

# Improvising Security Issues Using Quantum Cryptography

<sup>1</sup> Abhishek Pradhan, <sup>2</sup> Sushree Soujanya Padhi, <sup>3</sup> B.Giridhar, <sup>4</sup> Mr Chandan Kumar Giri

<sup>1,2</sup> B.Tech Student

<sup>3,4</sup> Asst.prof in CSE dept

**Abstract** - Steganography is the technique of hiding confidential information within any media. In recent years various steganography methods have been proposed to make data more secure. At the same time different steganalysis methods have also evolved. The number of attacks used by the steganalyst has only multiplied over the years. Various tools for detecting hidden informations are easily available over the internet, so securing data from steganalyst is still considered a major challenge. While various work have been done to improve the existing algorithms and also new algorithms have been proposed to make data behind the image more secure. We have still been using the same public key cryptography like Diffie-Hellman and RSA for key negotiation which is vulnerable to both technological progress of computing power and evolution in mathematics, so in this paper we have proposed use of quantum cryptography along with steganography. The use of this combination will create key distribution schemes that are uninterceptable thus providing our data a perfect security.

**Keywords** - Steganography, Steganalysis, Steganalyst, Quantum Cryptography.

## 1. Introduction

Internet users frequently need to store, send and receive private information. The most common way to do this is to transform the data into different forms. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known as encryption. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually decrypt the data. A solution to this problem is steganography. Steganography is also a form of writing namely concealed writing.

The Greek word *staginess* means “unseen” or “hidden.” Steganography is thus a form of communication, which is designed to be hidden from general view. Steganography should not be seen as a replacement for cryptography but rather as a

complement to it.. There has been a rapid growth of interest in this subject over the last two years, and for two main reasons. Firstly, the publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital images, audio recordings, books and multimedia products; an appreciation of new market opportunities created by digital distribution is coupled with a fear that digital works could be too easy to copy. Secondly, moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages. In modern terms steganography is usually implemented computationally, where cover Works such as text files, images, audio files, and video files are tweaked in such a way that a secret message can be embedded within them.

The techniques are very similar to that of digital watermarking; however one big distinction must be highlighted between the two. In digital watermarking, the focus is on ensuring that nobody can remove or alter the content of the watermarked data, even though it might be plainly obvious that it exists.

Steganography on the other hand, focuses on making it extremely difficult to tell that a secret message exists at all. If an unauthorized third party is able to say with high confidence that a file contains a secret message, then steganography has failed. Steganography also differs from cryptography because the latter does not attempt to hide the fact that a message exists. Instead, cryptography merely obscures the integrity of the information so that it does not make sense to anyone but the creator and the recipient. The art of detecting steganography is referred to as steganalysis. With rapid advances in the field of steganography and cryptography there have also been major advances made in the field of steganalysis and cryptanalysis. Typically, a steganalysis begins by identifying any artifacts that exists in the suspect file as a result of embedding a message. Electronically, each of the tool used for steganography leaves a fingerprint or signature in the image that can be exploited to find the

message in the image. Steganalysis does not however consider the successful extraction of the message, there is usually a requirement of cryptanalysis.

So, after performing cryptanalysis on the cipher text, the plain text can easily be obtained. Over the years our focus has been mainly on security of data but the security of keys is as important as the security of data. Often this aspect is neglected. We have been using the same public key cryptosystem for many years now.

Since, uncertainty looms over the security of these cryptosystems; we have used quantum cryptography for securing the key distribution. Quantum cryptography is thought to be secure for three main reasons. One, the quantum no-cloning theorem states that an unknown quantum state cannot be cloned. Theoretically, messages sent using quantum cryptography would be in an unknown quantum state, so they could not be copied and sent on. Two, in a quantum system, which can be in one of two states, any attempt to measure the quantum state will disturb the system. A quantum message that is intercepted and read by an eavesdropper will become garbled and useless to the intended recipient of the message. Three, the effects produced by measuring a quantum property are irreversible, which means an eavesdropper cannot “put back” a quantum message to its original state. These three properties provide the power of quantum cryptography.

