ISSN: 2321-7782 (Online)
Volume 2, Issue 2, February 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Hiding Data in Media Files Using Steganography and Quantum Cryptography

Vasim A. Shaikh[1]
B.E.Comp.
Department of Computer Engineering
Jaihind College of Engineering, Kuran,
Pune - India

Saddam Shaikh[2]
B.E.Comp.
Department of Computer Engineering
Jaihind College of Engineering, Kuran,
Pune - India

Shubhangi Dhamdhere[3]
Prof.
Department of Computer Engineering,
Institute Of Technology, Kuran,
Pune - India

Abstract: ***Security often requires that data be kept safe from unauthorized access. And the best line of defence is physical security (placing the machine to be protected behind physical walls). However, physical security is not always an option (due to cost and/or efficiency considerations). Instead, most computers are interconnected with each other openly, thereby exposing them and the communication channels that they use. Steganography secures information by protecting its confidentiality. It can also be used to protect information about the integrity and authenticity of data. Stronger Steganography techniques are needed to ensure the integrity of data stored on a machine that may be infected or under attack. So far Steganography is used in many forms but using it with Audio, Video & Image files is another Stronger Technique. The process of Steganography happens with Audio, Video & Image File for transferring more secure sensitive data. The Sensitive Data is Encoded with an Audio, Video & Image File and Passed over Insecure Channels to other end of Systems. Here we can use any file Format for Encryption and Decryption of Message. The given message will be encrypted with a given Audio, Video & Image file using a secret key. The System will then embed the secret message into the Audio, Video & Image file. The result will be a new Audio, Video & Image file, which has the secret message in it. While decrypting the same key should be given for encrypted Audio, Video & Image file to get the secret message from it.***

Keywords: Encryption, Decryption, GUI, Quantum Cryptography, Steganography.

I. INTRODUCTION

Steganography derives from the Greek word steganos, meaning covered or secret, and graphy (writing or drawing). On the simplest level, Steganography is hidden writing, whether it consists of invisible ink on paper or copyright information hidden in an audio file. Where cryptography scrambles a message into a code to obscure its meaning, Steganography hides the message entirely. These two secret communication technologies can be used separately or together—for example, by first encrypting a message, then hiding it in another file for transmission. As the world becomes more anxious about the use of any secret communication, and as regulations are created by governments to limit uses of encryption, steganography's role is gaining prominence. What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography.) The most common use of Steganography is to hide a file inside another file. When information or a file is hidden inside a carrier file, the data is usually encrypted with a password. Steganography includes the concealment of information within computer files. In digital Steganography, electronic communications may include

steganography coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganography transmission because of their large size.

II. DEFINITION

A. *Cryptography*

The art of protecting information by transforming data (*encrypting* it) into an unreadable format, called cipher text.

B. *Steganography*

The art and science of hiding information by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information.

C. *Encryption*

Encryption is a process which is applied to text messages or other important data, and alters it to make it humanly unreadable except by someone who knows how to decrypt it.

D. *Decryption*

Decryption is the reverse process to Encryption i.e. Decryption creates a Plain text from a Cipher text.

E. *Public-key cryptography*

Public-key cryptography is a cryptographic approach, employed by many cryptographic algorithms and cryptosystems, who's distinguishing characteristic, is the use of asymmetric key algorithms instead of or in addition to symmetric key algorithms.

F. *RSA algorithm*

RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, used encryption and authentication algorithm.

G. *DCT algorithm*

A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies.

H. *Stego Video*

Stego video is nothing but the video containing the secret data hidden into it.

I. *Framing*

Framing is concerned to the dividing the video file into sequence of individual frames.

J. *Embedding*

It is the process of hiding the information into the pixels information.

K. *Extracting*

It is the process of recovering the hidden information from the pixel information.

L. *DES Algorithm*

This algorithm is a block ciphering algorithm uses 128 bit block and 56 bit ciphering key for both encryption and decryption. It uses both substitutions as well as transformation technique.

