Vandana Publications

Volume-4, Issue-3, June-2014, ISSN No.: 2250-0758

International Journal of Engineering and Management Research

Available at: www.ijemr.net

Page Number: 154-156

Methods of Audio Steganography

Megha[1], Mahesh singh[2]

[1,2]Advanced Institute of Technology and Management, Palwal, INDIA

ABSTRACT

A steganography is a new kind of secret communication used mainly to hide secret data inside other innocent digital mediums. Audio files and signals make appropriate mediums for steganography due to the high data transmission rate and the high level of redundancy. Hiding data in real time communication audio signals is not a simple mission. Steganography requirements as well as real time communication requirements are supposed to be met in order to construct a useful data hiding application. In this paper we will describe various audio steganography techniques. These techniques will be evaluated both, steganography and real time communication requirements.

Keywords: audio steganography, data hiding , LSB,Real time communication, , signal processing.

I. INTRODUCTION

Steganography has a long history been used to protect the secrete data. A cryptography is a technique to protect the secure data by jumbling its content, while steganography is a technique to protect the secret data by concealing its mere existence.the concealment is achieved by embedding them into other seemingly-innocent host mediums.

Steganography can hide different types of data within a cover medium,the resultant stego message contain the secrete data.this method basically exploits the human observation and awareness of detecting the seek files that containing the secrete data, while tere are many third party programs can do that is called Steganalysis. Steganalysis, the inverse of steganography, is a method of detecting the seek file containing secrete data. In short the steganalysis analyse and break the steganography system.

A steganography is efficient where cryptography is inefficient.

A text steganography is supposed to be the hardest steganography due to the low redundancy of text compare to image, audio and video.

II. METHODOLOGY

2.1 *STRUCTURE OF STEGANOGRAPHY*

Various terminology used in steganography are:

1.emb(m):some information data or signal hidden in other medium.

2.steg(s):output of signal,data or file that has embedded the secrete message in it.

3.cover(c): The input to the information hiding process which represents the innocent carrier signal or file.

4.stego key(k): This is additional unembedded secret data which may be needed in the information hiding process.

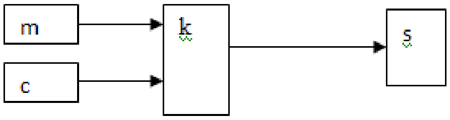

Figure 1: Terminology of steganography/encoding phase

In general, steganographic system consists of embedding or encoding phase and extracting or decoding phase. The embedding process is accomplished by encoding or embedding the secret message into a covert innocent message using a stego key. The result of this process is the stego message which contains both cover and secret messages combined according to the stego key. On the other hand, the decoding phase requires having the same stego key in order to be able to extract the embedded secret data from the stego message. In most steganography techniques, failing to have the stego key will make the process of extracting the secret message almost impossible.

Encoding phase: this phase includes embedding the secrete data using a stego-key(k) and the resultant is a steg message.

Extracting phase: this phase includes decoding a steg-message (embedding a secrete message) using the same stego-key(k)

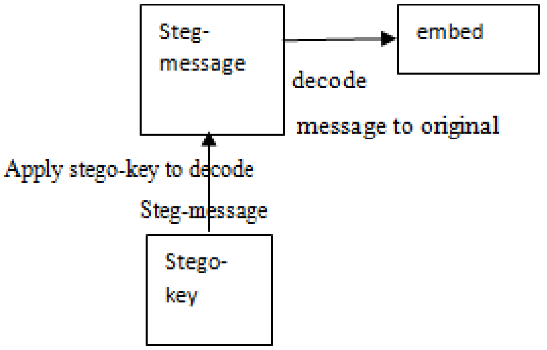

Figure 2: Extracting phase

III. PRIOR APPROACH

Communication security and robustness are vital for transmitting important information to authorized entities while denying access to not permitted ones. By embedding secret information using an audio signal as a cover medium, the very existence of secret information is hidden away during communication.

This is a serious and vital issue in some applications such as battlefield communications and banking transactions

The secret message is concealed into the audio media by slightly changing the binary sequence of the audio file.

Hiding secret information into digital audio media is generally more complicated than hiding secret information into other media, such as digital images. In order to hide secret information successfully, a range of techniques for inserting information into digital audio have been introduced. These techniques vary from simple ones that embed information as signal noises to more powerful ones that take advantage of complicated signal processing techniques to embed the secret message.

3.1 DIGITAL AUDIO SIGNAL

Digital audio signals are different from other traditional analogue sounds in the fact that they are discrete signal rather than continuous ones. Discrete signals are produced by sampling continuous analogue signals at specific rates. For instance, the typical sampling rate for CD digital audio is 44 kHz.

Typical sampling rate is generally set at a level in which the produced discrete signal is not imperceptibly distinguishable from the original continuous signal. Digital audio files are stored in computers as a series of 0's and 1's. With a correct tool, it is possible to change the bits that structure a digital audio file. Such accurate controls permit changes to be performed to the binary bits that are not perceptible to the human sense.

IV. OUR APPROACH

There are many steganographic techniques for hiding secret data or messages in audio in a way that the modifications made to the audio file are perceptually indiscernible. Several recent methods necessitate previous familiarity with signal processing techniques, Fourier transform, and other high level mathematics areas.

