Steganography – Hiding Critical Information through Multimedia-Audio File

Dr. Kuntal Patel [1] and Lalwani Mahesh [2] and Jadav Hardik [3]

[1] Asst. Prof., MCA Programme, Institute of Technology, Nirma University, Ahmedabad
[2, 3] Student, MCA Programme, Institute of Technology, Nirma University, Ahmedabad
Email: kuntal.patel@nirmauni.ac.in, mahesh_lalwani001@yahoo.com, hadu_123@yahoo.com

Abstract

Today's networked based information systems are transferring secret data electronically. Numbers of Cryptographic techniques are available to protect such data. One lesser known but rapidly growing method is Steganography; it is an art and science of hiding information such that it does not even appear to exist. Steganography can be used to hide messages, secret keys, private data or information into a text file, image, audio or a video file. There are certain disadvantages when we use only cryptographic techniques. Attacker can easily understand that something important is stored in the encrypted message. Combination of Cryptography and Steganography allows us to send the sensitive data through the use of multimedia file with the great security. In this paper we had proposed new algorithm for implementing greater security on the information being transferred over the network by combining Cryptographic techniques and Steganography using an audio file. The paper also describes the advantages and disadvantages of proposed algorithm, as well as, strengths and weaknesses of the Steganography.

Key words: Steganography, cryptography, Stegno-text, Cover text

1. Introduction

Steganography is the art and science of writing hidden messages in such a way that no-one apart from the sender and intended recipient even realizes there is a hidden message, a form of security through obscurity.[01] By contrast, cryptography obscures the meaning of a message, but it does not conceal the fact that there is a message. In countries where encryption is illegal, often steganography and cryptography are used together to ensure security of the message.

Historically various techniques have been used for Steganography. Some of them are Character marking, use of Invisible ink, Pin punctures on selected letters on documents and type writer correction ribbon. [02] Today, the term steganography provides the facility of hiding digital information within computer files. For example, the sender might start with an ordinary-looking image file, and then adjust the color of every 100th pixel to correspond to a letter in the alphabet; a change is so minor that someone who isn't actively looking for it is unlikely to notice it.

The idea of a data hiding is not a new. It has been used for centuries across the world. The word *steganography* is of Greek origin and means, *"covered, or hidden writing"*. Its ancient origins can be traced back to 440 BC. [03] The writing medium at that time was text. Herodotus mentions two examples of steganography; he describes how a man named Harpagus killed a hare and hid a message inside its belly. Then he sent the hare with a messenger disguised as a hunter. Another ancient example is that of Histiaeus, who shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden. Letter his hair grow back and then

shaving it again after he arrived at the receiving party to reveal message so in those days the data is hidden with such techniques and as the time passes the new techniques are evolved.

In modern times the steganography can be looked as study of art and science of communicating in a way that hides the existence of communication.

Currently there are two directions within a steganography which is shown in the figure 1: One of the branches is for *protection against detection* and other is for *protection against removal.*[04] The latter is used for hiding trademark in images, music and software and this technique is referred to as a watermarking.

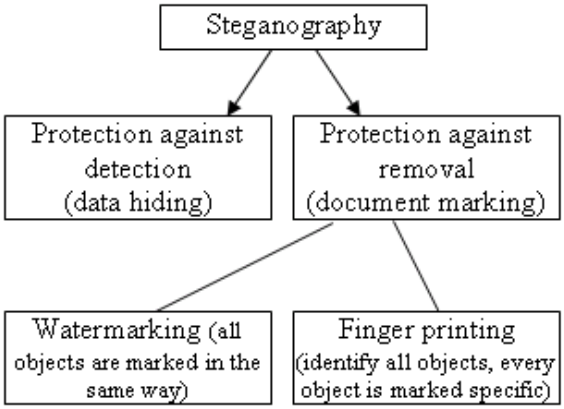

Figure 1: Schematic representation of steganographic procedure

Nowadays it is very popular with current industry demands for digital watermarking and finger printing of audio and video. One of the simple examples of it is: the least significant bits of an audio are replaced with a data from a text file in such a way that the third party would detect little if any loss of audio quality. An audio file posted to Internet or at public domain that contain highly sensitive message but it generate no suspicion at all.

In contrast to cryptography, the goal of steganography is to hide a message inside another 'harmless' message in such a manner that it does not allow other person to detect that there is a secret message present.

In the field of steganography some terminology has developed. The information is to be hidden into the cover data is known as "embedded" information. The process of putting the hidden or embedded data into the cover data is known as embedding. Especially when referring to the image steganography, the cover image is known as container. The term "cover" is used to describe the original, innocent message, data, audio, still, video and so on. When referring to the audio signal steganography, the cover signal is sometime called as "host" signal. This process could be represented in the following formula:
Cover medium + embedded message + stegokey = stego-medium

The possible carriers of these hidden messages are innocent looking carriers, such as images, video, audio and text. A message is to be transmitted could be plaintext, cipher text, images or anything that could be represented as a bit stream. Carrier and the message to be transmitted create a stego-carrier, it may use secret-key to embed the information. The secret-key is referred to as stego key.

In the stegnographic file system the attacker who does not know the name of file and password or stego-key for accessing, it cannot determine whether the file is even present or not. Note that the concept of steganography is different from cryptography file system, which enciphers the files to protect their contents until a decryption key or password is entered.

