# Secure Data Transmission using Digital Audio as A Carrier

**Richa P Ganvir**
*UG Student*
*Department of Electronics Engineering*
*Smt Rajshree mulak college of engineering, Nagpur*

**Swati V likhar**
*UG Student*
*Department of Electronics Engineering*
*Smt Rajshree mulak college of engineering, Nagpur*

**Krupali Samrit**
*UG Student*
*Department of Electronics Engineering*
*Smt Rajshree mulak college of engineering, Nagpur*

**Swati pahune**
*Assistant Professor*
*Department of Electronics Engineering*
*Smt Rajshree mulak college of engineering, Nagpur*

## Abstract

Due to huge amount of information exchange in digital world, it is necessary to secure the information. The need for secured communication introduces the concept of steganography. Steganography the word itself indicates information inside information. The goal of steganographic system is to obtain secure and robust way to conceal a high rate of information. The secret information may be text, image and audio file. But there are different steganographic techniques available. So in this paper we focus on digital audio steganography which is an efficient way to hide data. We also going to review current digital audio steganographic techniques with respect to their robustness, security and hiding capacity. We are also going to explain the technique of digital audio steganography.

**Keywords: carrier file, cover media, steganography, Stego file, audio steganography**

## I. INTRODUCTION

In modern days, communication has become a main aspect of life. Now a day's numbers of devices are available for communication. But as the information transmits it should be secured. Mostly in internet, public network and wireless networks there is the issue of insecurity of data. The data can be made secured using cryptography, steganography and watermarking.

Steganography, cryptography and watermarking is used for same purpose that is protecting information. In steganography the existence of hidden message is unknown but in cryptography hidden message is converted into a different form. Cryptography protects the contents of a message whereas steganography protects the message and communication parties. Digital watermarking hides the information in a carrier signal the hidden information should, but does not need to contain a relation to the carrier signal.

Today computer and network technologies provide easy to use communication channels for steganography. It is a data hiding technique which aims at transmitting a message on a channel where some other kind of information is already being transmitted. The goal of steganography is to hide message inside the media in such a way that does not allow any 'enemy' to even detect and there is a secret message present.

The basic structure of steganography is made up of three components:-

1) The carrier media
2) The message
3) The key

The carrier media is the object which is used to carry the secret message. The secret message is the message which is to be kept secret. The key is the element used to decode the secret message at receiver side which is basically used for security purpose.

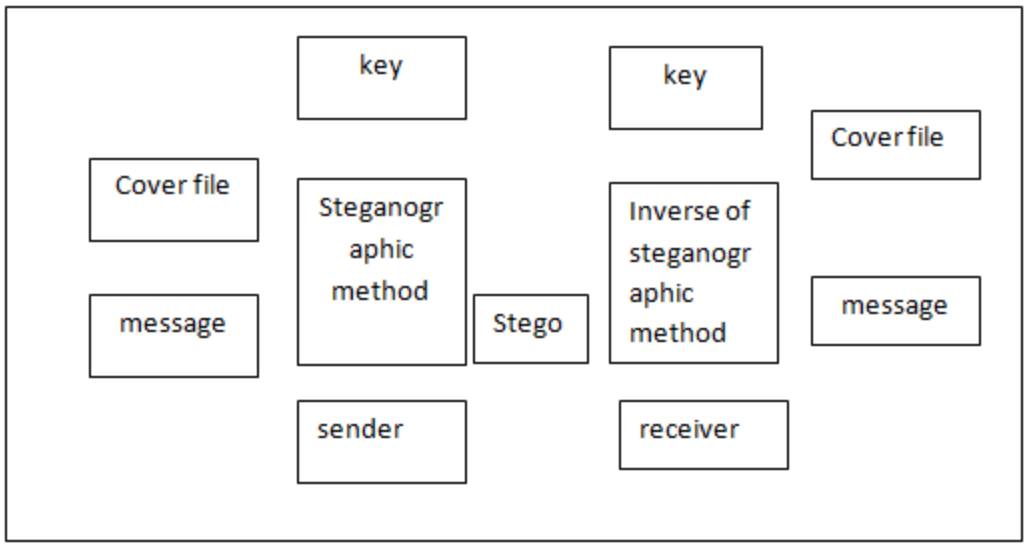


Fig. 1: Block diagram of steganography

## II. TYPES OF STEGANOGRAPHY

Steganography plays an important role with respect to the security of data. Steganography means a concealed writing. Here the secret object and the cover object May being any format. Steganography provides different ways to hide information as a secret message. The various techniques of steganography are:

1) Text Steganography
2) Image Steganography
3) Audio Steganography
4) Video Steganography

*1) Text Steganography:*

Steganography can be applied to text file i.e. if we hide information in text file it is called as text steganography. The general process of steganography i.e. preparing a Stego object that will not contain any change in the original file.