## 2. Related Work

S. K. Moon et al proposed an algorithm to hide data of any format in an image and audio file ( S.K Moon et al 2007).For steganography he used the least significant bit ( 4 LSB ) substitution method. The 4LSB method was implemented for color bitmap images and wave files as the carrier media. A new method of steganography in MMS was proposed by Mohammad Shirali et al .This paper presented a new method of steganography using both image and text steganography methods. This project was written in J2ME (Java 2 Micro Edition ) .In this method, data is broken into two parts with proper sizes and the parts were hidden in the image and text part of MMS message (Mohammad Shirali et al 2007).In order to further enhance the secrecy of steganography Piyush Marwaha and Pravesh Marwaha (Piyush Marwaha et al 2010 ) proposed an advanced system of encrypting data that combines the features of cryptography, steganography along with multi-media data hiding. This paper proposed the concept of multiple cryptography where the data will be encrypted in a cipher and the cipher will be hidden into a multimedia image file in encrypted format. This system was more secure than any other these techniques alone and also as compared to steganography and cryptography combined systems .Muhammad Asad et al proposed an enhanced least significant bit for audio steganography ( Muhammad Asad et al 2011 his paper proposes two ways to improve

the conventional LSB modification technique. The first way is to randomize bit number of host message used for embedding secret message while the second way is to randomize sample number containing next secret message bit. The improvised proposed technique works against steganalysis and decreases the probability of secret message being extracted by an intruder. Mohammad Hamdaqa used VoIP (Voice over IP) for real time network steganography, which utilizes VoIP protocols and traffic as a covert channel to conceal secret messages. This paper modifies the  $(k, n)$  threshold secret sharing scheme, which is based on *Lagrange's Interpolation*, and then applies a two phase approach on the LACK steganography mechanism to provide reliability and fault tolerance and to increase steganalysis complexity (Muhammad Hamdaqa et al 2011 ).A new perfect hashing based approach was given by Imran Sarwar Bajwa et al.It uses hashing based approach for steganography in grey scale images. The proposed approach is more efficient and effective that provides a more secure way of data transmission at higher speed. The presented approach is implemented into a prototype tool coded in VB.NET (Imran Sarwar Bajwa et al 2011 ).

## 3. Proposed Work

The proposed work consists of the given discussed phases.

### 3.1 Steganography

Steganography literally means covered writing. Its goal is to hide the fact that communication is taking place. Steganography is mainly applied to media such as images, text, video clips, music and sounds. Image steganography is generally more preferred media because of its harmlessness and attraction. The three basic techniques used for steganography are classified as follows:

(A)-Injection-Hiding data in sections of file that are ignored by the processing applications. Therefore avoid modifying those file bits that are relevant to an end user leaving the cover file perfectly usable.

(B)-Substitution-Replacement of least significant bits of information that determine the meaningful content of the original file with new data in a way that causes least amount of distortion.

(C)-Generation-Unlike injection and substitution, this does not require an existing cover file but generates a cover file for the sole purpose of hiding the message. There are many algorithms that can be used for steganography. The algorithm which we have used here for steganography is F5 which is much more secure than all the other algorithms. The F5 algorithm provides high steganographic capacity and can prevent visual attacks and

it is also resistant to statistical attacks. Even if the attacker is able to break this algorithm, he will get back only the cipher text and will have to perform cryptanalysis on it to get back the original text. Fig 1 shows the graphical representation of steganography.

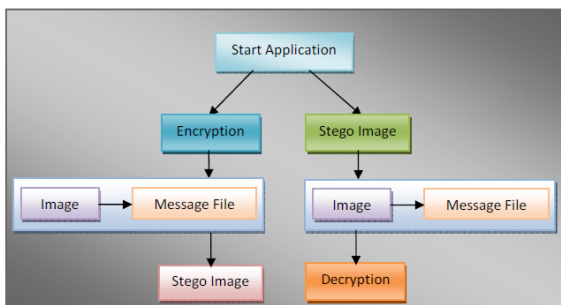


Figure 1. Graphical Representation of Steganography

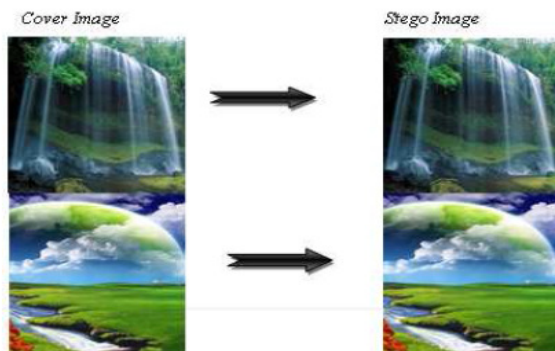


Figure 2. Results of Cover Image and Stego Image (after Hiding the Data behind the Cover Image)

