data protection for various scopes of cryptography. Quantum computations also induced a great deal since they allow realizing secure transmission of multimedia by using the peculiar properties of quantum theories including the superposition, no cloning and entanglement [3-5].

This paper is also processed to the quantum key distribution protocol in the classical computer which renders the greatest advancement in implementing the complex vectors of quantum image processing algorithm. So, the accuracy of QKD protocol [6, 7] is the only responsible factor for the secure image transmission and its security level measurement is the essential one. In this paper, the performance of quantum image transmission using BB84 protocol [8] will be analyzed by using various techniques.

QKD processes are simulated in the classical computer with Intel (R) Core (TM) i3-2330M CPU@ 2.20 GHz, 64 bit Operating system, 3GB RAM equipped with the MATLAB R2017a environment and Quantum Information Toolkit [9] which provides the Bra-Ket notations and quantum communication tools for state vector representations, qubit value representation and QKD process.

2. Proposed Method

In this research paper, the X-rayimages (For Knee, Teeth and Liver) and Scanned images (For Brain and Eye) of human organs are collected from hospitals and medical cares.

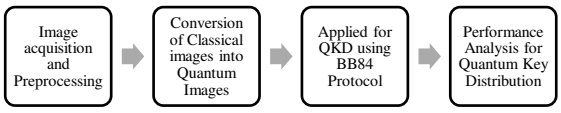


Figure.1: Block diagram for the working process of Quantum Image Transmission

The working process of Quantum Image Transmission is shown in Fig.1. The human organ images are collected in the.JPEG file. The collected images are applied to the processing techniques to improve the quality of the image. After, the preprocessing step, the image will be given as the input for Quantum Key Distribution (QKD) Process. The QKD works only for the processing of qubits, not for classical bits, so the bits to qubits conversions are done using Bloch sphere theory. The image is derived in the form of quantum vectors [10, 11], which follows

$$|I\rangle = \frac{1}{\sqrt{2^n}} \sum_{s=0}^{N-1} |A_s\rangle \otimes |s\rangle \qquad (1)$$

Where $N=2^n$ denotes the number of Qubits

$|I\rangle$ – Illustration of Input Image

$|A_s\rangle$ – Color value in s^{th} sample point

$|s\rangle$ – Position of samples (s=0, 1... N-1)

$\otimes$ - Kronecker Product

Quantum Key Distribution is the fundamental concept which relied on Superposition and No cloning theorem, which makes more secure communication than classical manner. But, QKD protocols [12, 13] are only used for key distribution, not for the data transmission. Alice (Sender) and Bob (Receiver) choose the keys erratically, so the secret key is random and neither Alice nor Bob can decide the key results. There are many types of QKD protocols for several uses like secure data transmission, entanglement, coherence, etc. In this research paper, BB84 protocol [14, 15] is used to key distribution process and its performance will be analyzed. The level of security will be verified which knows how the keys are shared without eavesdropping. The following methods are used to analyzing the performance of quantum image transmission.

2.1 Measuring Error Bits

Quantum bit error rate (QBER) is the measurement of error bits in the receiving ends Bob and Eve, which compare to the Alice bits, which is also characterizing the QKD systems and its functioning to give the secure signal transmission. From Eqn.1, QBER is the ratio between of the number of error bits to the total bits sent by Alice. Or other words, whose error bits are very low, then QBER rate also will be low for those receivers (Bob or Eve).

$$\text{QBER} = \frac{No.\,of\ bits\ in\ error}{Total\ detected\ bits} \qquad (2)$$

2.2 Measuring Security Level

The estimation of QBER is very important for the protection of the quantum computation system but not to find the security level. So we calculate the uncovered bits of data transmission and mismatch frequency to know the security level. If we uncover all bits to know that nobody has eavesdropped. Otherwise, there was a minimum knowledge about security. Assume T is the probability of uncovered bits and U is the number of uncovered bits during key distribution i.e. When U increases than T (U) is also increasing. The function T (U) can be defined in log function. Therefore the function T (U) should be lie between 0 and 1 i.e. range is between 0-100 %.

$$\text{T (U)} = \log_e \frac{U}{N} \qquad (3)$$

2.3 Measuring Mismatch Frequency

And also the mismatch frequency is calculated as follows

$$\text{MF} = \sum_{n=0}^{N-1} \frac{\text{XOR}_\text{n}(\text{Key A, Key B})}{\text{m}} \qquad (4)$$

