International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 2, 2013. ISSN: 2348-6600
Reference ID: IJCS-013 PAGE NO: 064-068

AUDIO STEGANOGRAPHY

D. Seetha [#1], Dr.P.Eswaran [*2]

[#1] Department of Computer science and Engineering,
Alagappa University, Karaikudi.
India.

[*2] Assistant Professor ,Department of Computer science and Engineering,
Alagappa University, Karaikudi.
India.

Abstract— **Steganography has been proposed as a new alternative technique to enforce data security. A perfect audioSteganographic technique aim at embedding data in an imperceptible, robust and secure way and then extracting it by authorized people. Hence, up to date the main challenge in digital audio steganography is to obtain robust high capacity steganographic systems. Leaning towards designing a system that ensures high capacity or robustness and security of embedded data has led to great diversity in the existing steganographic techniques. In this paper, we present a methods of audio steganography and how it works.**

Keywords: Steganography, information hiding, Parity coding, echo hiding , phase coding, spread spectrum

I. Introduction

Steganography is the art of passing information through original files in a manner that the existence of the message is unknown. The term steganography is arrived from Greek word means, "Covered Writing". The innocent files can be referred to as cover text, cover image, or cover audio as appropriate. After embedding the secret message it is referred to as stego-medium. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data. While cryptography is about protecting the content of messages (their meaning), steganography is about hiding the message so that intermediate persons cannot see the message. Steganography refers to information or a file that has been concealed inside a digital Picture, Video or Audio file.

Its primary goal is to hide the fact that a communication is taking place between two parties. The sender embeds secret data of any type using a key in a digital cover file to produce a stego file, in such a way that an observer cannot detect the existence of the hidden message .

At the other end, the receiver processes the received stego-file to extract the hidden message. An example of audio steganography is depicted in Fig. 1 where the cover file being used is a digital audio signal. An obvious application is a covert communication using innocuous cover audio signal, such as telephone or video conference conversations.

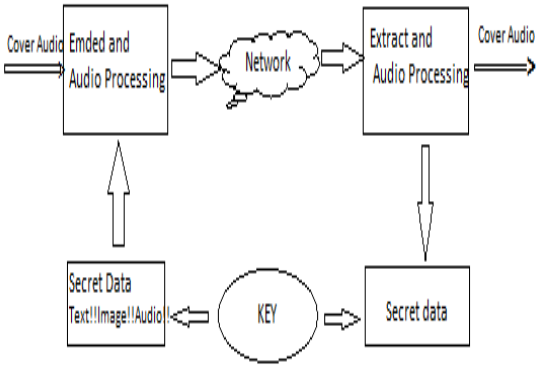

Fig. 1: Blocks diagram for audio steganography.

Steganography takes the opposite approach and attempts to hide all evidence that communication is taking place. Essentially, the information-hiding process in a Steganographic system starts by identifying a cover medium's redundant bits (those that can be modifie without destroying that medium's integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message.

II. INFORMATION-HIDING SYSTEM FEATURES

An information-hiding system is characterized be having three different aspects that contend with each other as shown in Figure 2: capacity, security, and

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 2, 2013. ISSN: 2348-6600
Reference ID: IJCS-013 PAGE NO: 064-068

robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information .

Generally speaking, information hiding relates to both watermarking and steganography. A watermarking system's primary goal is to achieve a high level of robustness-that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity, which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it.

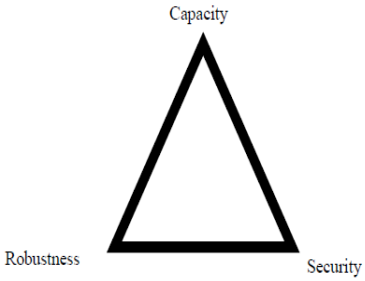

Figure 2:Information Hiding Features

Steganography System

A classical steganographic system's security relies on the encoding system's secrecy. Although such a system might work for a time, once it is known, it is simple enough to expose the entire received media (e.g., images) passing by to check for hidden messages ultimately, such a steganographic system fails.

