Quantum cryptography helps to improve security problems.

Mr.BGiridhar,
Associate Professor, Computer Science and Engineering
Sri Venkateswara College of Engineering and Technology, Srikakulam, A.P., India

Abstract
Integration is the method used to hide private information in any medium. In recent years, several techniques of steganography have been suggested to protect data. Different techniques of steganalysis have also developed. The number of assaults that the steganalyst has employed has increased throughout the years. Different methods for detection of concealed information are readily accessible over the Internet, thus it is still a significant problem to secure data from Steganalyst. During several works to enhance the current algorithms and also new algorithms, data underlying the picture have been suggested to be safer. We still utilise the same public key cryptography like Deffie-Hellman and RSA for key negotiations, which is susceptible both to the technical development of computer power and to the advancement of mathematics. The adoption of this combination will produce uninterceptable key distribution methods, giving our data with complete safety.
Keywords - Stenography, Steganalyst, Cryptography of Quantum.

1. Introduction

Internet users often require confidential information to be stored, sent and received. The most frequent method is to convert the data into various formats. Only those who know how to give it back to its original form can understand the resultant data. This information protection technique is known as encryption. One of the main disadvantages of encryption is that there is no concealed data. Crypted, while unreadable, data nevertheless remains as data. If enough time is provided, someone can finally decode the data. Stegnography is a solution to this issue. Stenography is also a kind of writing that is hidden.

The term staginess in Greek means "unseen" or "hidden." Stegnography is thus a type of communication intended to be concealed from the general point of view. Stegnographyshould not be seen as a substitute for cryptography but as a supplement to it. In the past two years, interest in this topic has increased rapidly and for two major reasons. First, the publishing and broadcasting industries have taken an interest in techniques to hide encrypted copyright marks and serial numbers from digital images, audio recordings, books, multimedia products and have been concerned that new markets generated by digital distribution will become too easy to copy digital works. Secondly, different Governments have moved individuals to research ways by which private communications may be integrated into apparently benign cover messages in order to limit the availability of encryption services. Modernly speaking, stegnogramming is generally computerised where work such as text files, pictures, audio files and video files may be altered to contain a hidden message.

The methods are quite similar to digital watermarking, but there has to be a significant difference between the two. In digital watermarking, it is important to ensure that no one can delete or change the contents of the watermarked data, even though it may be clear that it exists. On the other hand, Stegnography concentrates on making it very difficult to say that a hidden message exists. If an unauthorised third party can confidently claim that a file contains a hidden message, stegnography has failed. Stegnography also differs from cryptography since cryptography does not try to disguise the fact that there is a message. Rather, cryptography just obscures the integrity of information such that no one, save the originator and the receiver, has meaning. Steganalysis is the art of identifying stegnography. In steganalysis and cryptanalysis significant progress was also achieved with fast progress in the areas of stegnography and cryptography. A steganalysis typically starts by detecting any devices that exist as a consequence of a message being embedded in the suspicious file. Electronically, the stegnography instrument leaves in the picture a fingerprint or signature that may be used to locate the message in the image. However, steganalysis does not consider successful extraction of the message, cryptanalysis is generally required.
Thus, following cryptanalysis on the encrypted text, it is possible to get plain text simply. Over the years we have focused primarily on data security, but key security is as essential as data security. This element is often overlooked. For many years now, we have been utilising the same public key cryptosystem.

Since then, the safety of these crypto-systems remains unclear; we have utilised quantum cryptography to secure the key. Quantum encryption is believed to be safe for three major reasons. First, the quantum theorem does not say that an unknown quantum state cannot be duplicated. Theoretically, communications transmitted via quantum cryptography could not be duplicated and delivered in an unknown quantum state. Two, a quantum system that may be in one of two states will disrupt the system in every effort to measure the quantum state. For the intended receiver of the communication, a quantum message intercepted and read by the eavesdropper is confused and worthless. Three, the effects generated by a quantum property measure are irreversible, thus an eavesdropper cannot "return" the quantum communication to its original condition. The power of quantum cryptography comes from these three characteristics.