*2) Image Steganography:*

The image steganography is the process in which we hide the data within an image so that there will not be perceived change in the original image.

*3) Audio Steganography:*

Steganography is also applied to the audio file i.e, secret information is hidden under the cover object which is audio format this process is called audio steganography. The audio file should be undetectable.

*4) Video Steganography:*

Steganography using video files means that the data has to be hiding inside the video called as video steganography. The changes in the video file format should be undetectable by the attacker.

## III. INTRODUCTION TO AUDIO STEGANOGRAPHY

Audio steganography means a mechanism in which audio files are used as cover media to hide the information which is to be kept confidential. It is art or science of hiding information. The main goal of steganography is to communicate in a completely undetectable manner. It does not alter the secret message but rides it inside cover media. It is a means through which manipulation of digital media is done with a very high security. The message could be accessed by the person who has authorization through authenticate keyword. This is a type of communication where exchange of information between two parties is kept confidential.

The project is based on providing the highly secure data transfer without the disruption of anyone else other than sender and receiver. The concept is that the secret data to be hidden will be accepted from user and will encrypt and then embedded into the carrier files after suitable transformation. This will in turn make it difficult intruder to identify the message. Only intended recipient will be able to extract the message using the authenticated password. The information is hidden in basically two techniques

1) Embedding flow
2) Extraction flow

*1) Embedding Flow:*

It is a part of the information hiding at the transmitter side. The embedding flow includes the cover media which is an audio and a secret message both are given as an input to the Stego system encoder whereas the transformation takes place and at the output stego file is generated.

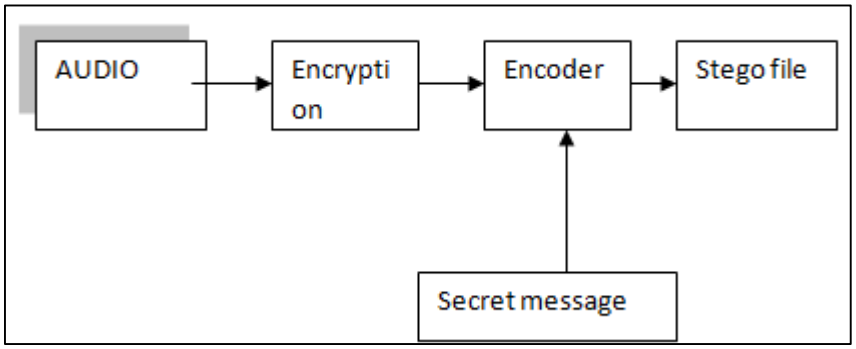


Fig. 2: Transmitter of Audio Steganography

*2) Extraction flow:*

The extraction is the process which takes place at the receiver side. The decryption of the message takes place with the help of key available only with the receiver. The pillars of steganography are confidentiality; Integrity and unremovability which is inevitable to make the system full fledge protected. The transmitter and receiver require a channel to communicate with each other.

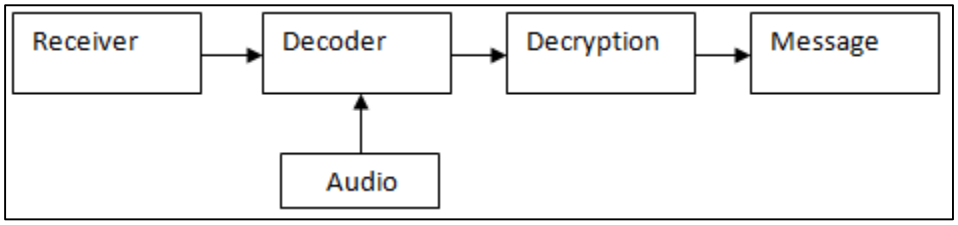


Fig. 3: Receiver of audio steganography

## IV. TECHNIQUES OF AUDIO STEGANOGRAPHY

### *A. Temporal Domain*

*1) LSB:*

LSB is one of the earliest and simplest methods for hiding information in audio signals. It is the commonly used techniques for audio Steganography. In LSB encoding, the least significant bits of the cover media audio is altered to include the correct message. This is simple method an attacker can easily extract the secret message from the stegno object.

