Data Concealing Using Audio Steganography

Harleen Kaur[1], **Meena Aggarwal**[2], **Amrinder Kaur**[3]
[1] AP (ECE Department), SBBSIET PADHIANA, India
[2] Student (M.Tech) NITTR Chandigarh, India
[3] AP (ECE Department) SBBSIET, India

Abstract:

Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. A perfect audio Steganographic 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. In this paper , the encoding and decoding of data is done using audio steganography techniques implemented in MATLAB.

Keywords: Audio Steganography, data hiding, Echo hiding. , LSB coding

I. INTRODUCTION

In our daily life, we communicate via various modes from one place to another and these involve the use of telephones, emails, fax etc. While sending and receiving the data through these modes, the main need of communicating through these modes is the security of the data being communicated. The techniques such as watermarking and encryption have already been used in this regard which makes no attempt to hide or disguise the hidden information. Therefore the main goal of steganography is make the information to be unsuspected by the human eyes or human ear i.e. it is used to prevent unauthorized persons from becoming aware of the existence of a message[2].

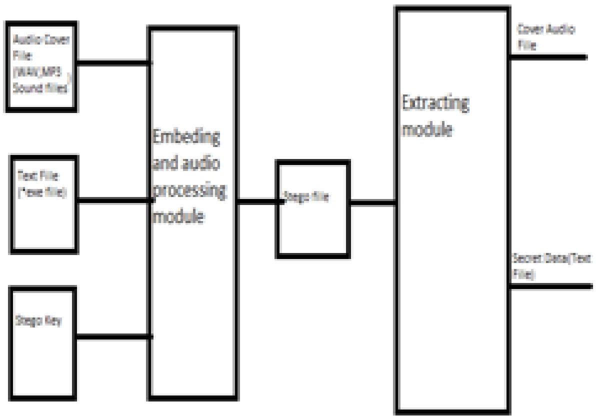


Fig. 1 Overview of Steganography

1.1 NEED OF STEGANOGRAPHY

Steganography becomes necessary as more people join the cyberspace revolution and they want their data to be transferred in a secure manner so that no one even knows that a message even exists.

Military communications system make increasing use of traffic security technique which, rather than merely concealing the content of a message using encryption, seek to even conceal its existence. Thus it becomes necessary to use a technique which even hides the existence of information.

1.2 STEGANOGRAPHY VERSUS CRYPTOGRAPHY

Though the aim of cryptography and steganography is to provide secret communication but steganography is not the same as cryptography. Cryptography hides the contents of a secret message from a malicious people, whereas steganography even conceals the existence of the message [1].

In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise the encoded message. Basically it offers the ability of transmitting information between persons in a way that prevents a third party from reading it.

In contrast, steganography does not alter the structure of the secret message, but hides it inside a audio cover so that it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists.

1.3 APPLICATIONS

There are many applications of digital audio steganography, including copyright protection, feature tagging, media forensic and secret communication.

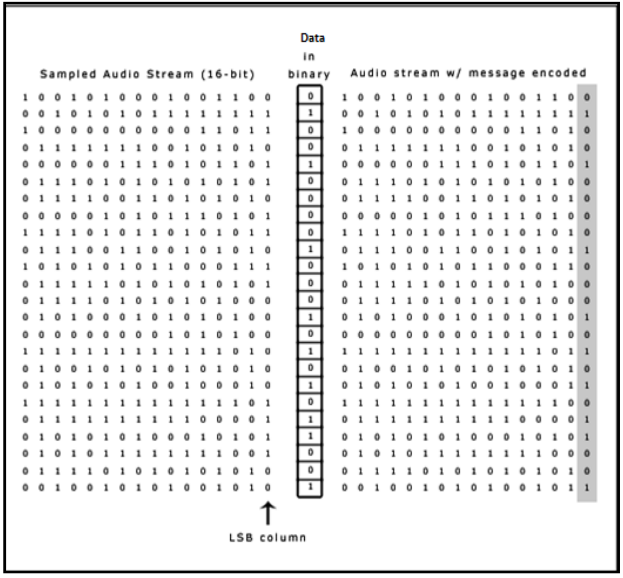
In feature tagging, captions, annotations, time stamps, and other descriptive elements can be embedded inside an audio signal. Copying the *stego–audio* also copies of the embedded features and only parties who possess the decoding *stego-key* will be able to extract and view the features.

II. TECHNIQUES OF STEGANOGRAPHY

The techniques for the implementation of steganography are basically divided in four domains: Temporal,domain,Frequencydomain,Wavelet domain and Codec domain. The various methods lying under these domains are discussed in the upcoming sections.

2.1 TEMPORAL DOMAIN

A. LSB Encoding: It is also known as Least Significant Bit Encoding. It is one of the earliest used methods for implementing steganography.In this technique the data to be hidden is embedded into the lower bits of the cover audio signal. The size of the data and the audio signal must be the same for e.g. for an 16kbps data signal 16khz audio signal is required.Though this technique is simple and easy to implement but it suffers from the disadvantage of low robustness and low security because in this an unauthorized person can easily extract the data hidden by completely removing the entire LSB of the cover audio. Figure 2.1 shows the implementation of LSB coding.