2. Work related

S. K. Moon et al. developed a method to conceal picture and audio data from any format (S.K Moon et al 2007).
He utilised the least significant bit (4 LSB) replacement technique for stegnography. The 4LSB technique was used as the carrier medium for colour bitmap and wave files. Mohammad Shirali et al. developed a novel technique of stegnography in MMS. This article introduced a novel technique of picture and word stegnography. It's written in J2ME (Java 2 Micro Edition). The data is divided into 2 pieces with the correct sizes and the portions are concealed in the picture and text of the MMS message (Mohammad Shirali et al 2007). In order to further increase the security of PiyushMarwaha and PraveshMarwaha'sstegnography (PiyushMarwaha et al 2010), they have developed an up-to-date encryption system which combines the functionality of encryption with the concealing of multimedia data. This article

introduced the idea of multiple encryption, with data encrypted in a cypher and the cypher concealed in an encrypted multimedia picture file. This method was safer than any other such technology alone and compared to the combined systems of stegnography and cryptography
The improved least meaningful bit for audio stegnography was suggested by Muhammad Asad et al (Muhammad Asad et al 2011), in his work, to improve the traditional LSB modification method. The first method is to randomise the host message bit number used for secret message insertion whereas the second way is to randomise the sample number Next hidden message bit contains. The improvised technology acts against steganalysis and reduces the likelihood of an intruder extracting secret message. For real-time network stegnography, Mohammad Hamdaqa uses voice-over-IP (Voice-over-IP) as a covert route for covering secret communications. This article amends the (k, n) secret sharing threshold method based on Interpolation of Lagrange and then uses a two-step approach to LACK stegnography to ensure reliability and default tolerance and enhance the complications of steganalysis (Muhammad Hamdaqa et al 2011). Imran SarwarBajwa et al. presented a novel perfect hashing method. It utilises a hazardous technique for graphic artwork in grey pictures. The method suggested is more efficient and efficient, ensuring that data transfer is secured at greater speeds. The proposed method is implemented in a VB.NET-coded prototype tool (Imran SarwarBajwa et al 2011).

3. Work proposed

The work suggested comprises of the stages mentioned.

3.1 Stegnography

Steganography means covered writing, literally. Its objective is to conceal the fact that communication takes happening. Steganography is used primarily to material like pictures, text, video clips, music and sounds. Image steganography is usually favoured in the media because of its harmlessness and appeal. The following are the three primary methods used for steganography:
(a)-Injection-Hiding data in file sections which are disregarded by programmes for processing. Consequently, avoid changing those file bits important for the end user that leave the cover file fully functional.
(b)-Substitution-Replacement of minor information bits that define the relevant contents of the original file with new data in a manner that is less distortive.

(c)-generation - This doesn't need an existing cover file, but it creates a cover file for the express purpose of concealing the message unlike injection and replacement. There are numerous algorithms for stegnography. The stegnography method we utilised here is F5 which is much safer than any other algorithms. The F5 algorithm offers great stenographic capacity and is also resistant to statistical assaults. Even if the attacker breaks this method, he will only receive the cypher text back and have to cryptanalyze it to obtain the original text back. Figure 1 displays the graphical stegnography depiction.

ISSN 2515-8260 Volume 07, Issue 04, 2020

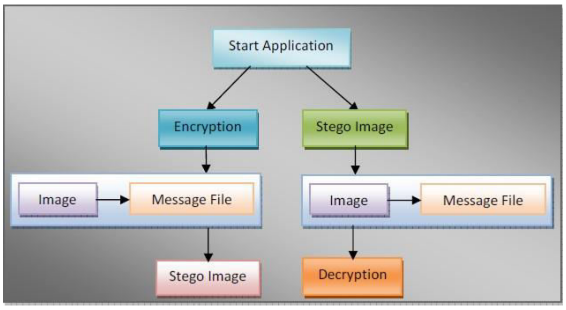

Figure 1. Stegnography graphical representation

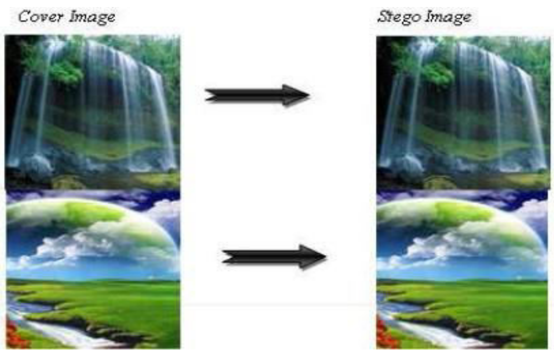

Figure 2. Cover Image and Stego Image results (after the Cover Image hidden data).