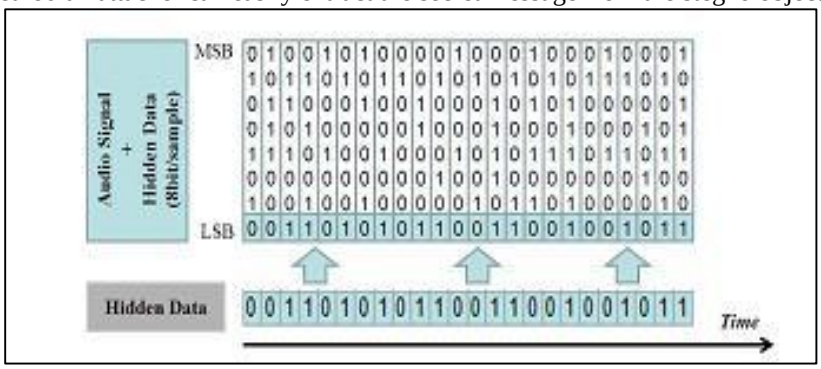


Fig. 4: LSB

*2) Parity Coding:*

This technique is one of the robust audio steganography techniques. Instead of breaking a signal into individual samples, it breaks a signal into separate samples sections and embeds each bit of the secret message information from a parity bit. If the of a selected parity bit region does not match the secret message bit to be encoded, the process inverts the LSB of one of the section in the region. Then the sender has many choices for encoding the secret bit.

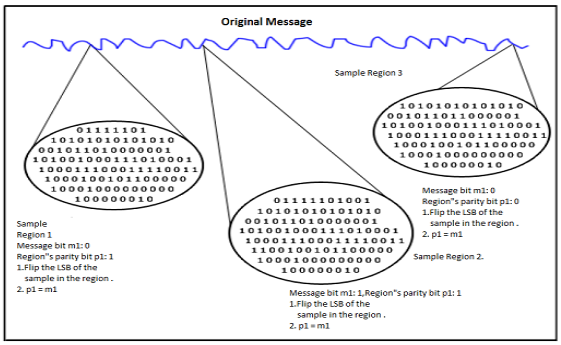


Fig. 5: Parity Coding

*3) Echo Hiding:*

Echo hiding used to embeds secrete data in a audio file by pass an echo into the desecrate signal. The echo is a resonance added to the host signal and hence the problem with the addictive noise is avoided. This technique has advantages of providing a high data transmission rate and robustness when we make comparison of echo hiding to other method. One bit secrete data could be encoded if one eco was produced from the original signal; before the encoding process start the original signal is broken down into blocks. Once the encoding process is done the blocks are concatenated together to create the final signal.

### *B. Frequency Domain:*

Frequency domain techniques and wavelet domain techniques come under transform domain. The main techniques under frequency domain are: tone insertion, Phase coding and Spread Spectrum Techniques.

*1) Tone Insertion:*

Frequency masking property is exploited in tone insertion method. A work pure tone is masked in the presence of a stronger tone. This property of inaudibility is used in different ways to embed information.

*2) Phase coding:*

Phase coding method is based on the fact that the phase component is not audibled human noise components. This method embeds the secrete message bits as phase shift in the phase spectrum of the original audio signal. The method tolerates better signal distortion, better robustness but it doesn't survive low phase filtering. Here the secrete message is inserted only as the phase vector of the first signal segment.

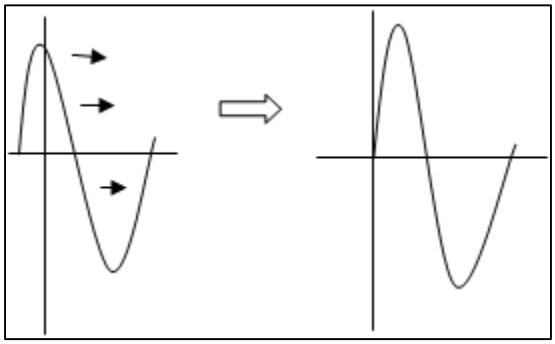

Fig. 6: Phase Coding

*3) Spread Spectrum Techniques:*

This techniques takes the advantages of masking property HAS. A masking threshold is calculated using a Psycho-acoustic model. The spread signal now lies below the masking threshold. Apart from shifting, here the secrete message is distributed along with the host signal. Here the final signal occupies a bandwidth which is more than is actually required for transmission.