### 3.3 Steganalysis

Steganography basically exploits human perception, as human senses are not trained to look for files that have information inside them. The art of detecting steganography is referred to as steganalysis.

Steganography have made rapid advances over the years and so have steganalysis. Steganography (and Steganalysis) is neither inherently good nor evil; it is the manner in which it is used which will determine whether it is benefit or detriment to our society. The number of attacks used by the steganalyst for detecting hidden informations has been only multiplied over the years. The types of attacks used by the steganalysts are following.

1. Stego only attack
2. Chosen stego attack
3. Known cover attack
4. Known stego attack

Various tools for detecting steganography are easily available over the internet. Various tools like Stegdetect and Xsteg are freely available over the internet for

detecting steganography. By performing Steganalysis on the image the attacker will only get the cipher text and he will have to perform Cryptanalysis to get back the original text.

### 3.4 Quantum Cryptography

Public key cryptosystems such as RSA and DEFFIE-HELMAN are still considered to be secure for key distribution. They have undergone over lots of public scrutiny over the years. The power of these algorithms are based on the fact that there is no known mathematical operation for quickly factoring very large numbers given today's computer processing power. The public cryptosystem has been working very well over the years but in the recent years it has been exposed to a handful of risks. Firstly a computer scientist at the Indian Institute of Technology, Manindra Agarwal solved a problem, how to tell if a number is prime, without performing any factoring, solving this problem may open the door for mathematician to figure out how to factor large numbers. Secondly, the advancements in computer processing will be able to defeat these cryptosystems in timely fashion thus making the public key cryptosystems obsolescent instantly.

So here we have used quantum cryptography for exchanging the keys efficiently. At this time, transmission speed and hardware expenses have generally limited the use of quantum devices to distribute the keys rather than the entire message. Classical methods of information security using encryption decryption or otherwise are known to be secure but not 100 percent. Increasing computation powers helps hackers to crack down the security cover. Quantum level is one which behaves somewhat differently than classical ones. Classical methods can never give 100% security for example even strong encryption like DES, AES are prone to be broken as much effective work has been done to break these. Dealing things at quantum level will definitely give perfect security because of the behavior of microscopic particles.

Assuming laws of Quantum mechanics is true, which follow Heisenberg's uncertainty principle and photon polarization we can provide 100% security.

#### 3.4.1 Why Quantum Cryptography

Rather than depending on the complexity of factoring large numbers, quantum cryptography is based on the fundamental and unchanging principles of quantum mechanics. In fact, quantum cryptography rests on two pillars of 20th century quantum mechanics –the Heisenberg Uncertainty principle and the principle of photon polarization. Heisenberg's uncertainty principle says that if you measure one thing, you can not measure another thing accurately. For example, if you measure

the position of an electron flying around an atom, you can not accurately measure its velocity. It can be represented using this equation. According to the Heisenberg Uncertainty principle, it is not possible to measure the quantum state of any system without disturbing that system. Thus, the polarization of a photon or light particle can only be known at the point when it is measured. This principle plays a critical role in thwarting the attempts of eavesdroppers in a cryptosystem based on quantum cryptography. Secondly, the photon polarization principle describes how light photons can be oriented or polarized in specific directions. Moreover, a polarized photon can only be detected by a photon filter with the correct polarization or else the photon may be destroyed. It is Heisenberg's uncertainty principle that makes quantum cryptography an attractive option for ensuring the privacy of data and defeating eavesdroppers.