3.3 Stegnalysis

Basically, stegnography exploits human perception, since human senses are not trained to search for files containing information. Steganalysis is the art of identifying stegnography. Over the years, stegnography has made tremendous progress and so has steganalysis. Stegnography (and steganalysis) is fundamentally neither good or malignant; it is the way it is utilised that determines whether it is to our society's advantages or to our disadvantage. The number of attacks the steganalyst employed to discover concealed information has only increased over the years. There are the kinds of assaults that steganalysts employ.

1. Stego attack alone 1.
2. Selected stego assault.
3. Known assault cover cover
4. Known attack of stego

Various stegnography detection programmes are readily accessible on the Internet. Various programmes such as Stegdetect and Xsteg are free to detect stegnography via the Internet. By conducting Steganalysis on the picture, the attacker gets just the text and must perform Cryptanalysis to recover the original text.

3.4 Quantum Encryption

Public cryptosystems like RSA and DEFFIE- HELMAN are still deemed safe for key sharing. Over the years, they have faced a lot of public scrutiny. The strength of these algorithms relies upon the fact that, given today's computer processing capacity, there is no mathematical operation known to rapidly produce extremely big numbers. The public cryptosystem has worked extremely effectively over the years but has been exposed to a number of dangers in recent years. Manindra Agarwal solved a problem, firstly a computer scientist from the Indian Institute of Technology, how to determine whether a number is prime without any factoring, and resolving this issue may open the way for a mathematician to find how to factor big numbers. Secondly, progress in computer processing may quickly overthrow these cryptosystems, making public cryptosystems immediately obsolescent. Here we have thus utilised quantum cryptography to efficiently exchange the keys. At present moment, the use of quantum devices to disseminate the key rather than the whole message has usually been restricted by transmission speed and hardware costs. Classical data security techniques with or without encryption decryption are recognised to be safe but not 100 percent. Increasing computing capacities let hackers break through the safety cover. Quantum level is one that is distinct from classical ones. Classical techniques will never provide 100% security for example, even powerful encryption such as DES, AES is likely to be cracked since many effective work has been carried out to break them. Dealing Due to the conduct of tiny particles, objects at the quantum level would surely offer complete security. It is true that quantum mechanics legislation is accurate and that the Heisenberg principle of uncertainty and photon polarisation can guarantee 100 percent safety.

3.4.1 Why Cryptography of Quantum

Quantum cryptography is not based on the difficulty of big numbers but on the basic and unchangeable laws of quantum physics. Quantum cryptography really relies on two foundations of the quantum physics of the twentieth century - the Heisenberg Uncertainty principle and the photon polarisation principle. The uncertainty principle of Heisenberg states that you cannot measure one thing correctly. For example, you cannot precisely determine the location of an electron travelling around an atom. This equation may be expressed. Under the Heisenberg Uncertainty principle, without disrupting this system, it is not feasible to measure the quantum state of any system. The polarisation of a photon or light particle may thus only be determined at the measurement location. This concept plays a key role in preventing the efforts of eavesdroppers in a quantum cryptography based encryption. Secondly, the concept of photon polarisation explains how light photons may be directed or polarised in certain orientations. Furthermore, only a photon filter with a proper polarisation can detect a polarised photon otherwise the photon may be destroyed. Heisenberg is the concept of uncertainty that makes quantum encryption an appealing alternative for data privacy and the defeat of eavesdroppers.

3.5 Generation Key

Quantum light property is utilised for key generation. Individual photons are fully polarised. They may be linear or circular, or elliptical, which is somewhere between linear and circular polarisation.