Where Key A – Sender's Key (Alice),

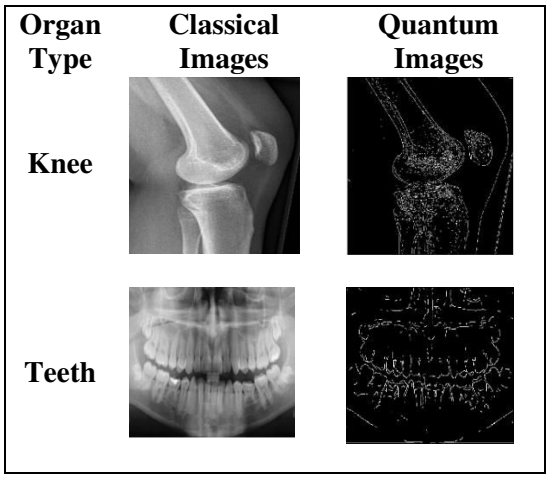
Key B – Receiver's Key (Bob or Eve)

m - Length of Key A n - n^{th} Bit value upto N-1 values

3. Results

In this research paper, the simulation-based experiments are done for the database of five different X-ray and Scanned images of human being organs (Knee, Teeth, Liver, Brain and Eye). The execution of the quantum image representation equation Eqn.1 on the bit values of the original image to get its qubit form, which is complex value.

The classical and quantum illustrations of images follow in Fig.2, which classified that the classical and quantum representations of digital images. In Fig.2, the classical images are based on color values and its position. And the quantum images are based on α-Qubit value (α|000>) and state vector value. From these simulations, the classical image is saved as ann-Qubit system in the classical computer.



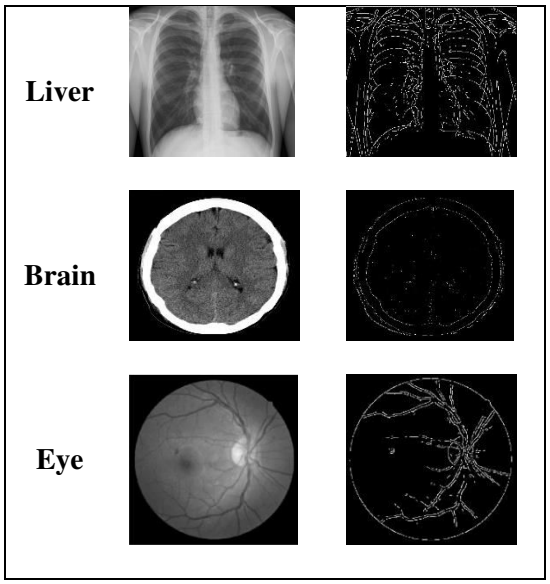


Figure.2: Classical vs Quantum representations of Input Images

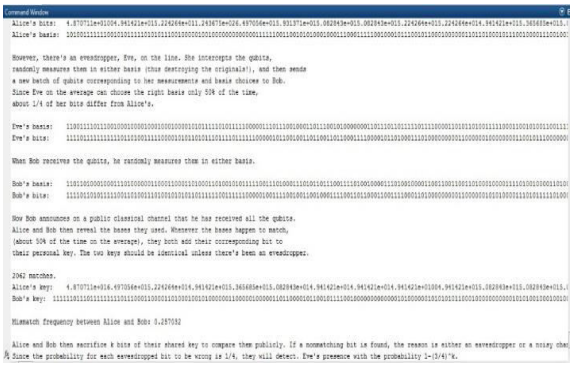


Figure.3: The example key generation for Human Eye image.

The key generation of human eye image as shown in Fig.3. The keys are generated for the input image of the human eye and also eavesdropper is present. The security levels are calculated for the all image transmissions.

4. Performance Analysis

From the results, the quantum images are transmitted to Bob from Alice, but the powerful eavesdroppers are may be presented. By the performance of QKD protocol, the shared qubits will be analyzed between Alice to Bob and Eve. The following methods are used to analyze the performance of BB84 protocol, by using existing equations.

4.1 Quantum Bit Error Rate

In the quantum key distribution process, total bits are 4096 and the error bits for the Bob's and Eve's keys are tabulated as follows in Table.1.

Table.1 Number of Error Bits for Bob and Eve

Organ Type	Number of Error bits of Bob	Number of Error bits for Eve
Knee	918	4017
Teeth	927	3014
Liver	942	3006
Brain	972	3015
Eye	876	2891

From the Table.1, the number of error bits of eve is greater than Bob's bits. And also from the Fig. 4, the evaluation of the QBER, relying upon our experimental characterization results is used to characterize the quality of signal transmission in (QKD) systems.