III. System Design

A. *Proposed Algorithm Architecture*

The proposed architecture is a blend of dynamic video generation and digital Steganeography thus providing a protected and reliable transmission of data over the network . The following diagram represents the working of our proposed algorithm. The sender and the receiver will possess a database consisting of the 16 same images. Each image will have a 4 bit combination allocated to it. This same 16 images and their associated 4 bit code can be exchanged between the users by meeting face to face or by simply passing it over the net securely. First input to the proposed algorithm is 4 integer values. The next input by the user will be the data file which is converted into bytes. The whole data is divided into small chunks of 4 byte. For the last chunk if the data is less than 4 bytes then dummy data is added to it. Now the data from the 4 byte chunk is converted into bits resulting in 32 bits of data. Then the 4 bits are selected based on the 4 integer values supplied by the user. The image associated with this 4 bit code is picked. Now using the key 28 pixels are dynamically selected and the bits are hidden into the respective pixels.

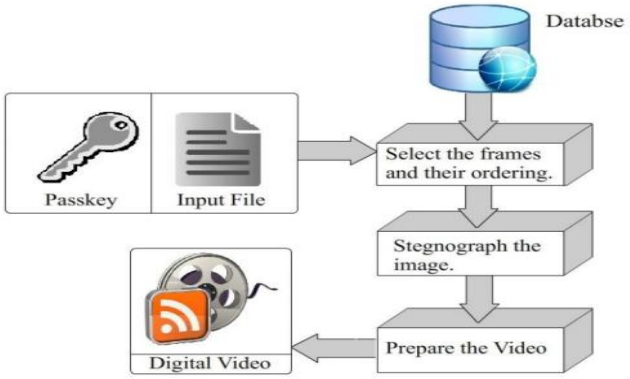

Fig. Proposed Algorithm Architecture

Thus each image consists of 4 byte of data hidden in it. The rest chunks are steganograped in the similar manner. Then all the images are combined to form a video which is then passed over the network. At the receiver end the video file is split back into images. An image comparison algorithm is used to compare the images in the video and find out their respective codes. The bits are placed back in the right position by using the passkey supplied. Even the hidden data in the rest of the image retrieved using the passkey. Thus the data file is reproduced.

B. *System Architecture*

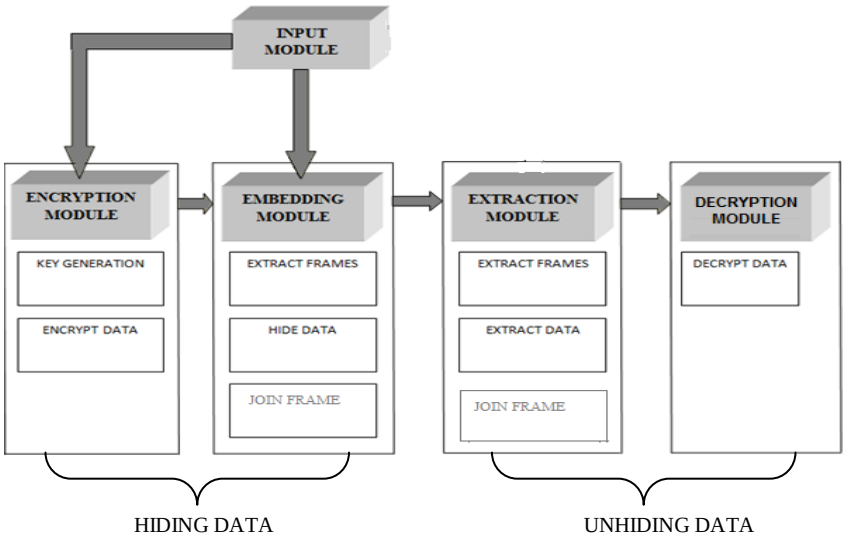

Fig. Steganeography Architecture

C. Quantum Cryptography

Quantum cryptography is the single most successful application of Quantum Computing/Information Theory. For the first time in history, we can use the forces of nature to implement perfectly secure cryptosystems. Classical Cryptography relies heavily on the complexity of factoring integers. Let ***K*** is called the key. The key is known only to sender and receiver: it is secret, Anyone who knows the key can decrypt the message. Key distribution is the problem of exchanging the key between sender and receiver. Using quantum effects, we can distribute keys in perfect secrecy.

