Classical and Quantum Cryptography for Image Encryption & Decryption

Harshad R. Pawar
Computer Engineering
PRMCEAM
Badnera, India
harshad09pawar@gmail.com

Dr. Dinesh G. Harkut
Computer Engineering
PRMCEAM
Badnera, India
d_harkut@rediffmail.com

***Abstract*—Now a days, where all well aware about the internet and other means of sharing of multimedia information between two parties which happens in public environment, so it is important to maintain the security of these kind of personal data which is stored at computers, on cloud or in the personal storage. There are many techniques which are used to provide authenticity, confidentiality, secrecy, and integrity to the data one of them is the Cryptography. In this paper, we survey and compare the existing work and concepts of Classical (Modern) Cryptography (CC) and Quantum Cryptography(QC) used for image encryption and decryption. Each encryption and decryption techniques have their strengths and weakness. In this paper, we focus on the selecting the best cryptography technique to be used for image encryption and decryption so that researchers can get idea about the selection of efficient cryptography technique.**

***Keywords*— Classical Cryptography, Quantum Cryptography, Quantum Key Distribution, Image Processing, Qubit.**

I. INTRODUCTION

It is said that “One picture is worth more than thousand words” as it can provide clear and more pictorial information than the information collected from the description for human interpretation. So, this results in the requirement of the proper image data representation, store, and transmission. Nowadays, the security of information is more important in data storage and transmission. As images can carry much more data, they are used in various processes. Digital images are used in various fields like medical, military, in private businesses therefore the protection of these contains is very important and that’s why image encryption and decryption techniques play important role in image data security.

Cryptography is the technique which is used for doing secure communication between two parties in the public environment where unauthorized users and malicious attackers are present. In cryptography there are two processes i.e. encryption and decryption performed at sender and receiver end respectively. Encryption is the processes where a simple multimedia data is combined with some additional data (known as key) and converted into un-readable encoded format known as “Cipher”. Decryption is the reverse method as that of encryption where the same or different additional data (key) is used to decode the cipher and it is converted in to the real multimedia data [9]. There is one more term cryptanalysis, it is the processes which can be used by intruder to analyze and break down the secure communication between two parties [10].

Cryptography techniques can be categorized according to their basic principles or protocols they follow. But here in this survey we are going to concentrate on the two types of cryptography technique: Classical Cryptography and Quantum Cryptography

Classical cryptography is based on the mathematics and it relies on the computational difficulty of factorizing large number. The security of classical cryptosystem is based on the high complexity of the mathematical problem for the instance factorization of large number. And classical cryptosystem is further divided into two types: Symmetric System and Asymmetric System

Whereas the Quantum Cryptography is based on physics and it relies on the laws of quantum mechanics. It is arising technology which emphasizes the phenomena of quantum physics in which two parties can have secure communication based on the invariabilities of the laws of the quantum mechanics. Quantum mechanics is the mathematical framework or set of rules for the construction of physical theories. Two important elements of quantum mechanics on which quantum cryptography depends: Heisenberg Uncertainty Principle (HUP) and Photon Polarization Principle

II. METHODOLOGY

Different types of data have their own unique features; therefore, each of them required different type of cryptographic techniques. There are so many algorithms available which are suitable for textual type of data but it may be happen that these algorithms are not suitable for multimedia type of data like image, video etc.

Here we are performing comparison between the classical cryptography and quantum qryptography

A. Classical Cryptography and its techniques

In the classical Cryptography the original data i.e., the plain text is transformed into the encoded format i.e. cipher text so that we can transmit this data through unsecure communication channels. A data string which known as “Key” is used to control the transformation of the data from plain text to cipher text. This arrangement helps to keep data safe as it

978-1-5386-2599-6/18/$31.00 ©2018 IEEE

required the key for extracting the original information from the cipher text. Without the key no one can read the data. In this technique it is assumed that the only authorized receiver has the key.

This cryptography has two types of techniques [2]:

- Symmetric Cryptography: In the symmetric cryptography a single key is used for encrypting and decryption the data. This encryption key is private key. This is the limitation of this encryption technique that this private key must be distributed only among the authorized sender and receiver.
- Asymmetric Cryptography: In the Asymmetric cryptography a pair of key i.e. public key and private key is used for encryption and decryption. A Sender can use its public key to encrypt the data and on receiver end receiver can decrypt the data by using its private key. This technique overcomes the problem of key distribution.