### *C. Wavelet domain:*

Wavelet Domain is suitable for frequency analysis because of its multi-resolution. Multi-resolution properties that provides access to both most significant parts and details of spectrum. Wavelet domain techniques works with the wavelet coefficient. Upon applying the inverse transform, the stegno signal can be reconstructed.

Table - 1
Summary of Audio Steganography Techniques

| *Method* | *Strength* | *Weakness* |
|---|---|---|
| *LSB* | *It is simple.* | *It is extract* |
| *Parity Coding* | *It is more robust than LSB.* | *It is easy to extract.* |
| *Echo Hiding* | *Avoids problems with additive noise.* | *Low capacity.* |

| | | |
|---|---|---|
| *Tone Insertion* | *Exploits masking property.* | *It is low embedding capacity.* |
| *Phase Coding* | *It is robust.* | *It is low capacity.* |
| *Spread Spectrum* | *Increased transpherency* | *It's occupies more bandwidth* |
| *Wavelet Domain* | *It is high hiding capacity and transparency.* | *It is a lose data retrieval.* |

## V. LEAST SIGNIFICANT BIT ALGORITHM

LSB coding is the simplest method to hide the secret information. With help of LSB coding, we can hide more information. In this technique LSB of binary equivalent of each sample of digitized audio is replaced with binary equivalent secret message.
To hide the letter "D" as an example which has the ASCII code equal to 68 that is 01000100 inside eight byte of cover, the process of LSB can be shown follow.

| *Original data bytes* | *Text data to hide* | *Text data embedded audio byte* |
|---|---|---|
| *10010010* | *0* | *10010010* |
| *01010011* | *1* | *01010011* |
| *10011011* | *0* | *10011010* |
| *11010011* | *0* | *11010010* |
| *10001010* | *0* | *10001010* |
| *00000010* | *1* | *00000011* |
| *01110010* | *0* | *01110010* |
| *00101011* | *0* | *00101010* |

## VI. WORKING

The secret message which may be text file, image is used as input given to the system. The audio file used which is a cover media for a secret message is in WAV format. The audio file is selected to perform encryption as well as to hide message. The secret message is hidden into an audio file .firstly; it read the ASCII code of secret message and then converted into bit pattern. This process is done by using LSB algorithm. Whenever the secret message hides in an audio file it will generate one encryption key while transmitting the message through the network at the receiver side. After hiding the secret message into the audio file, it will carry out through a network along with the encryption key. The person at the receiver side must know the encryption key to extract the original message. The key will send to receiver by an email. Once the key receives, it will enter and then person at receiver side can successfully extract the message.

Among many different data hiding techniques proposed to embed secret message within an audio file, the LSB algorithm technique is one of the secure methods for inserting data into audio signal in noise free environment.
The following steps used to hide the encrypted data into audio signals:

1) Receives the audio file and converted into bit pattern.
2) Each character in the message converted into bit pattern.
3) Replace the random bits of audio file with encrypted message bit.

This proposed system is to provide a good, efficient method for hiding data from hackers and send it to destination in safe manner. The proposed system will not change the size of the file even after encoding.

This method is suitable for any type audio format. Encryption and decryption techniques have been used to make the security system robust.

## VII. CONCLUSION

In this paper, we have introduced a robust method of imperceptible audio data hiding. This is to provide a good efficient method for hiding the data from hackers and sent to the destination in a safer manner. The system which is proposed will not even change the size of audio file after encoding also and could use any type of audio file formats. Thus we conclude that audio data hiding technique can be used for a number of purposes other than covert communication, information tracing, finger printing and tamper detection.

## REFERENCES

[1] Rahul Joshi, Lokesh Gagnani , Salony Pandey,"Image Steganography with LSB", International journal of Advance Research In Computer Engineering and Technology, Volume-2 January-2013.
[2] Mrs. Kavita, kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Significant Bit Algorithm", International journal of Engineering Research And Application, Volume-2, May-June2012.
[3] jayeeta Majumder, Sweta Mangal,"An Overview of Image Steganography Using LSB Techniques", National Conference On Advance in Computer Science And Application With International Journal Of Computer Apllication,2012.
[4] Champakamala B.S, Padmini K, Radhika D. K.,"Least Significant Bit Algorithm for Image Steganography", International Journal of Advanced Computer Technology.