4.1 METHODS OF AUDIO STEGANOGRAPHY

1. ***least significant bit (lsb) coding:***

This is a simplest method to embed a secrete data behind a digital audio media.In this method least significant bit of sample word is replaced by least significant bit of secrete data.this method can embed large size of data.

For example: Here the secret information is “Hi” and the cover file is an audio file. “Hi” is to be embedded inside the audio file. First the secret information “Hi” and the audio file are converted into bit stream. The least significant column of the audio file is replaced by the bit stream of secret information “Hi”. The resulting file after embedding secret information “Hi” is called Stego-file.

It is possible to encode messages using frequencies that are inaudible to the human ear. Using any frequencies above 20.000 Hz, messages can be hidden inside sound files and will not be detected by human checks.

2. ***Parity coding***

In parity coding, audio signal is broken down into separate areas of samples and hide the secret message in the parity bit of each sample area. If the parity bit of a sample area does not match the secret message bit to be embedded, the LSB of one of the samples in the area is inverted. Therefore, this will give a wider range of choices on where to hide the secret bit, and will keep the change in the signal more unobservable.

3. ***Phase coding***

Phase coding is based on the reality that, unlike noises, audio phase components are imperceptible to the human ear. Rather than adding noises, this technique encodes the secret data bits to phase shifts in the phase spectrum of the audio signal, attaining inaudible encodings in terms of signal-to-noise ratio.

In phase coding, the phase of an initial audio segment is substituted with a reference phase that represents the data.

Following segments phase is modified back to maintain the relative phase between segments. Phase coding, when applicable, is one of the most efficient audio steganographic methods in terms of the signal to noise ratio (SNR). When the phase relation between each frequency component is dramatically changed, noticeable phase dispersion will occur. On the other hand, on condition that the alteration of the phase is small enough, an inaudible steganography can be accomplished.

4. ***Spread spectrum coding***

This is equivalent to implementing LSB coding by spreading the secret data bits over the entire audio signal. However, different from LSB coding, the SS techniques spread the secret bits over the frequency spectrum of the audio media by using a code that is not reliant on the genuine signal. Consequently, the resultant signal will utilize a bandwidth wider than what is essentially needed for communication.

Two types of spread spectrum are used in SS audio steganography:

- Direct spread spectrum: the secret data is distributed using a constant named the chip rate then adapted with a pseudorandom signal and then interleave with the cover signal.
- Frequency hoping spread spectrum: the frequency spectrum of the audio medium is changed so that it hops quickly among frequencies.

5. Echo hiding

In echo hiding techniques, secret data is inserted into an audio medium by introducing an echo into the discrete signal. It allows high data communication rates and offers greater robustness.

In order to hide secret message effectively, three echo related factors are involved and changed:

Amplitude, decay rate, and offset (delay time) from the genuine audio signal. All of those factors should be set lower than the human hearing threshold in order to keep the echo imperceptible. Additionally, offset values are changed corresponding to the binary secret data targeted. A specific offset value represents a binary one, and another offset value represents a binary zero.

V. CONCLUSION

This paper includes various methods of real time audio steganography techniques. These techniques make data hiding obtainable and accessible. While a degree of success has been achieved, each technique has its limitations. The ultimate goal of attaining protection of large amounts of secret data against deliberate attempts at removal may be still far from being obtained, but the five techniques discussed above offer numerous choices and make this data hiding technology more obtainable and accessible. Although some data hiding techniques have been proposed by various researchers, the specific requirements of each data hiding technique vary from one application to another; with each of these techniques have some advantages and disadvantages. The flexible nature of audio formats, signals and files, is what makes them good and practical medium for steganography. Another aspect of audio steganography that makes it so attractive and promising is the ability to combine steganography techniques with existing cryptography technologies. We do not have to depend on one technique only. Secret data not only can be encrypted, they can be hidden and encrypted at the same time

REFERENCES

[1] Mazurczyk, W. and K. Szczypiorski, "Covert Channels in SIP for VoIP Signalling", in Global E-Security, H.Jahankhani, K. Revett, and D. Palmer-Brown, Editors. 2008, Springer Berlin Heidelberg. p. 65-72.

[2] Hui, T., et al. "An M-Sequence Based Steganography Model for Voice over IP". in Communications, 2009. ICC09. IEEE International Conference on. 2009.

[3] Tian, H., et al., "A Covert Communication Model Based on Least Significant Bits Steganography in Voice over IP", in Proceedings of the 2008 The 9th International Conference for Young Computer Scientists. 2008, IEEE Computer Society. p. 647-652.

[4] Nutzinger, M., C. Fabian, and M. Marschalek. Secure Hybrid Spread Spectrum System for Steganography in Auditive Media. in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on. 2010.

[5] Petitcolas, F.A.P., R.J. Anderson, and M.G. Kuhn, Information hiding-a survey. Proceedings of the IEEE,1999. 87(7): p. 1062-1078.

[6] Currie, D.L. and C.E. Irvine, 1996. Surmounting the effects of lossy compression on steganography. Proceedings of the19th National Information Systems Security Conference, Oct. 22-25, Baltimore, Maryland, pp: 194-201

[7] Anderson, R.J. and F.A.P. Petitcolas, On the limits of steganography. Selected Areas in Communications, IEEEJournal on, 1998. 16(4): p. 474-481.