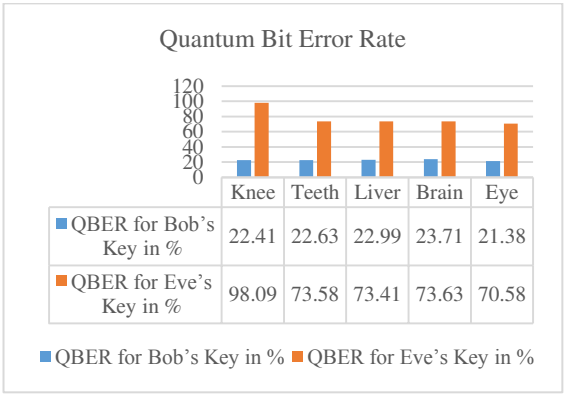


Figure 4: QBER for Bob and Eve

For the image of the human eye, the qubit information is transmitted from Alice to Bob, the error bits of Bob is 918 and the error bits of Eve is 2890. When applying in Equation (2), the QBER values are found, which are 21.38% for Bob's error bits and 70.58% for Eve's error bits. By the comparison, Eve's QBER values are higher than Bob's QBER values. Hence the results prove the secure communication between Sender (Alice) and Receiver (Bob)in the presence of Eavesdropper.

4.2 Level of Security

The level of security in quantum key distribution using BB84 protocol system is shown in Fig.5.The security of Quantum Key Distribution using BB84 protocol system depends on the number of uncovered bits (U) and the probability of Uncovered bits T (U).

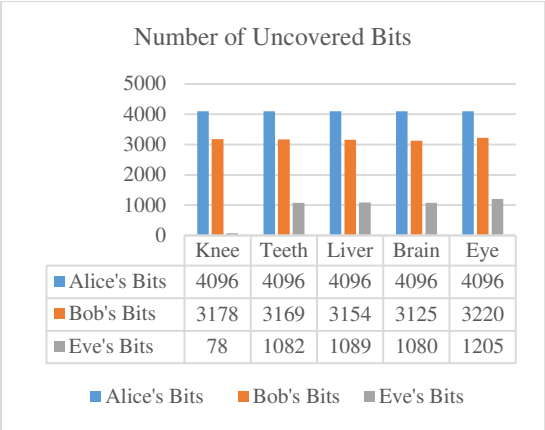


Figure 5: Level of Security in Quantum Key Distribution using BB84 Protocol

The total number of uncovered bits of Alice is 4096. For the image of Knee, the qubit information is transmitted from Alice to Bob in the presence of Eve, the number of uncovered bits for Bob is 3178 and for Eve is only 78. The number of uncovered bits is for Bob is very near to Alice and greater than Eve. So the security level of quantum key distribution is very high against the eavesdropper's attack.

4.3 Mismatch Frequency

The mismatch frequency between Alice's key and Bob key will be very low than 0.5 in the simulation result, to be correct. And the mismatch frequency between Alice to Eve and Bob which describes the mismatch frequency between Eve and Bob with Alice, Bob's values are very low mismatch frequency. This gives the results as Bob's keys are very near to Alice's keys when compare to Eve's keys.

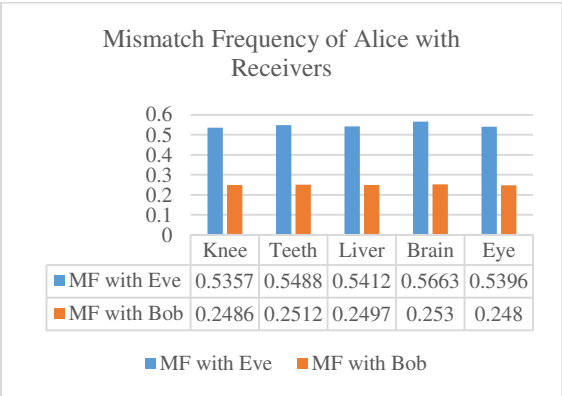


Figure 6: Mismatch Frequency for Eve and Bob with Alice

The Eve's keys have the mismatch frequencies which are greater than 0.5 which are demonstrated in the Fig-6. For the brain image, the mismatch frequency value for Alice with Bob is 0.248 and for Alice with Eve is 0.5396. These results show Eve's bits are mismatched with Alice than Bob's Bits. Finally, the performance of the quantum key distribution system is analyzed by using QBER estimation process, the security measurement and mismatch frequency between sender and receivers will be measured by the proposed equations to prove the maximum protection of Quantum Images.