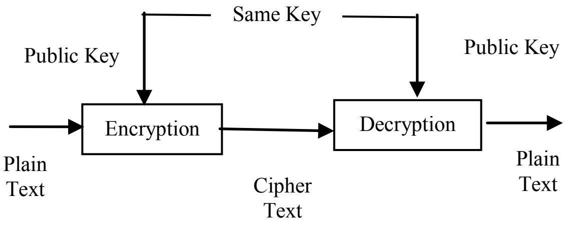

Fig. 1. Symmetric Cryptography

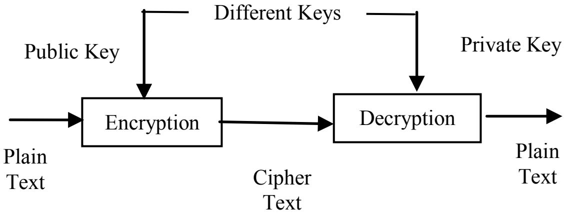

Fig. 2. Asymmetric Cryptography

B. Quantum Cryptography and Quantum Key Distribution:

Quantum Cryptography: It gives us the most secure way to transfer the data as it is based on the principals of quantum physics in which two parties can have secured communication based on invulnerabilities of the laws of quantum mechanics. Quantum mechanics is the mathematical framework or set of rules used for the construction of physical theories. The two important elements of quantum cryptography on which quantum cryptography depends are: Heisenberg Uncertainty Principle and Photon Polarization Principle.

- Heisenberg Uncertainty Principle: This principle says that if you measure one thing, you cannot measure another thing accurately. For example, if you apply this principle to human, you could measure a person's height, but you can't measure his weight. The only odd thing about this principle is that it becomes true only for the instant at which you try to measure something. This principle is applied to the photons. Photons have wave like structure and are polarized or tilted in certain direction. While measuring photon polarization, all subsequent measurements are get affected by the choice of measures that we made for polarization. This principle plays the vital role to prevent the efforts of attacker in quantum cryptography [1].
- Photon Polarization Principle: this principle refers that, an eavesdropper cannot copy the unique "qubits" (quantum bit) i.e. unknown quantum state, due to the no-cloning principle. If an attempt is made for measuring any properties, it will disturb the other information.
- Quantum Key Distribution (QKD): There are some flows in classical cryptography while distributing the key which are overcome by the Quantum Key Distribution Approach in quantum Cryptography. QKD is used for generating secret key which is shared between both parties using both channels. QKD uses two channels. First, quantum Channel which is used for transmit single photon transparent path it can be made of optical fiber or space. Second is classic channel which is used to transfer encoded data, it can be a telephone or internet line. [2]- [3].
- QKD is based on following Protocols. The BB84 Protocol: In 1984, Charles H. Bennett and Gilles Brassard developed the first key distribution protocol known as "BB84". It was based on Heisenberg Uncertainty Principle [4].

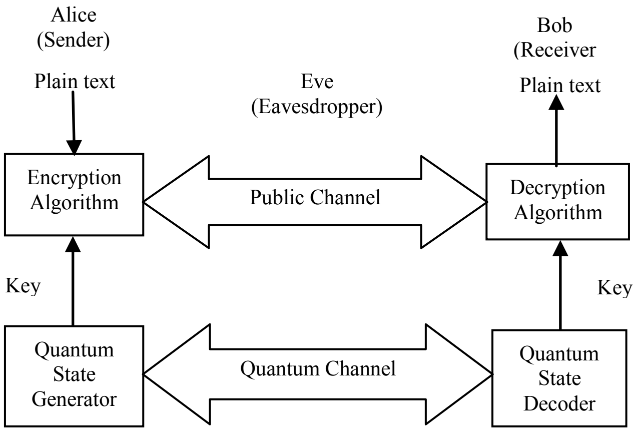

Fig. 3. A Quantum Cryptographic Communication

The Quantum Key Distribution sequence of operations is done as follows:

First, a sequence of photons that polarized randomly (0°, 45°, 90°, and 135°) is generated by Alice and then forwarded to the Bob. After receiving the photons Bob chooses randomly whether to measure its diagonal or rectilinear polarization for each photon. Next Bob publically announced about the choice he has made for measuring the polarization (Rectilinear or Diagonal) but not the measurement result of each photon. After that Alice tells Bob openly about whether he has made correct type of measurement for each photon or not. Finally, Alice and Bob discard all the cases in which Bob has made incorrect measurements or the cases in which the detectors are failed to record photons [6].