Modern steganographic system, as shown in Figure 3 attempts to be detectable only if secret information is known namely, a secret key. In this case, cryptography should be involved, which holds that a cryptographic system's security should rely solely on the key material. For steganography to remain undetected, the unmodified cover medium must be kept secret, because if it is exposed, a comparison between the cover and stego media immediately reveals the changes .

Three basic types of stego systems are available:

- Pure stego systems - no key is used.
- Secret-key stego systems - secret key is used.
- Public-key stego systems - public key is used.

The technique that is followed in this paper will use secret key to encrypt the hidden message that will be encapsulated inside a cover media.

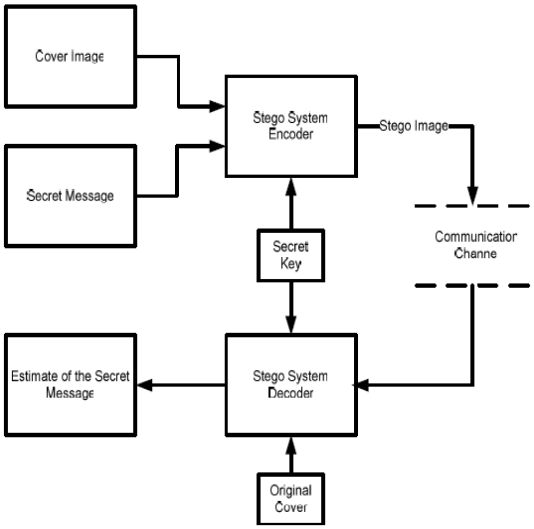

Figure 3: A Modern Steganography System

Steganalysis

Steganalysis is a relatively new research discipline with few articles appearing before the late-1990s. Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes". It is the art of discovering and rendering useless covert messages. The goal of steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information.

The challenge of steganalysis is that:

1. The suspect information stream, such as a signal or a file, may or may not have hidden data encoded into them.
2. The hidden data, if any, may have been encrypted before being inserted into the signal or file.
3. Some of the suspect signal or file may have noise or irrelevant data encoded into them (which can make analysis very time Consuming).
4. Unless it is possible to fully recover, decrypt and inspect the hidden data, often one has only a suspect information stream and cannot be sure that it is being used for transporting secret information.

III. TYPES OF ATTACKS

Attacks and analysis on hidden information may take several forms: detecting, extracting, and disabling, destroying or modifying hidden information. An attack approach is dependent on what information is available to the steganalyst (the person who is attempting to detect steganography-based information streams). The possible attacks on a stego media can be one of the following:

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 2, 2013. ISSN: 2348-6600
Reference ID: IJCS-013 PAGE NO: 064-068

1. Steganography-only attack: Only the steganography medium is available for analysis.
2. Known-carrier attack: The carrier, that is, the original cover, and steganography media are both available for analysis.
3. Known-message attack: The hidden message is known.
4. Chosen-steganography attack: The steganography medium and tool (or algorithm) are both known.
5. Chosen-message attack: A known message and steganography tool (or algorithm) are used to create steganography media for future analysis and comparison. The goal in this attack is to determine corresponding patterns in the steganography medium that may point to the use of specific steganography tools or algorithms.reserved.
6. Known-steganography attack: The carrier and steganography medium, as well as the steganography tool or algorithm, are known.

IV. AUDIO STEGONOGRAPHY:

The basic model of Audio steganography consists of Carrier (Audio file), Message and Password.
Carrier is also known as a cover-file, which conceals the secret information.
Basically, the model for steganography is shown in Fig 4.
Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

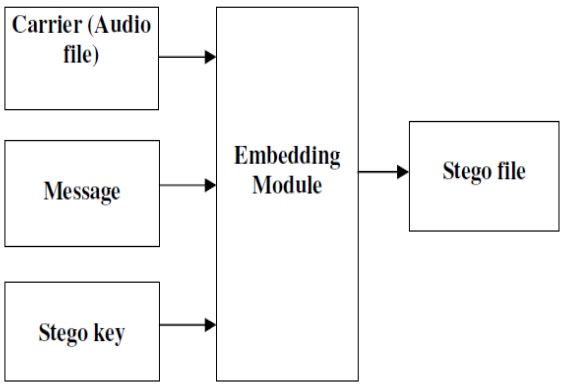

Figure 4 Basic Audio Steganographic Model.

