IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 1 (May. - Jun. 2013), PP 15-19
www.iosrjournals.org

An Overview of Steganography

Sheelu[1] , Babita Ahuja[2]
[1](M. Tech (CSE) - Manav Rachna College Of Engineering, Faridabad, India)
[2](Assistant Professor (IT), Manav Rachna College Of Engineering, Faridabad, India)

Abstract: *The paper explore about an overview of steganography, different methods of steganography, its applications and how it is different from cryptography Digital communication has become an essential part of infrastructure. Nowadays, a lot of applications are Internet-based and demand of internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So different techniques like cryptography and steganography are used to secure the communication. Steganography is the scheme of hiding the existence of secret information in the cover file.*

Keywords : *Steganography, Cryptography, Cover file, Stego file, key*

I. Introduction

Steganography is the technique of hiding secret information in a communication channel in such a manner that the very existence of information is concealed. It is the science of "invisible" communication and prevents an unintended recipient from suspecting that the data exists. Steganography is derived from the Greek word steganos which means "Covered" and graphy means "Writing", i.e. covered writing. Many different carrier file formats can be used like Text, Images, and videos, but digital Images and Audios are the most popular because of their frequency on the Internet.

The steganography hides different types of data within a cover file. The resulting stego file also contains hidden information, although it is virtually identical to the cover file. Steganography 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).Fig.1[1] shows the block diagram of a secure steganographic system. Input messages can be images, texts, video, etc. The components of steganographic system are:

secret message: The secret message or information to hide.
cover file/ digital medium: The data or medium which concealed the secret message.
stego file: A modified version of cover that contains the secret message.

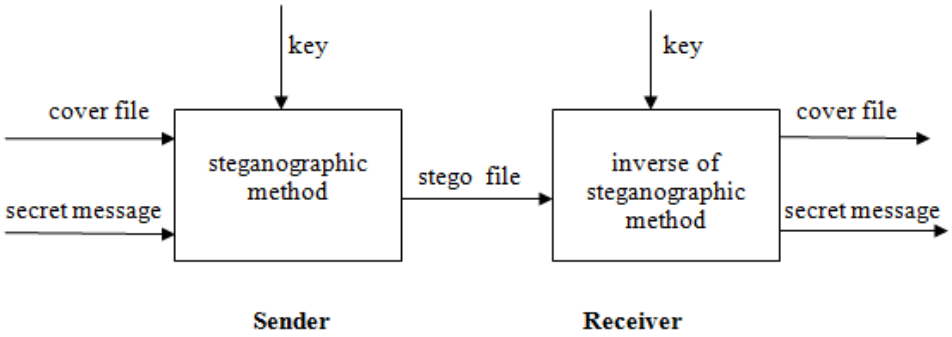

Figure 1. A generic Steganography System

key: Additional secret data that is needed for the embedding and extracting processes and must be known to both, the sender and the recipient
steganographic method: A steganographic function that takes cover, secret message and key as parameters and produces stego as output.
inverse of steganographic method: A steganographic function that has stego and key as parameters and produces secret message as output. This is the inverse of method used in embeding process in the sense that the result of the extracting process is identical to the input of the embedding process.

The embedding process embeds the secret message in the cover file. The result of the embedding function is slightly modified version of Cover file: the stego file. After the recipient has received stego file, he starts the extracting process with the stego file and the key as parameters. If the key that is supplied by the recipient is the same as the key used by the sender to embed the secret message and if the stego data the recipient uses as input is the same data the sender has produces, then the extracting function will produce the original secret message.

II. Difference between Steganography and Cryptography

In cryptography[1], the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to cover or hide the encoded message. Cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. The purpose of cryptography is to secure communications by changing the data into a form that cannot be understand Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography does not alter the structure of the secret message ,but hides it inside a cover image so that it cannot be seen. Steganography is the technique of hiding secret information in a communication channel in such a manner that the very existence of information is concealed. It is the science of "invisible" communication and prevents an unintended recipient from suspecting that the data exists. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data

Table1 Difference between steganography and cryptography

Steganography	**Cryptography**
Message passing is umknown	Message passing is known
Steganography prevents discover of the very existence of communication	Encryption prevents an unauthorized party from discovering the contents of a communication
Little known technology	Common technology
Technology still being developed for certain formats	Most of algorithm known by all
Once detected message is known	Strong current algorithm are currently resistant to attack, larger expensive computing power is required for cracking
Steganography does not alter the structure of the secret message	Cryptography alter the structure of the secret message

III. Types of Steganography

There are basically three types[2] of steganographic protocols used. They are:

- Pure Steganography
- Secret Key Steganography
- Public Key Steganography

Pure Steganography is defined as a steganographic system which does not require the exchange of a cipher such as a stego-key. This method of is not much secure because the sender and receiver can rely only upon the assumption that no other parties are aware of the secret message.