The Result: The Perfect Cryptosystem, **QC = QKD + OTP**

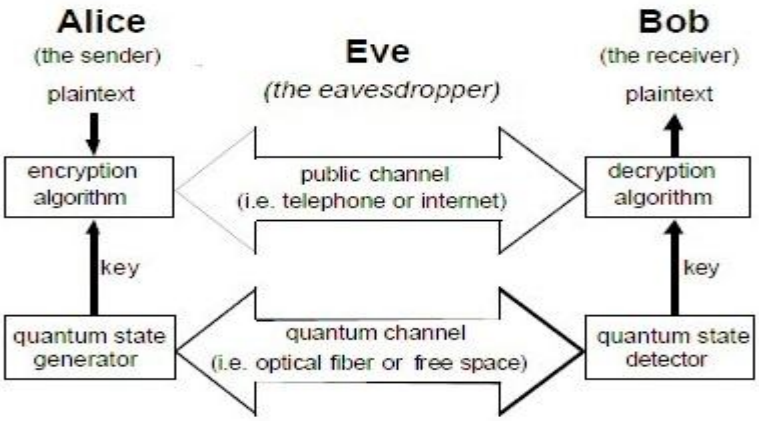

Fig. Quantum key Distribution

IV. ADVANTAGES

a) This system uses features offered by Public key Infrastructure or Private key Infrastructure.

b) It protects data from exposure to people who are not using this tool.

c) This system offers encryption as well as decryption of text files using various encryption algorithms.

d) It supports File formats as .wav for audio, .jpeg for image, .wm4, avi for video.

V. APPLICATIONS

a) This tool provides secure communication over unsecured medium.

b) It distribute key over the user using quantum cryptography.

c) Use of image, audio, video steganography in a single software module.

VI. CONCLUSION

The main aim behind this paer is to provide a security for our confidential data using steganeography and quantum cryptography. By using quantum cryptography we are able to distribute a key over a receiver so nobody can identify exact key of decryption. This tool can be used for hiding the text message in the image or the audio files or video files. Also, the message that is sent can be encrypted, so as to support secure Steganography. Regardless, the technology called Steganography is easy to use and difficult to detect. The more that you know about its features and functionality, the more ahead you will be in the game.

References

1. "Data Hiding In Video" (*Arup Kumar Bhaumik,Minkyu Choi,Rosslin R. Robles,Maricel O.Balitanas*) From International Journal of Database Theory and Application Vol.2-2 June 2009.
2. "Stego Machine-Video Steganography using Modified LSB Algorithm" *(Mritha Ramlingam*) From World Academy of Science, Engineering & Technology 50,2011 .
3. "Hiding text in audio using multiple LSB Steganography and provide security using cryptography" (*S.S.Divya,M.Ram Mohan Reddy*) From International Journal of Scientific & Technology Research Volume 1-6 July 2012.

4. "Steganography- A Data Hiding Technique" From International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.
5. "Developing an application with RSA algorithm with JAVA" *(M. Nusret SARISAKAL, Selcuk SEVGEN, Dogal ACAR.)*.
6. Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.
7. Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010 DOI : 10.5121/sipij.2010.1206 60 titled 'two new approaches for secured image steganography using cryptographic techniques and type conversions'
8. Journal of Theoretical and Applied Information Technology © 2005 -2009 JATIT. All rights reserved. www.jatit.org 35 'a novel information hiding technique for security by using image steganography' by m. sitaram prasad

AUTHOR(S) PROFILE

Mr. Vasim Shaikh currently pursuing his B.E degree in Computer Engineering from Jaihind College of Engineering, Kuran (University of Pune). Also received the Diploma in Computer Technology from Vamanrao Ithape Polytechnic,Sangamner (MSBTE) in 2011.

Mr. Saddam Shaikh currently pursuing his B.E degree in Computer Engineering from Jaihind College of Engineering, Kuran (University of Pune). Also received the Diploma in Computer Technology from Vamanrao Ithape Polytechnic,Sangamner (MSBTE) in 2011.

Prof. Shubhangi Dhamdhere currently pursuing her Mtech degree in Computer Engineering from S.P.C.O.E, Otur .