Steps for Data Embedding:
1. Read the cover audio signal.
2. Write the text in an in file to be embedded. Convert it into a sequence of binary bits.
3. Every message bit from step 2 is embedded into the variable and multiple LSBs of the samples of the digitized cover audio cover.
4. For embedding purpose, the MSB of the cover sample is checked. As shown in above table.

If MSB is „0" then use 6 LSBs for data embedding.
If MSB is „1" then use 7 LSBs for data embedding.
5. The modified cover audio samples are then written to the file forming the stego object.

Steps for Data Retrieval:

1. Read the stego object.
2. Retrieval of message bits is done by checking the MSB of the samples.

If MSB is „0" then use 6 LSBs for data retrieve.
If MSB is „1" then use 7 LSBs for data retrieve.
3. After every such 16 messages bits retrieved, they are converted into their decimal equivalents and finally the secret audio signal reconstructed.
Process :

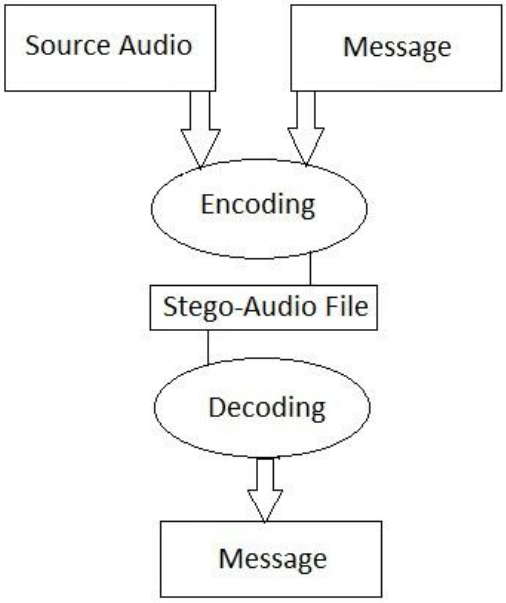

Figure 5 Process of audio steganography

V. AUDIO STEGANOGRAPHIC METHODS

There have been many techniques for hiding information or messages in audio in such a manner that the alterations made to the audio file are perceptually indiscemible.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 2, 2013. ISSN: 2348-6600
Reference ID: IJCS-013 PAGE NO: 064-068

LSB CODING

A very popular methodology is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. That's usually an effective technique in cases where the LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps.

In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.

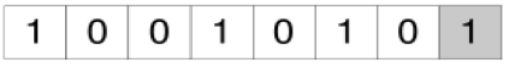

Figure 4: Binary representation of decimal 149

PARITY CODING

Parity coding is one of the robust audio steganographic techniques. Instead of breaking a signal into individual samples, this method breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit.

PHASE CODING

The phase coding technique works by replacing the phase of an initial audio segment with a reference phase that represents the secret information. The remaining segments phase is adjusted in order to preserve the relative phase between segments. In terms of signal to noise ratio, Phase coding is one of the most effective coding methods. When there is a drastic change in the phase relation between each frequency component, noticeable phase dispersion will occur. However, as long as the modification of the phase is sufficiently small, an inaudible coding can be achieved.

SPREAD SPECTRUM

In audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal. This is similar to a system which uses an implementation of the LSB that spreads the message bits randomly over the entire sound file. However, unlike LSB coding, the Spread Spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which is independent of the actual signal . As a result, the final signal occupies a bandwidth which is more than what is actually required for transmission.

The Spread Spectrum method is capable of contributing a better performance in some areas compared to LSB coding, phase coding, and parity coding techniques in that it offers a moderate data transmission rate and high level of robustness against removal techniques. However, the Spread Spectrum method has one main disadvantage that it can introduce noise into a sound file .