Sampled Audio Stream (16-bit)	Data in binary	Audio stream w/ message encoded
1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0	0	1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0
0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1	1	0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1
1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 1	0	1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0
0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0	0	0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0
0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1	1	0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1
0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1	0	0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 0
0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0	0	0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0
0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 1	0	0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 0
1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 1	0	1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 0
0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 0	1	0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 1
1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 1	0	1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 0
0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 1	0	0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 0
0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 0	0	0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 0
0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 0	1	0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 1
0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0	0	0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0
1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0	1	1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1
0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0	0	0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 0	1	0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1	0	1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0
0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1	1	0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1
0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1	1	0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1
0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 1	0	0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0
0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0	0	0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0
0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 0	1	0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 1

Fig. 2.1 Implementation of LSB Coding [6]

2.2. ECHO HIDING

In echo hiding, information is embedded in the audio cover file by introducing an echo into the discrete signal. One echo signal produced in the original signal embeds only one bit of information. Therefore in this original signal is split into blocks and echo's are inserted and these echo's then embed the information bits in them. When the encoding process is completed the blocks are then joined together to form the final signal.

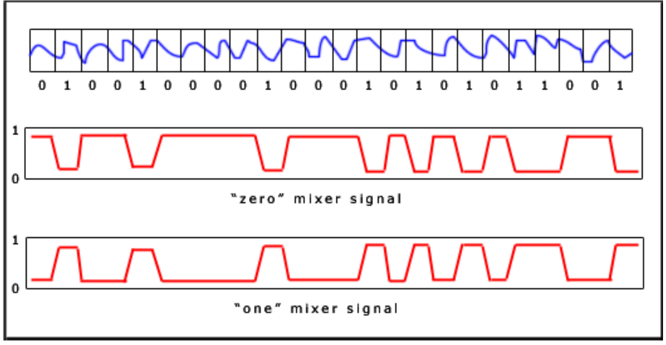


Fig. 2.2 Echo Hiding [6]

2.3 FREQUENCY DOMAIN

Phase Coding: The phase coding technique implements steganography by replacing the phase of an initial audio segment with a reference phase that represents the secret information. The phase of remaining segments is adjusted in order to preserve the relative phase between segments [4]. Figure 2.3 represents the phase coding implementation technique.

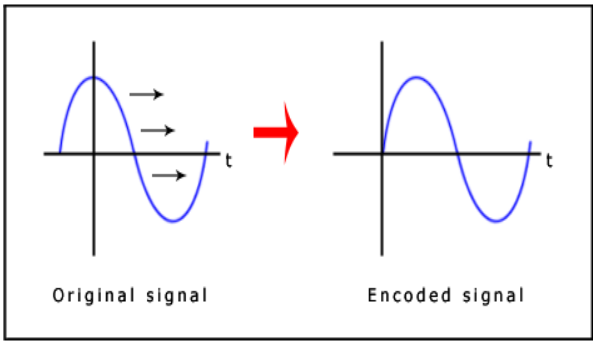


Fig. 2.3 Phase Coding Technique [6]

Spread Spectrum Coding

Spread Spectrum (SS) method tries to spread secret data 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. 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[4].

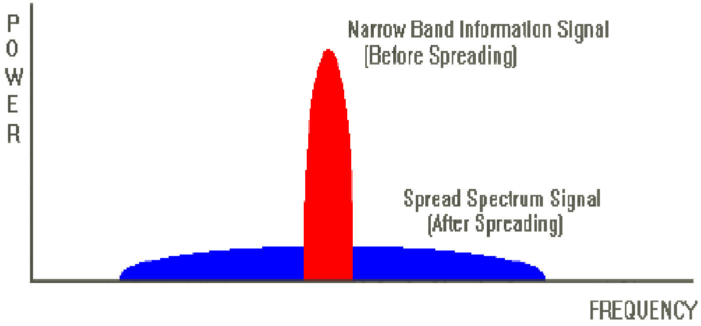
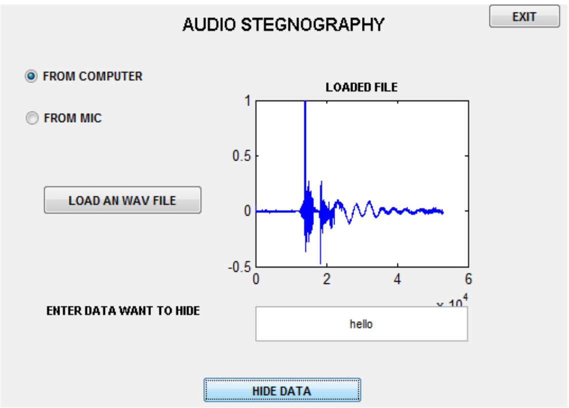