5. Conclusion

The BB84 protocol for the quantum image transmission is simulated and it is secured against the most arbitrarily powerful eavesdroppers. Simulation results show that the images are stored as the qubit systems, which can be reliably recognized and recovered on realistic quantum computers. Finally, from the results, the quantum image transmission through BB84 protocol is much secured and those performances are analyzed. In future, other QKD protocols should be simulated to reduce the limitations of this system which make even more security by using the weird quantum mechanics properties.

6. Acknowledgement

This research is supported by Promotion of University Research and Scientific Excellence (PURSE) - Phase II, Department of Science and Technology (DST), Bharathiar University, Coimbatore, Tamilnadu. Award Letter No.: BU/DST PURSE (II)/ APPOINTMENT/ 9

REFERENCES

[1] Zhou Nan-Run, Zeng Gui-Hua, "*A Realizable Quantum Encryption algorithm for Qubits*", Chinese Physics, Vol.14 No 11, November 2005, 1009-1963/2005/14(11)/2164-06

[2] M. Shalaby "*Two-way and one-way quantum cryptography protocols*" Optik 123 (2012) 1852–1857

[3] Dan C.Marinescu, M.Marinescu, "*Approaching Quantum Computing*" Copyright 2008 by Pearson Education, Inc. ISBN 978-81-317-2233-6

[4] Grover, L: "*A fast quantum mechanical algorithm for database search*". In: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, pp. 212-219(1996)

[5] Carlo A. Trugenberger, "*Quantum Pattern Recognition*", Quantum Information Processing, Vol. 1, No. 6.

[6] Omer K. Jasima , Safia Abbasb, El-Sayed M. El-Horbatyb and Abdel-Badeeh M. Salem "*Quantum Key Distribution: Simulation and*

Characterizations" (ICCMIT 2015), Procedia Computer Science 65 (2015) 701 – 710

[7] Ergün Gümüş , G.Zeynep Aydin, M.Ali Aydin "*Quantum Cryptography and Comparison of Quantum Key Distribution Protocols*" Journal of Electrical & Electronics Engineering, Year: 2008(503-510), Volume: 8, Number:1

[8] Peter W. Shor and John Preskill "*Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*" Physical Review Letters, Volume 85, Number 2

[9] Quantum Information Toolkit, Version: 0.10.0 (beta), released 2014-03-29 download from the web address: http://qit.sourceforge.net

[10] Phuc Q. Le, Fangyan Dong, Kaoru Hirota, "*A flexible representation of quantum images for polynomial preparation, image compression and processing operations*", Quantum Inf Process (2011) 10:63–84, DOI 10.1007/s11128-010-0177-y

[11] Fei Yan, Salvador E. Venegas-Andraca Abdullah M.,*"A survey of quantum image representations",* Quantum Inf Process (2016) 15:1–35 DOI 10.1007/s11128-015-1195-6

[12] Hitesh Singh , D.L. Gupta , A.K Sing "*Quantum Key Distribution Protocols: A Review*" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014), PP 01-09

[13] Michael A.Nelson, Issac L.Chuang, "*Quantum computation and quantum information*" Cambridge university press, ISBN 978-1-107-00217-3.

[14] Rahul Aggarwal, Heeren Sharma, Deepak Gupta, "*Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol*", International Journal of Computer Applications (0975 – 8887) Volume 20– No.8, April 2011

[15] Mohamed Elboukhari, Mostafa Azizi and Abdelmalek Azizi, "*Analysis of the security of BB84 by Model Checking*", International Journal of Network Security & its Applications (IJNSA), Volume 2, Number 2, April 2010, ISSN Number : 0974 – 9330

[16] Hui Qiao, Xiao-yu Chen, "*Simulation of BB84 Quantum Key Distribution in depolarizing channel*" Proceedings of 14th Youth Conference on Communication, ISBN: 978-1-935068-01-3 Pub. Date: October 2009 Scientific Research Publishing, USA

[17] Vishal Sahni, "*Quantum Computing*" Tata McGraw-Hill Publishing Company Limited, ISBN 978-0-07-065700-7

[18] Yu-Guang Yang, Ju Tian, Si-Jia Sun, Peng Xu, "*Quantum-assisted encryption for digital audio signals*", Optik 126 (2015) 3221–3226