

Enhanced Audio Steganography System (EASS)

Ankit Shelar¹ Shailesh Hadkar² Jueli Paygude³ Sagar Keluskar⁴ Mrs. Prachi Kshirsagar⁵

^{1,2,3,4,5}Department of Information Technology

^{1,2,3,4,5}Mumbai University, Padmabhushan Vasantdada Patil Pratishthan's College of Engineering
Sion, Chunabhatti, Mumbai – 400022

Abstract— Steganography is an art and science of hiding information by embedding messages into media files (image, audio, and video) for secure message transmission. EASS (Enhanced Audio Steganography System) is a system that sends secret information through audio in a secured way. This software takes information from user embed this information into audio and sends that audio to other user via LAN. The wav Audio format is used to send information. Advanced LSB algorithm is used for embedding information into audio file. It is concerned with embedding information in an innocuous cover Speech in a secure and robust manner. This system makes the Files more secure by using the concepts Steganography and Cryptography.

Key words: Steganography, Cryptography, Data Security, LSB algorithm, embedding

I. INTRODUCTION

In this era of modern computing, data security is crucial and also need of the hour for all organizations as well as in defense. Steganography is the art of hiding messages inside other messages such that the very existence of the message is unknown to third party. The goal of cryptography is to make data unreadable by a third party, the goal of stenography is to hide the data from a third party Through the use of advanced computer software, authors of images and software can place a hidden trademark in their product, allowing them to keep a check on piracy. Cryptography is one option to send message secretly. But when we convert plain text into cipher text then intruder comes to know something important message is there in cipher text and then he tries to break that cipher text. Intruders may leak the information to others manipulate it to misinterpret as well as to misrepresent an individual or organization. Steganography is one of the solutions to overcome this problem by making intruder believe that there is no useful information.

In this paper we described EASS for secure data transmission.

It is useful in following sectors:

- Chemical companies.
- Military.
- Corporate industries.

This document is intended for description of existing system, proposed system and challenges in current Audio Steganography tools.

II. EXISTING SYSTEM

LSB algorithm is one of the most easiest and secured algorithm in audio Steganography. By modifying the least significant of several bytes of an audio file, only minor changes occur in the original sound, most of which cannot be distinguished by the human auditory system. We make use wav files to hide the message since it can be edited and manipulated with ease relatively.

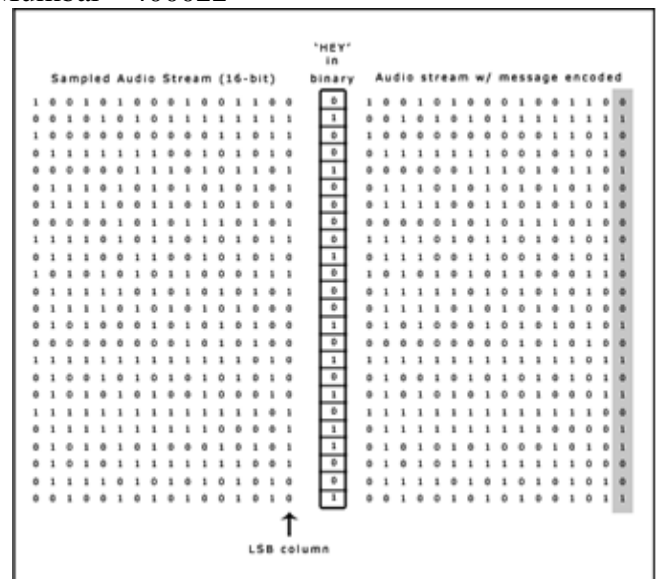


Fig. 1: Message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method

.Wav files make use of either 8 or 16 bits to store sound information. 8 bit files allow values of sound in the range between 0 and 255 and the 16 bit files will have values from 0 to 65535. By changing the values of bytes slightly, we can store our secret data. If for example, we have 8 byte sample of wav audio: 200 234 157 141 these values would be represented in binary as:

11001000 11101010 10011101 10001101

Suppose we want to hide the binary file 1110 (14) inside this sequence. We replace the least significant bit in each byte of wave sample (the least significant bit because it will cause the least amount of change in the value) by bits of the binary form that makes up 14. The sequence of binary after modifying wav by stuffing 14 is shown below:

11001001 11101011 10011101 10001100

To increase the storage capacity another approach is to add message bits in higher LSB layers (4th and 5th LSB layer). It is shown as below,

A. *Before Embedding:*

Sample bits are: 00101111

Target layers are 4th and 5th and message bits are 0 and 1.