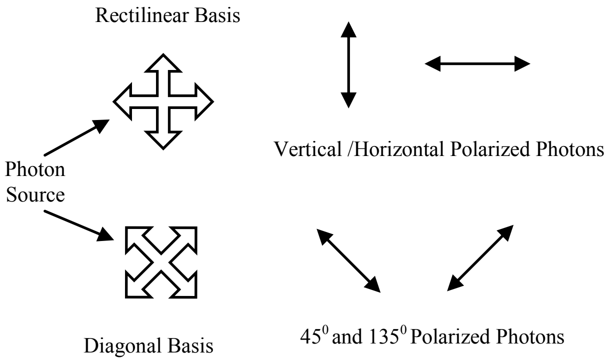
Rectilinear Basis
Photon Source
Vertical /Horizontal Polarized Photons
Diagonal Basis
45^0 and 135^0 Polarized Photons

Fig. 4. Rectilinear and Diagonal Polarization Base [1]

There are some variants of BB84 Protocol like Two-state Protocol B92, KMB09 Protocol, Eckert's Protocols, COW Protocol, and SARG04 Protocol [4]-[1].

III. CLASSICAL BITS AND QUANTUM QUBITS

In the classical cryptography works on "Bits" i.e. the information is represented by using "0" and "1". Whereas Quantum Cryptography works on the Quantum Bits also known as "Qubits". Qubit is the two-state mechanical system, such as the polarization of the photon. We can say that the qubit can be in the superposition of "0" and "1" but here the two states vertical polarization and horizontal polarization. In classical cryptography, Bits would have to be either "0" or "1" but according to the fundamental property of quantum computing, quantum mechanics allows qubit to be in the superposition of both the states at the same time that's why they cannot be copied [5]-[7].

Representation of qubit [5]-[7]

Before moving towards the qubit representation, we must have to understand the special way of vector representation known as "Bra-Ket". Let "V" be the vector in two dimensional spaces such as

$$|V >\in C^2 \tag{1}$$

The Ket of this vector is:

$$|V \geq= \begin{pmatrix}1\\0\end{pmatrix} \tag{2}$$

The Bra of this vector is triangle transpose, T denotes the transpose.

$$|v \geq= ((|0 >)^*)^T = \begin{pmatrix}1^*\\0^*\end{pmatrix} \tag{3}$$

Here, * denotes entry wise conjugate, and thus "Ket" denoted |·> is the d-dimensional column vector and the "Bra" denoted <·| is d-dimensional row vector.

Now the state of qubit can be represented as a two dimensional "Ket" vector

$$|\Psi >\in C^2 \tag{4}$$

Therefore,

$$|\Psi >= \alpha|0 > +\beta|1 > \tag{5}$$

Where α and β ∈ C are the amplitudes and $|\alpha|^2 + |\beta|^2 = 1$

TABLE II REPRESENTATION OF CLASSICAL BITS AND QUANTUM BITS (QUBITS) [5]

Classical Bits	Quantum Bits (Qubits)
00	α 00
01	β 01
10	µ 10
11	€ 11

IV. CLASSICAL AND QUANTUM ONE TIME PAD (OTP)

The electrical One-Time Pad for telegraph encryption was invented by Gilbert Verman in 1917 [5].

In classical cryptography, one time pad provides perfect secrecy i.e. if we don't know about the key which is used for encrypting the plain text then from the cipher text we will not able to extract any information about the plain text.

M= m1, m2 …..mi , be the message of length "i" bits.

K= k1, k2…..ki , be the key of the exact length as that of message i.e. "i".

C= c1, c2…...ci, be the cipher text string.

Now let us consider a single bit message "m" and key "k" then-

The encryption function "e" can be written as:

$$e = m\oplus k \tag{6}$$

The decryption function can be written as:

$$m=e\oplus k \tag{7}$$

In quantum cryptography, Qubits are encrypted by using quantum one time pad. Let Alice sends a qubit |Ψ> to Bob using the key k. Here, Eve be an intruder who is trying to listen the communication between Alice and Bob. Alice performs some operations on message |Ψ> by using key "k" which converts ate actual message into encrypted message say "ρ". When ρ reached to the Bob he decrypts the message by using decryption function and key k.