Secret Key Steganography is defined as a steganographic system that requires the exchange of a secret key (stego-key) previous to communication. Secret key Steganography takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can

reverse the process and read the secret message. Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key Steganography exchanges a stego-key, which makes it more vulnerable to interception. The benefit to Secret Key Steganography is even if it is intercepted; only parties who know the secret key can extract the secret message.

Public Key Steganography is defined as a steganographic system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly. Sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public Key Steganography provides a more strong way of implementing a steganographic system because it can utilize a much more robust and researched technology in Public Key Cryptography. It also has multiple levels of security in that unwanted parties must first suspect the use of Steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message.

3.1 Characteristics of Steganograhic system

An effective steganographic scheme should posses the following desired characteristics[3] :

- Secrecy: A person should not be able to extract the hidden data from the host medium without the knowledge of the proper secret key used in the extracting procedure.
- Imperceptibility: The medium after being embedded with the hidden data should be indiscernible from the original medium. One should not become suspicious of the existence of the covert data within the medium.
- High capacity: The maximum length of the covert message that can be embedded should be as long as possible.
- Resistance: The secret data should be able to survive when the host medium has been manipulated, for example by some lossy compression scheme .
- Accurate extraction**: T**he extraction of the covert data from the medium should be accurate and reliable.

IV. Different File Formats Used as Carrier in Steganography:

The four main categories of file formats[4] that can be used as carrier in steganography are:
I. Text
II. Images
III. Audio/ Video
IV. Protocol

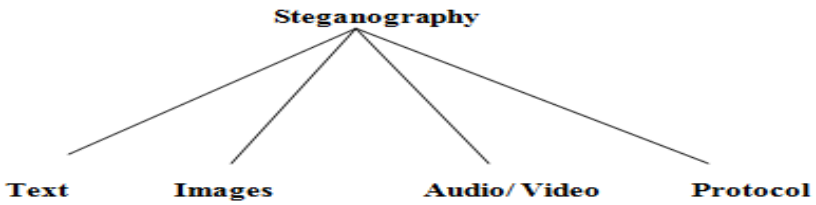

Figure 2:Different carriers in steganography[4]

I. **Text steganography**: Hiding information in text is the most important method of steganography. The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data
.

II. **Image steganography:** Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message.

III. **Audio steganography:** Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information.

IV. **Protocol steganography:** The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

V. Literature Survey

Jayaram[1] in his paper discuss the disadvantages of the different procedure and how those are different with present method. The main disadvantages of existing methods like echo hiding, spread spectrum and parity coding are, human ear is very sensitive to noise and it can often detect even the slightest bit of noise introduced into a sound file and another problem is robustness. The disadvantage of Phase coding is low data transmission rate because the secret message is encoded only in the first signal segment. Hence this method is used only when a small amount of data needs to be transferred. LSB method allows large amount of secret information to be encoded in an audio file.

Steps to hide secret information using LSB are:

a. Covert the audio file into bit stream.

b. Convert each character in the secret information into bit stream.

c. Replace the LSB bit of audio file with the LSB bit of character in the secret information.

This proposed method provides greater security and it is an efficient method for hiding the secret information from hackers and sent to the destination in a safe and undetectable manner. This proposed system also ensures that the size of the file is not changed even after encoding and it is also suitable for any type of audio file format.

K.P.Adhiya[3] in his paper proposed an algorithm that has been implemented for Audio Signal to hide text. The algorithm was based on the redundancy of bits in binary code of numbers, lowercase and uppercase alphabets. The binary code of numbers from 0 to 9, A to O, O to P, a to o and a to p the last 4 bits are different and first 4 bit are similar. So any number and alphabet can be represented by the last 4 bits and adding either '0' or '1' at the first position. To differentiate whether the character is number, uppercase alphabet or lowercase alphabet control symbols are used which is of the same type as that of number or alphabet.

At the sender side, first of all input the text which is to be embed then convert the text into 5 bit code by checking the redundancy in binary code of alphabets and numbers. Now read WAV audio file as cover file, Select audio sample and hide the converted 5 bit code of the text in WAV file using LSB algorithm and Repeat till the whole message embed in audio and get the stego file. At the receiver side, Read the stego-file i.e. cover audio after encoding then extract the message by reading the control symbols in samples and reading LSB. Now select all samples and store all LSB position bits in array. Divide the array into number of rows and columns and display the secret message. 16bitWAV and 8bitWAVaudio file are supported and the secret message can be hidden in the audio file with less storage capacity. The proposed algorithm gives better result for 16 bit wav audio as compared to 8 bit .

