

Survey on Techniques for Steganography of Audio Files

Charu Arora¹, Nitish Anand²

¹Assistant Professor, ²Student,
IT department, MSIT
New Delhi, India

Abstract— The rise and development of multimedia and digital information has made communication easier and quicker. However with digital information, comes a responsibility to communicate securely and effectively. As digital information is easy to distribute and alter, therefore it is prone to various attacks and threats. Various security measures are taken while dealing with digital information. Audio Steganography is one such method to communicate securely. In this paper we will study and analyse various techniques of Audio Steganography

Keywords— Steganography, security, communication, digital information, LSB (Least significant bit).

I. INTRODUCTION

Audio Steganography is the technique of hiding covert data or message in audio files, which act as an envelope for the data to be transmitted. The data is transmitted in such a way that no one can detect the presence of any hidden data or message except for the authorized receiver. Fig. 1 demonstrates the process

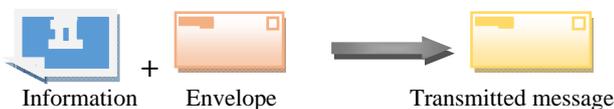


Fig. 1. Steganography process

The advantage of this technique is that, as the detection of hidden data or message is not possible by others, so the audio files or the covering media is less prone to attacks and interceptions. Thus the sender in this case transmits the data stealthily and effectively. There are various techniques known for audio steganography. Here in this paper we will be discussing the following ones.

1. LSB
2. PHASE CODING
3. ECHO HIDING
4. SPREAD SPECTRUM
5. PARITY ENCODING

II. VARIOUS TECHNIQUES FOR STEGANOGRAPHY

A. LSB

This technique is one of the easiest techniques for hiding data in audio files. Due to its simple algorithm it is one the most widely used Steganography technique. In this

technique the LSB of the audio signal is changed to the message bits. This small change in bits of audio data is not perceivable by humans. Samples of the audio signals are taken, each sample of 16 bits. Then the LSB of 8 consecutive such samples are replaced with the 8 bits of each character of the message to be hidden. The LSBs are the extracted by the receiver for reconstruction of the message.

B. Phase Coding

Due to the fact that the human auditory system does not perceive phase changes as easily as noise, phase coding comes out to be an important technique for steganography. In this technique the message bits are encoded as phase shifts in the phase spectrum, hence an inaudible encoding in terms of signal to-perceived noise ratio is achieved.

C. Echo Data Hiding

Text can be embedded in audio data by introducing an echo. The information is then hidden by varying physical quantities of the echo: initial amplitude, offset and decay rate. This method uses various complex algorithms making it one of the toughest method for data hiding. This technique relies on the fact that if offset is shorter or if the initial amplitude or decay rate is below the audible level of human ears then an unperceivable echo can be produced. In this method the original signal is divided into various blocks for encoding, and then after encoding the blocks are combined together to create the final message

D. Spread Spectrum

Unlike LSB technique, where only the LSBs of the audio signal get changed to the bits of the message data, here in spread spectrum technique the message is spread across the whole frequency spectrum of the audio signal. This is one of the most secure steganography techniques and hence has various military applications.

E. Parity Encoding

In this technique the signal is broken down into regions of samples instead of breaking it down into individual samples. Each message bit is encoded in a specific region's parity bit. If the message bit is different to the parity bit of the region the LSB of the sample region gets complemented. The hidden information is recovered without any error.

III. ANALYSIS OF TECHNIQUES

A. LSB

This algorithm is used where the security of the data is required, but not necessary. It acts as a good foundation for other steganography techniques. This technique is simple to implement and understand also it gives an advantage of higher channel Capacity. LSB has a major drawback that it lacks robustness and is very susceptible to loss of data.

B. Phase Coding

This algorithm works perfect when dealing with small amount of data and provides low noise levels. As this method uses the first segment only for encoding of the message, it provides low data transmission rate. In addition to that as the message is not spread over the signal, it leads to localized data which can be easily removed by an attacker with cropping.

C. Echo Data Hiding

This algorithm offers very high level of robustness and provides very high data transmission rate. The drawback of this algorithm is that it is complex to implement, being a more sophisticated algorithm for providing security

D. Spread Spectrum

This algorithm gives an advantage of high level of robustness while also keeping a moderate data transmission rate. This algorithm falls behind echo data hiding on the fact that this method induces noise in the audio signal.1.

E. Parity Encoding

Like LSB this is one of the easiest methods for steganography but due to flipping of the bits, it is quite susceptible to errors.

IV. CONCLUSION

Audio steganography has various applications where data security is required. For example, in defence, for protecting intellectual property. The extent of application is unimaginable. Every user wanting security with the help of audio steganography can use the above discussed techniques based on his requirements. Each method has its pros and cons and can be suited for different scenarios. The level of security the user wants, the level of difficulty of implementation, the hiding capacity, all such factors decide the selection of the technique to be used.

REFERENCES

- [1] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.
- [2] Sridevi R., Damodaram A., SVL.Narasimham, Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security, Journal of Theoretical and Applied Information Technology, 2009. and K.H. Hofmann, 1967. Compact semitopological semigroups and weakly almost periodic functions. Lecture Notes in Mathematics, No. 42, Springer-Verlag, Berlin-New York.
- [3] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, An introduction to steganography methods, World Applied Programming, Vol (1), No (3), August 2011. 191-195.
- [4] Bender W, Gruhl D & Morimoto N (1996) Techniques for data hiding. IBM Systems Journal 35(3): p 313-33
- [5] S.S. Divya, M. Ram Mohan Reddy, Hiding text in audio using multiple lsb steganography and provide security using cryptography. International Journal Of Scientific & Technology Research Volume 1, Issue 6, 6 July 2012.
- [6] Methods Of Audio Steganography, <http://www.snotmonkey.com/work/school/405/methods.html#echo>
- [7] Ajay.B.Gadicha1, Audio Wave Steganography, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1 issue-5.