B. *After Embedding:*

Sample bits are: 00110111

III. PROPOSED SYSTEM

In Proposed system, the data to be transferred is initially encrypted followed by transferring of the embedded file in audio format thus increasing security of the system. The system allows embedding large amount of data with reduction in glitches. System allows transferring of data when connected to LAN. Also system provides with secured

and more efficient database storage which consists of encrypted audio files.

The system architecture is as follows,

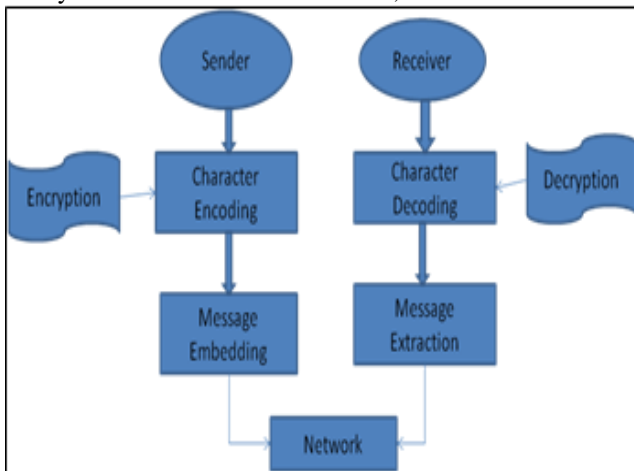


Fig. 2: System Architecture

A wav audio file is first of all divided into segments of 8 bits. Then a particular pattern is selected.

For Eg. Consider an audio segment
11001000 11101010 10011101 10001101
200 234 157 141

– Message bits: 1100

And pattern is 1324

That means,

1st bit of message is stored in 1st LSB layer of 1st segment

Then first segment becomes,

11001001=201

2nd bit of message is stored in 3rd LSB layer of 2nd segment

Then second segment becomes,

11101110=238

3rd bit of message is stored in 2nd LSB layer of 3rd segment

Then third segment becomes,

10011101=157

4th bit of message is stored in 4th LSB layer of 4th segment

Then fourth segment becomes,

10000101=133

As we can see that there is large difference between values of 2nd and 3rd segments before embedding and values of 2nd and 3rd segments after embedding. So to minimize this difference we have introduced an adjustment step for 3rd and 4th LSB layer.

It is shown as below,

2nd segment is,

11101110=238

Now adjust remaining LSB layers in such a way that difference will get minimized

After adjustment,

11101100=236

236 is more closer to 234 hence we can say that noise is reduced.

Similarly, for 4th segment,

10000101=133

After adjustment,

10000111=135

IV. APPLICATION

The System can be used whenever an individual wants to hide data to prevent unauthorized person from becoming aware of the existence secret data. In the business world Audio data hiding can be used to hide a secret chemical formula or plan for a new invention. Audio data hiding can also be used in the non-commercial sector to hide information that someone wants to keep private. It can also be used in forensic applications for inserting hidden data into audio files for the authentication of spoken words and other sounds, and in the music business for the monitoring of the songs over broadcast radio.

V. CONCLUSION

We can say that the existing system is less secured as information is not encrypted and directly embedded into audio file. While new system is more secured as we are encrypting data before embedding. As we are developing more robust and secured system it can be used in chemical companies to send chemical formulas secretly as well as in military communication. A method of embedding information in the cepstral domain of a cover audio signal is described for audio steganography applications. The proposed technique combines the commonly employed psychoacoustical masking property of the human auditory system with the decorrelation property of the speech cepstrum, and achieves imperceptible embedding, large payload, and accurate data retrieval. Results of embedding using a clean and a noisy hot utterance show the embedded information is robust to additive noise and bandpass filtering.

VI. ACKNOWLEDGMENT

We would like to express our gratitude towards the professor Mrs. Prachi Kshirsagar for her guidance, help and constant encouragement through the various difficult stages while making this paper. We are also thankful to all those who directly or indirectly helped us in making this paper a reality.

REFERENCES

- [1] Padmashree G, Venugopala P S ,“Audio Stegnography and Cryptography: Using LSB algorithm at 4th and 5th LSB Layer” International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012
- [2] Ajay.B.Gadicha1, “Audio Wave Steganography”, and International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-1, Issue-5, and November 2011.
- [3] R Sridevi, Dr. A Damodaram, Dr. Svl.Narasimham, “Efficient Method Of Audio Steganography By Modified LSB Algorithm And Strong Encryption Key With Enhanced”, Journal of Theoretical and Applied Information Technology.
- [4] Swati Malviya, Manish Saxena, Dr. Anubhuti Khare,“Audio Steganography by Different Methods”, (ISSN 2250-2459, Volume 2, Issue 7, July 2012)