Samir Kumar Bandyopadhyay[5] in his paper present two layered approach . Here two secret messages rather than one can be transmitted with a single cover file. Layering approach gives opportunity to do this. At the first level, cover file (C) was embedded with the first secret message S1. Assume the stego file as C1 which is cover file for next level where secret message can be denoted as S2. Now the final stego file created as C12. So C12 holds both S1 and S2.

Two levels of steganography can be identified as layer 1 and layer 2. At layer 1 LSB modification technique and at layer 2 parity encoding technique has been used. After the implementation of LSB technique, it is observed that stego-file hasn't been audibly modified and there is reasonable no change between input carrier file and output stego file. The parity encoding has been implemented by breaking the data part of the wav file into number of regions. Each region includes same number elements of secret message text. Then parity flag of each region calculated. If it does not match with the message bit then the last bit of that region has been changed with the message bit. Stego object hasn't been audibly modified. Also after decoding, secret message object can be retrieved. When stego object decoded means passes through the decoding algorithm of phase encoding method the secret message of second level is retrieved. When decoy object passes through the decoding algorithm of LSB modification method the secret message of first level is retrieved

R Sridevi[6] in his paper introduced Enhanced Audio Steganography , which is a method of hiding the message in the audio file of any formats. EAS contain extra layers of encryption and decryption. The four layers in EAS are: Encoding, Decoding, Encryption, Decryption. At the sender side first of all secret message is encrypted using a key, then encrypted message is encoded with audio file (carrier file) and stego file is send to the destination. At the receiver side, stego file is decoded and encrypted file is extracted, then encrypted file is decrypted using the key and secret message is extracted The quality of sound depends on the size of the audio which the user selects and length of the message. The main two features of this system are

1) Size of file is not changed after encoding.

2) Since it is bit level manipulation the sound variations cannot be determined by any current software.
It provide the user to give secret key for encryption. The length of message is more than the existing system. The quality of the audio doesn't change variably. The encryption key can be any combination of characters, symbols, numbers. The key which is used for encoding is also used for decoding .This is a secret key where the both user have to agree upon a single common key.

Vivek Jain[7] in his paper describe how to implement public key steganography : first of all he Find the shared stego- key between the two communication parties let user A and user B, by applying Diffie Hellman Key exchange protocol. Diffie-Hellman key exchange protocol shows the technique for the key exchange between two parties (user A and user B) to get shared Stego-key values. User A must generate the keys (public and private keys) and use his private keys to give new public key and send it to user B's side. User B must obtain and issue new public keys. Then at the end the protocol, each side recovers his/her received public key to reach the shared values between them, which mean user A and user B have arrived same sego-key value. Then information is encrypted by using the shared stego-key which already generated.

VI. Conclusion

Steganography is not intended to replace cryptography but supplement it. Hiding a message with steganography methods reduces the chance of a message being detected. However, if that message is also encrypted, if discovered, it must also be cracked. There are an infinite number of steganography applications. Steganography does not only pertain to digital images but also to other media (files such as voice, other text and binaries; other media such as communication channels, the list can go on and on).

steganography is not a good solution to secrecy. If a message is encrypted using substitution (substituting one alphabet h another), permute the message (shuffle the text) and apply a substitution again, then the encrypted ciphertext is more secure than using only substitution or only permutation. NOW, if the ciphertext is embedded in an image, video, voice, etc. it is even more secure. If an encrypted message is intercepted, the interceptor knows the text is an encrypted message. With steganography, the interceptor may not know the object contains a message.

References

[1] Jayaram P, Ranganatha H R, Anupama H S, " Information Hiding Using Audio Steganography – A Survey" in The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011

[2] Jammi Ashok, Y. Raju, S. Munishankaraiah, K. Srinivas "Steganography: An Overview" in International Journal of Engineering Science and Technology Vol. 2(10), 2010

[3] K.P.Adhiya and Swati A. Patil, " Hiding Text in Audio Using LSB Based Steganography" in Information and Knowledge Management Vol. 2, No.3, 2012

[4] Pratap Chandra Mandal Modern "Steganographic technique: A survey" in International Journal of Computer Science & Engineering Technology (IJCSET)

[5] Prof. Samir Kumar Bandyopadhyay and Barnali Gupta Banik "Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique" in International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 1, Issue 2, July – August 2012

[6] R Sridevi, Dr. A Damodaram, DR. Svl. Narasimham "Efficient Method Of Audio Steganography By Modified LSB Algorithm And Strong Encryption Key With Enhanced Security" in Journal of Theoretical and Applied Information Technology

[7] Vivek Jain , Lokesh Kumar, Madhur Mohan Sharma, Mohd Sadiq, Kshitiz Rastogi "Public-Key Steganography Based On Modified LSB Method" in Journal of Global Research in Computer Science Volume 3, No. 4, April 2012