### 3.5 Key Generation

Quantum property of light is used to generate key. Individual photons are completely polarized. Their polarization state can be linear or circular, or it can be elliptical, which is anywhere in between of linear and circular polarization

### 3.6 Securing Key Distribution

It is the one-way-ness of photons along with the Heisenberg uncertainty principle that makes quantum cryptography an attractive option for ensuring the privacy of data and defeating eavesdropper. The representation of bits through polarized photons is the foundation of quantum cryptography that serves as the underlying principle of quantum key distribution. Thus, while the strength of modern digital cryptography is dependent on the computational difficulty of factoring large numbers, quantum cryptography is completely dependent on the rules of physics and is also independent of the processing power of current computing systems. Since the principle of physics will always hold true, quantum cryptography provides an answer to the uncertainty problem that current cryptography suffers from; it is no longer necessary to make assumptions about the computing power of malicious attackers or the development of a theorem to quickly solve the large integer factorization problem.

Keys can be distributed using quantum cryptography in the following manner. The sender will send the message to the receiver using a photon gun. The stream of photons will be in one of the four polarization that corresponds to vertical, horizontal or diagonal in opposite directions (0,45,90,135 degree). At the receiver's end the receiver will randomly choose a filter and count and measure the correct photon polarization. Now, receiver will communicate with sender (out-of-band) about their correct measurement (without sending

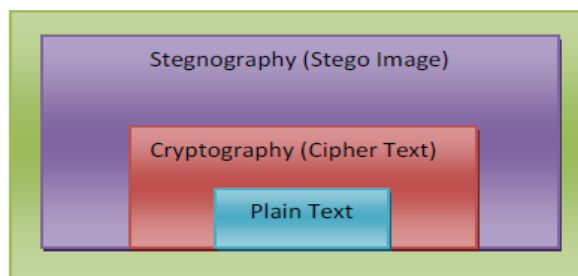
actual measurement values. The photons that were incorrectly measured will be discarded and the correctly measured photons will be translated into bits based on their polarization. Now, sender and receiver will generate one time pad combining their results. This one-time pad will be used in one time information exchange between them. None of them can know the actual key in advance because the key is the product of both their random choices.

Now, if an attacker tries to eavesdrop, he must select the correct filter otherwise the photon will get destroyed. Even if attacker is able to successfully eavesdrop, the information which he will get will be of little use unless he has the knowledge of correct polarization of each particular photon. As a result attacker will not correctly interpret meaningful keys and thus be thwarted in his endeavors.

### 3.7 Security

The data which has to be secured here is wrapped around number of security layers. If the attacker gets access to the stego image file in which the message is embedded. At first he will have to perform steganalysis to find out that this message contains a message or not. Even if after performing steganalysis he finds out that image contains some data, he will have to apply the same algorithm to retrieve the embedded file. Unfortunately, if he finds out the algorithm by which the texts have been embedded into the medium, he could get back only the cipher text file. The encryption algorithm which we have used here is AES, which is one of the most secure encryption algorithms used today. This provides an extra layer of security.

Now the hacker is left with only one choice to extract the embedded file and that is to compromise the encryption key used somehow. Since modern cryptography is vulnerable to both technological progress of computing power and evolution in mathematics, there is uncertainty that Diffie-Hellman and RSA will be secure for key distribution in future or not. Here we would like to propose a new model. This model could be easily applied on the web for making data more secure.



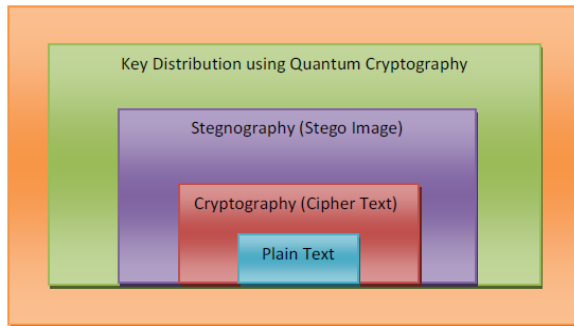


Figure 4. The proposed model of Steganography with Key Distribution using Quantum Cryptography

Main idea behind this model is to use quantum cryptography for securing key distribution thus providing our data another layer of security. This way we can provide perfect security to data over the internet.