The quantum encryption function is:

$$|e > = x^k|m > \tag{8}$$

The quantum decryption function is:

$$|m > = x^k|e > \tag{9}$$

V. COMPARISION OF CLASSICAL AND QUANTUM CRYPTOGRAPHY

There are some parameters on the basis of which we can measure the performance of the image encryption techniques which are Visual Degradation (VD), Compression Friendliness (CF), Format Compliance (FC), Encryption Ratio (ER), Speed (S), and Cryptographic Security (CS) [8].

TABLE III COMPARISON OF CLASSICAL AND QUANTUM CRYPTOGRAPHY [6]

Sr No.	Feature	Classical Cryptography	Quantum Cryptography
1.	Basis	Mathematical computation	Quantum mechanics
2.	Development	Deployed and Tested	In initial stage, not tested fully
3.	Existing Infrastructure	Widely Used	Sophisticated
4.	Digital Signature	Present	Not Present
5.	Bit Rate	Depends upon computing power	1MBPS Avg.
6.	Expenditure	Almost zero	Crypto chip About 8058625 rupees
7.	Bit Storage	2n n-bit strings	One n-bit string
8.	Communication Range	Millions of miles	Maximum 10 miles
9.	Requirements	Software and Portable	Devoted Hardware and Communication line
10.	Life Expectancy	Required Up gradation as computing power increases	No changes as it is based on physics laws
11.	Communication Medium	Independent	Dependent

VI. CONCLUSION

The quantum cryptography is surely more secure than that of classical cryptography approach as it is working on principles of quantum mechanics and the features provided by the quantum bits approach. The quantum cryptography is very helpful to perform secure exchange of multimedia data like videos and images. The Quantum cryptography is in its initial stages, lots of work needs to be done to improve its performance and overcome its limitations like the problems to implement it and to increase the communication rang and the bit transfer rate.

REFERENCES

[1] Premlata sonawne, Leena Ragha, “Quantum Cryptography with Key Distribution in Wireless Network”, International Journal on Advanced Computer Theory and Engineering, ISSN: 2319-2526, volume 2, issue-6, 2013.

[2] Pooja Anil Patil, Renuka Boda, “Analysis of Cryptography: Classical Verses Quantum Cryptography”, International Research Journal of Engineering and Technology, e-ISSN: 2395-0056 p-ISSN: 2395-0072, Page no.1372-1376, volume: 03, Issue: 05, May 2016.

[3] Ms. Deepa Harihar Kulkarni, “Research Direction in Quantum Cryptography and Quantum Key Distribution”, International Journal of Scientific and Research Publications, ISSN: 2250-3153, volume 2, issue 6, June 2012.

[4] Sneha Charjan, D. H. Kulkarni, “Quantum Key Distribution using Different Techniques and Algorithms”, International Journal of Engineering Research & Technology, ISSN: 2278-0181, Vol. 3 Issue 11, November-2014.

[5] Seema S. Kute, Chitra G. Desai,” Quantum Cryptography: A Review”, Indian Journal of Science and Technology, ISSN (Print): 0974-6846, ISSN (Online): 0974-5645, Volume 10 (3), DOI:10.17485/ijst/2017/v10i3/110635, January 2017.

[6] Aakash Goyal, Sapna Aggarwal, Aanchal Jain, “Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper”, 5th IEEE International Conference on Advanced Computing & Communication Technologies [ICACCT-2011], ISBN-81-87885-03-3.

[7] Ch. Krishna, A. Sujith Kumar, “Secure Quantum Key Distribution Scheme with EPR Sequences”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Page no. 565-568, Volume 3, Issue 10, October 2013.

[8] Gajendra Singh Chandel, Vinod Sharma, Uday Pratap singh, “Different Image Encryption Techniques- Survey and Overview”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 6, Issue 8, August 2016.

[9] Noor Dhia Al-Shakarchy, Hiba Jabbar Al-Eqabie, Huda Fawzi Al-Shahad, “Classical Image Encryption and Decryption”, International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064. Volume 4, Issue 11, November 2015.

[10] Omar Farook Mahammad, Mohad Shafry Mohad Rahim, Subhi Rafeeq Mohammed Zeebaree and Falah Y.H. Ahmed, “A Survey and Analysis of the Image Encryption Methods”, International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 12, Number 23(2017) pp.13265-13280.