Fig. 2.4 Spread Spectrum Technique

III. SIMULATION RESULTS

3.1 Loading of wav file and Entering of Text to Hide

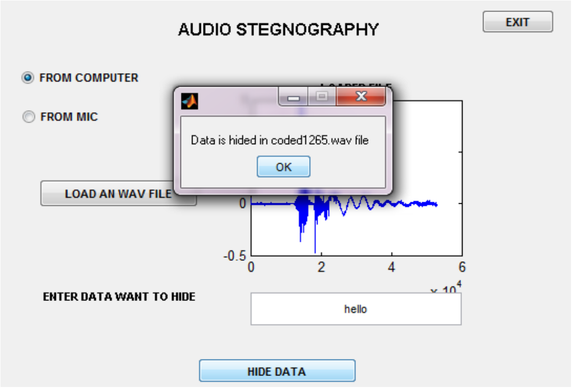
Here any wav file will be loaded and the text to be hidden is entered. The figure below will show the process:



● FROM COMPUTER
○ FROM MIC

ENTER DATA WANT TO HIDE: hello

by clicking "HIDE DATA" tab , the data hidden in the wav file is retrieved.



● FROM COMPUTER
○ FROM MIC

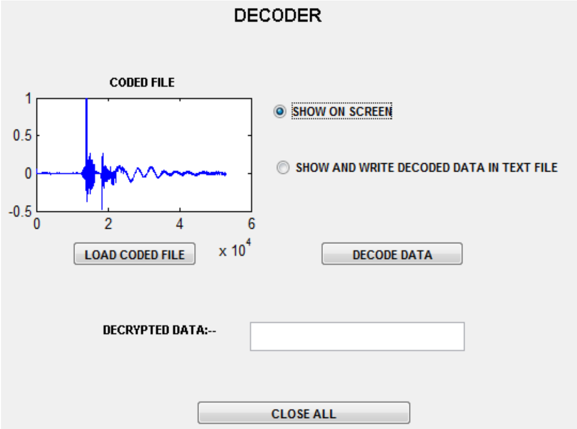
Data is hided in coded1265.wav file

ENTER DATA WANT TO HIDE: hello

3.2 Decoding of Hidden Data

Here the data is decoded by loading the code file. Then the option "show on screen" or "show and write the decoded data in a text file" will be selected.

For example the option "show on screen" is selected.

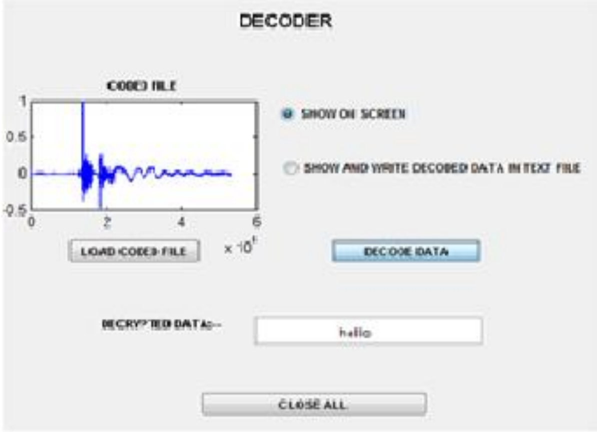


● SHOW ON SCREEN

○ SHOW AND WRITE DECODED DATA IN TEXT FILE

DECRYPTED DATA:--

Then the information is got back by by clicking on "DECODE DATA" tab as shown in fig below.



● SHOW ON SCREEN

○ SHOW AND WRITE DECODED DATA IN TEXT FILE

DECRYPTED DATA:-- hello

IV. CONCLUSION

Steganography techniques involving audio file formats appear to be increasing in popularity. To ensure digital information security, various techniques have been presented .

- Audio steganography, in particular, addresses issues related to the need to secure and preserve the integrity of data hidden in voice communications, even when the latter passes through insecure channels.
- The advantage on using one technique over another one depends strongly on the type of the application and its exigencies such as hiding capacity or the type of attacks that might encounter the transmitted signal.

REFRENCES

[1] Shahreza, S.S. and Shalmani, M.T. " High capacity error free wavelet domain speech steganography. ".IEEE International conference on Acoustics, Speech and Signal Processing. Pp. 1729-1732, Las Vegas,NV.

[2] M. L. Mat Kiah "A review of Audio based Steganography and digital watermarking."International Journal of the Physical Sciences Vol. 6(16), pp. 3837-3850, 18 August, 2011.

[3] Sos S. Agaian "Two Algorithms in Digital Audio Steganography Using Quantised Frequency Domain Embedding and Reversible Integer Transform ."Non-linear Signal Processing Lab, University of Texas at San Antonio, Texas 78249, USA.

[4] Poulami Dutta "Data Hiding in Audio Signal: A Review." International Journal of Database Theory and Application Vol. 2, No. 2, June 2009.

[5] Pierre Moulin Fellow "Data-Hiding CodesProceedings of the IEEE, VOL. 93, NO. 12, December 2010.

[6] Jayaram P "Information Hiding Using Audio Steganography" The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.