3.6 Key Distribution Securing

In conjunction with the uncertainty principle of Heisenberg, quantum encryption is the only method of guaranteeing data privacy and thwarting eavesdropper. The encoding of bits by polarised photons is the basis of quantum cryptography, which serves as the basic principles of quantum key distribution. While the strength of contemporary digital encryption depends on the difficulties of computer production in big numbers, quantum encryption is entirely reliant on physics principles and also independent of the processing capacity of current computing systems. Since the principle of physics is always true, quantical encryption offers a response to the uncertainty issue suffered by present-day encryption; assumptions about the computer power of malicious attackers or the development of theorems to solve the large integer factorization problem quickly are no longer necessary.

The keys may be distributed in the following way using quantum cryptography. The sender sends the message with a photon cannon to the recipient. The photon stream is in one of four polarizations that match the vertical, horizontal or diagonal direction (0,45,90.135 degree). At the end of the receiver, the recipient selects the filter and counts randomly and measures the proper photon polarisation. Now, the receiver will transmit their accurate measurement to the sender (out-of-band) (without providing real measurement values. The wrongly measured photons should be deleted and the properly measured photons converted into bits depending on their polarisation. Sender and receiver will now produce a single pad with their results. This one-time pad is utilised in one-time exchange of information between them. None of them can know the key in advance, since the product of the two random selections is the key.

Now when an attacker attempts to eavesdrop, the appropriate filter has to be selected else the photon is destroyed. Even if the attacker is successful in eavesdropping, the information he receives is of little value unless he knows the proper polarisation of each photon. As a consequence, the attacker won't read meaningful keys properly and thus his efforts will be hindered.

3.7 Security

The data to be protected here are enveloped in many security layers. If the attacker has access to the image file stego that embeds the message. He has to do teganalysis first to figure out if this message includes or does not contain a message. Even if he finds out after steganalysis that the picture includes certain data, the same method must be used to extract the embedded file. If he discovers a method by which the messages are encoded in the medium, he can only receive the encrypted text file back. The encryption method we've chosen here is AES, one of today's safest encryption algorithms. This offers an additional security layer.

Now, the hacker can only retrieve the embedded file and compromise the encryption key somehow utilised. Since contemporary cryptography is susceptible to technical advances in computer power as well as to developments in mathematics, Deffie-Helman and the RSA are unsure whether key distributions will be secured in future or not. We want to offer a fresh model here. This approach can be simply used on the web to make data safer.

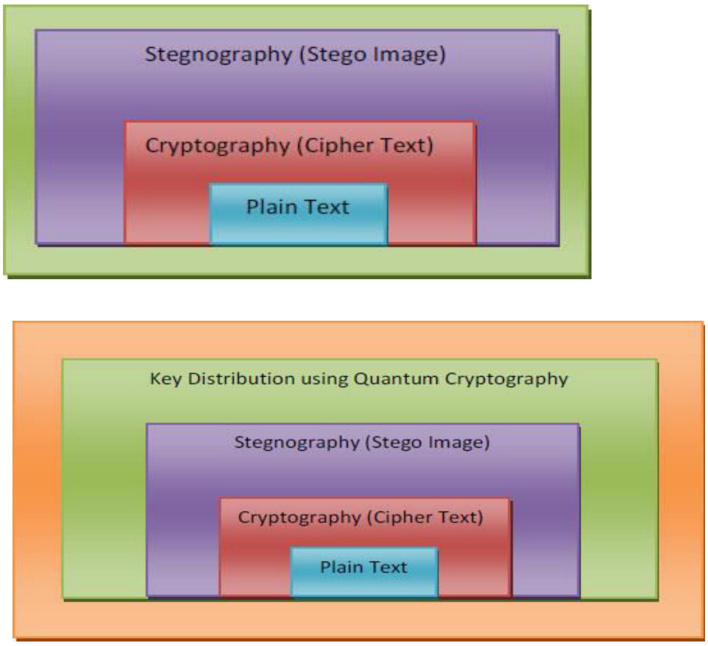

Figure 4. The suggested Key Distribution Stegnography model utilising Quantum Cryptography

The main concept behind this approach is to utilise quantum cryptography to secure key distribution, thus ensuring a new level of security for our data. This allows us to offer complete data security over the internet.