#### 4. Future Work

At present quantum cryptography is used in very small area, the use of quantum cryptography should be encouraged and it should be used in wide area of applications beside that, maximum guaranteed transmission distance between remote parties is very less at present. As, optical fibers are not perfectly transparent, a photon will at times get absorbed and therefore not reach the end of the fiber. Although, quantum cryptography is secure but information retrieved is very less (due to loss). It should be improved. Another problem that needs to be addressed in future is if an attacker tries to tamper with the message whole message gets destroyed. It is a nice feature of quantum cryptography that no one can tamper with the message but at the same time due to this the receiver is also suffering because correct message was not delivered to the recipient, and now the sender will have to resend the message either from the same path or he will have to choose a different path.

#### 5. Conclusion

Securing the key distribution is as important as securing the data itself. In this paper we have made use of quantum cryptography thus improving the security of the keys and providing our data a perfect security. The use of quantum cryptography has added another layer of defense to our data. Even if we use most secure encryption algorithm and best stego technique to hide our data, if the keys gets compromised these security will be of no use. Quantum cryptography addresses current as well as emerging threats and it definitely has "competitive advantage" over other public key cryptosystems. We have used quantum cryptography only for key distribution rather than for entire messages because of limitations of transmission speeds and hardware expenses. The representation of bits through polarized photon is the foundation of quantum

cryptography that serves as the underlying principle of quantum key distribution. This paper concentrates on theory of quantum cryptography and the use of quantum cryptography for key distribution and how the use of quantum cryptography contributes to the field of steganography. In this paper we have shown that using quantum mechanics and photon polarization we can provide perfect security.

#### References

- [1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena (2004). Primes is in P. *Annals of Mathematics*, 160,781-793.doi: 10.4007/annals.2004.160.781
- [2] Imran Sarwar Bajwa and Rubata Raisat (2011). A New Perfect Hashing based Approach for Secure Steganograph. *Digital Information Management (ICDIM)*,174-178. doi: 10.1109/ICDIM.2011.6093325
- [3] Muhammad Asad, Junaid Gilani and Adnan Khalid (2011). An Enhanced Least Significant Bit Modification Technique for Audio Steganography Computer Networks and Information Technology (ICCNIT), 143-147. doi: 10.1109/ICCNIT.2011.6020921
- [4] Mohammad Hamdaqa and Ladan Tahvildari (2011). ReLACK: A Reliable VoIP Steganography Approach. *Fifth International Conference on Secure Software Integration and Reliability Improvement* ,189-197.doi: 10.1109/SSIRI.2011.24
- [5] S. Changder, N.C. Debnath and D.Ghosh (2011). A Greedy Approach to Text Steganography using Properties of Sentences. *Eighth International Conference on Information Technology: New Generations*, 30-35. doi: 10.1109/ITNG.2011.13
- [6] Piyush Marwaha and Paresh Marwaha (2010). VISUAL CRYPTOGRAPHIC STEGANOGRAPHY IN IMAGES. *Second International conference on Computing, Communication and Networking Technologies*, 1-6. doi: 10.1109/ICCCNT.2010.5591730
- [7] Jinsuk Baek, Cheonshik Kim, Paul S. Fisher and Hongyang Chao (2010). (N. 1) Secret Sharing Approach Based on Steganography with Gray Digital Images. *IEEE Conference on Wireless Communications, Networking and Information Security (WCNIS)* ,325-329.doi: 10.1109/WCINS.2010.5541793
- [8] Ferruccio Pisanello, Luigi Martiradonna, Piernicola Spinicelli, Angela Fiore and Jean-Pierre Hermier (2009). Polarized Single Photon Emission for Quantum Cryptography Based on Colloidal Nanocrystals. *11th international conference on Transparent Optical Networks*,1-4. doi: 10.1109/ICTON.2009.5185131
- [9] Vladimir L. Kurochkin and Igor G.Neizvestny (2009). Quantum Cryptography. *10th INTERNATIONAL CONFERENCE AND SEMINAR EDM'2009*, 166-170. doi: 10.1109/EDM.2009.5173960
- [10] Mehrdad S. Sharbaf (2009). Quantum Cryptography: A New Generation of Information Technology

Security System. Sixth International Conference on  
Information Technology: New Generations, 1644-  
1648.