ECHO HIDING

Echo hiding technique embeds secret information in a sound file by introducing an echo into the discrete signal. Echo hiding has advantages of providing a high data transmission rate and superior robustness when compared to other methods. Only one bit of secret information could be encoded if only one echo was produced from the original signal. Hence, before the encoding process begins the original signal is broken down into blocks. Once the encoding process is done, the blocks are concatenated back together to create the final signal .

VI. PROPOSED WORK

Here we will discuss the limitation of the previous procedure and how those are different with present method. There are two main disadvantages associated with the use of methods like parity coding. The human ear is very sensitive and can often detect even the slightest bit of noise introduced into a sound file, although the parity coding method does come much closer to making the introduced noise inaudible. Another problem is robustness. One disadvantage associated with phase coding is a low data transmission rate due to the fact that the secret message is encoded in the first signal segment only. Phase coding method is used when only a small amount of data needs to be considered. Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. Among many different data hiding techniques proposed to embed secret message within audio file, the LSB data hiding technique is one of the simplest methods for inserting data into digital signals in noise free environments, which merely embeds secret message-bits in a subset of the LSB planes of the audio stream. The following steps are: a. Receives the audio file in the form of bytes and converted in to bit pattern. b. Each character in the message is converted in bit pattern. c. Replaces the LSB bit from audio with LSB bit from character in the message. This proposed system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. In fig 7. we can see the spectrogram of cover audio signal and stego audio signal.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 2, 2013. ISSN: 2348-6600
Reference ID: IJCS-013 PAGE NO: 064-068

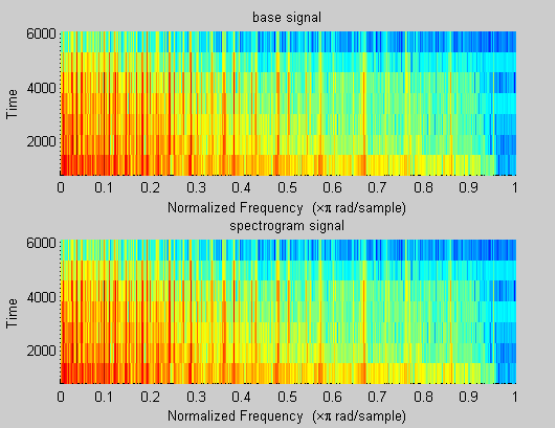

Fig .7 spectrogram of cover audio signal and stego audio signal

VII. CONCLUSION

An effective audio steganographic scheme should possess the following three characteristics: Inaudibility of distortion (Perceptual Transparency), Data Rate (Capacity) and Robustness. These characteristics (requirements) are called the magic triangle for data hiding .

This method of LSB modification of Steganography is the least secure. This method's security lies on the presumption that no other parties are aware of this secret message. This method is easy to implement but is very susceptible to data loss due to channel noise and re-sampling.

Disadvantages associated with phase coding are a low data transmission rate due to the fact that the secret message is encoded in the first signal segment only and to extract the secret message from the sound file, the receiver must know the segment length. As a result, this method can be used when only a small amount of data needs to be concealed. Otherwise this can be proved as a good method for audio Steganography.

References:

[1] Vijay Kumar Sharma, 2vishal Shrivastava,"A Steganography Algorithm For Hiding Image In Image By Improved LSB Substitution By Minimize Detection "Journal Of Theoretical And Applied Information Technology 15th February 2012. Vol. 36 No.1

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

[3] Prof.SamirKumar,BandyopadhyayBarnali, Gupta Banik,"LSB Modification and Phase Encoding Technique of Audio Steganography Revisited", *International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012.*

[4] Swati Malviya, Manish Saxena "Audio Steganography in a Nutshell", International Journal of Electronics Communication and Computer Technology (IJECCT) Volume 2 Issue 5 (September 2012).

[5] Swati Malviya, Manish Saxena, Dr. Anubhuti Khare," Audio Steganography by Different Methods ",International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, July 2012)

Published by SK Research Group of Companies (SKRGC).