2. Proposed Algorithm for Hiding Data

Step 1: Convert your plain text (secret critical information) into cipher text using any one encryption algorithm. While doing encryption of plain text into cypher text private key 1 is applied so that only authorized person can decrypt it.

Step 2: Hide your cypher text into the audio or video file using Steganography algorithm and also apply another private key 2 for authentication purpose. Again there are number of steganography algorithms available for it.

The outcome of this step is the audio or video file with the coded message containing secret critical information. This file is then transmitted by the sender to receiver through the transmission medium. Here while transmitting file if any unauthorized person receives it although he/she is not able to gain the critical information as it is in the encrypted form.

First two steps are done by the sender who wants to transmit the critical information. The remaining two steps are performed by the receiver to get the critical information back.

Step 3: This is the reverse process of step 2. Apply the steganography algorithm on the encoded file received by the receiver. Also while using this algorithm private key 2 is applied to obtain the cipher text.

Step 4: Apply the decryption algorithm on the cipher text received from step 3 to get the original critical information back. The private key 1 is applied while decryption process in order to ensure that receiver is authorized person.

So this way critical information is transmitted from sender to receiver using audio or video file. The figure no. 2 is graphical representation of above algorithms. The disadvantage of this algorithm is that it requires lot of overhead to hide a few bits of information.

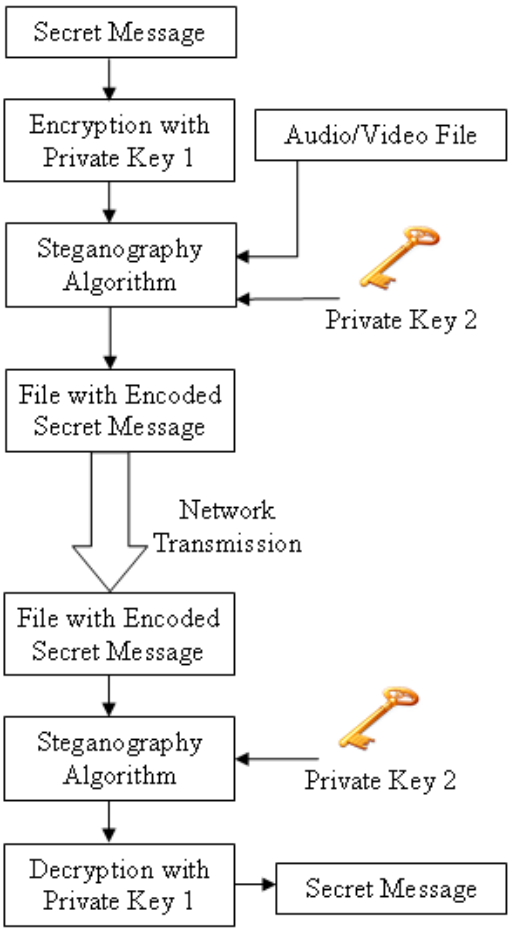

Figure 2: Implementation of data hiding using Steganography

3. Important Issues in Audio Steganography

Because of the range of the human auditory system (HAS), data hiding in audio signals is especially challenging[05]. Also, the auditory system is very sensitive to additive random noise. When performing data hiding on audio, one must exploit the weaknesses of the HAS, while at the same time being aware of the extreme sensitivity of the human auditory system.

Audio environments: When working with transmitted audio signals; one should bear in mind two main considerations. First, the means of audio storage, or digital representation of the audio and second, the transmission medium the signal might take.

Digital representation: Digital audio files generally have two primary characteristics.

Sample quantization method: The most popular format for representing samples of high-quality digital audio is a 16-bit linear quantization, such as that used by WAV (Windows Audio-Visual) and AIFF (Audio Interchange File Format).

Temporal sampling rate: The most popular temporal sampling rates for audio include 8 kHz. Another digital representation that should be considered is the ISO MPEG-Audio format, a perceptual encoding standard.

Transmission medium: Transmission medium of an audio signal refers to the way you transfer the data from sender to the receiver.

4. Advantages and disadvantages of algorithm

Data encryption only can used to hide the data but the problem with it is that encrypted file is distinguishable from regular files and authorization can force the user until the user's gives the key to convert it into the regular files. However in steganographic file system the data / information is hidden in regular files so the attacker is not able to even know that any secret message is hidden in the file.

The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients. The disadvantage of proposed algorithm is that to provide security on few buts/bytes, lots of processing is required on both sender and receiver side.

5. Conclusion

One can use the Cryptographic - encryption and decryption technique for providing security to the information being transmitted over the network. Also we have to take care that only cryptographic techniques cannot provide absolute safety to the information. By using Steganography for the transmitting the critical information over the network, we can increase one more security level to the information. By using the model proposed in the paper, combination of the Cryptography and the Steganography will offer the enhanced security on the critical information being transmitted over the network.

References

1. http://en.wikipedia.org/wiki/Steganography, [date: 11/06/2009]
2. William Stalling, Cryptography and Network Security 3rd edition (page 66), Prentice Hall 2005
3. http://www.bookrags.com/wiki/Steganography, [date:13/06/2009]
4. Kefa Rabah., Department of Physics, Eastern Mediterranean University, Gazimagusa, North Cyprus, via Mersin 10, Turkey. http://www.scialert.net/qredirect.php?doi=itj.2004.245.269&linkid=pdf
5. W. Bender, D. Gruhl, N. Morimoto, A. Lu, Page 323, IBM System Gernel Vol. 35 NOS 3&4.