4. Work for the future

Currently, quantum cryptography is employed in very limited areas, it should be encouraged to use quantum cryptography and to be utilised in a large area of use, notwithstanding that the maximum assured transmission distance between distant parties is now quite short. Since optical fibres are not completely transparent, a photon is absorbed sometimes and therefore does not reach the end of the fibre. Quantum cryptography is safe but information is much less recovered (due to loss). It needs to be improved. A further issue to be addressed in the future is if an attacker attempts to manipulate the whole message. It is good to see that no one can manipulate the message, but that also hurts the recipient since the recipient did not get the proper message, and the recipient must either resend the message from the same route or select a new path.

5. Conclusion

It is just as essential to secure the key distribution as to secure the data. In this article, we have used quantum cryptography to improve the security of the keys and provide complete protection to our data. The implementation of quantic encryption provided another protection layer to our data. Even if we employ the safest encryption method and the finest stego technology to conceal our data, this protection will not be useful if the keys are compromised. Quantum cryptography tackles existing and future risks and certainly has a "competitive edge" over other key public systems. Because of transmission speed limits and hardware costs, we utilised quantum cryptography just for the main distribution rather than for full communications. Polarized photon representation of bits is the cornerstone of quantum cryptography which serves as the basis of the quantum key distribution concept. This article focuses on the theory of quantum encryption and how quantum cryptography adds to the area of stegnography and the application of quantum cryptography. In this article we have demonstrated that we can offer complete security using quantum physics and photon polarisation.

References

[1]Agrawal Manindra, KayalNeeraj and SaxenaNitin (2004). P. Mathematics Annals, 160,781-793.doi: 10.4007/annals.2004.160.781.

[2]RubataRaisat and Imran SarwarBajwa (2011). A New Perfect Hashing Secure Stegnograph Approach. Management of Digital Information, 174-178.doi:10.1109/ICDIM.2011.6093325. Digital Information Management.

[3]Muhammad Asad, GilaniJunaid& Khalid Adnan (2011). 143-147. Doi: 10.1109/ICCNIT.2011.6020921 Enhanced Bit Signifying Bit Modification Technique for Audio Steganography Computer Networks and Information Technology (ICCNIT)

[4]LadanTahvildari and Mohammad Hamdaqa (2011). ReLACK: A Trustworthy VoIP Steganography Approach. Fifth international conference for the integration and enhancement of secure software,189-197.doi: 10.1109/SSIRI.2011.24

[5] S. Changder, D.Ghosh and N.C. Debnath (2011). A Greedy text Steganography approach that uses the properties of sentences. Eighth International Conference on IT: New Generations, 30-35. DOI: 10.1109/ITNG.2011.13

[6]MarwahaPiyush and MarwahaParesh (2010). VISUAL CRYPTOGRAPHY IMAGE STEGANOGRAPHY. Second International Conference on Technologies of Computers, Communications and networking,1-6. doi: 10.1109/ICCCNT.2010.5591730

[7]JinsukBaek, Cheonshik Kim, Hongyang Chao and Paul S. Fisher (2010). (N. 1) Approach to secret sharing based on grey digital images. IEEE WLAN Conference, WCNIS, 0325-329.doi: 10.1109/WCINS.2010.5541793 IEEE Conference on WLAN Communications.

[8]Luigi Martiradonna, FerruccioPisanello, PiernicolaSpinicelli, Angela Fiore and Jean-Pierre Hermier (2009). Polarized single photon emission from colloidal Nanocrystals for quantum cryptography. 11th Transparent Optical Networks international conference,1-4.doi: 10.1109/ICTON.2009.5185131.

[9]Kurochkin and Igor G. Neizvestny Vladimir L. (2009). 10th EDM'2009 INTERNATIONAL CONFERENCE AND SEMINAR, 166-170. doi: 10.1109/EDM.2009.5173960