International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT5228368

# Audio Steganography

**Vaibhavi P. Naik*, Dr. Aisha C. F. Fernandes**
Department of Information Technology, Goa College of Engineering, Farmagudi, Goa, India

**Article Info**
Volume 8, Issue 3
Page Number : 196-201

**Publication Issue :**
May-June-2022

**Article History**
Accepted: 10 May 2022
Published: 30 May 2022

**ABSTRACT**

Electronically communicating has increased in the covid scenario giving birth too numerous new styles to transmit information securely and robustly. So to achieve communication in secured way audio steganography can be used. Audio steganography is a method to hide text message in audio. In this paper, comparison between Least Significant bit (LSB) and phase encoding steganographic methods are carried out by implementing these techniques. Also the audio extraction features like amplitude envelope, Root mean squared energy, Zero crossing rate, Band energy ratio, Spectral centroid, Spectral bandwidth and mfccs.

**Keywords :** Audio steganography, steganographic methods, phase encoding, Least Significant bit (LSB)

## I. INTRODUCTION

As internet applications have a huge demand and new technologies are been introduced, there is an increased possibility of attacks. Hence, there are issues like security and confidentiality. Steganography is the technique that can be used to solve these issues where the secret message is embedded on the sender side and retrieving it on the receiver side.

The data that is protected using images may not be always safe. Audio steganography is the most difficult technique to hide data when compared to image and video steganography since the Human Auditory System (HAS) is more sensitive than the human visual system. Audio Steganography hides the secret message in an audio file, the resulting message is called a stego message, which can be called encoding, and a stego message is transmitted to the receiver side, the process can be called decoding. Before implementing audio steganography: capacity, transparency, and robustness are the conditions that need to be remembered. In this paper, we have implemented two audio steganography techniques that are Least Significant bit (LSB) and phase encoding followed by some feature extraction.

## II. AUDIO STEGANOGRAPHY

Audio steganography is a steganography method that uses an audio file as the stego message. In this method, the message to hide can be audio, image or text. This method requires revision of audio signal in an imperceptible manner.

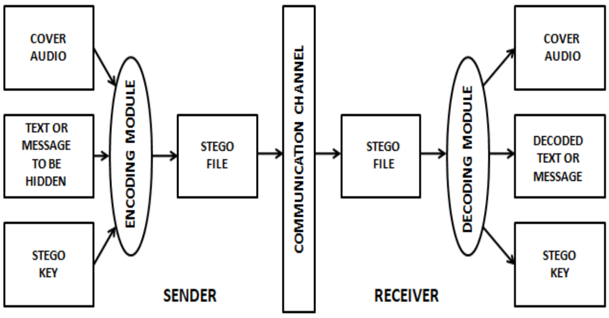


Figure 1. General Audio Steganography Block Diagram

## III. Approach

### A. Least Significant Bit (LSB)

The Least Significant Bit is one of the earliest methods used to hide information which comes under spatial domain methods. This method embeds the secret message into the least significant bit of audio file. Modification of audio files using LSB is achieved in such a way that the quality of the audio file is not compromised. This method helps to get high data embedding capacity and can be easily incorporated for hiding data.

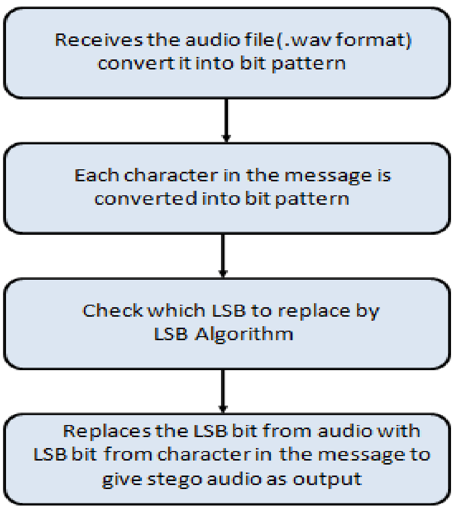


Figure 2. Flowchart for Least Significant Bit (LSB)

### B. Phase coding

Phase coding is a transform domain method exploits the fact that Human Auditory System cannot recognize the phase change as easily as it can recognize the noise in the signal. It is based on the fact that phase components of sound are not as distinguishable to human ear as noise is. In Phase coding the secret message is encoded as phase shifts in the spectrum of a digital signal. The low transmission rate in phase coding is a disadvantage as the secret message is embedded only in the first signal segment. Increasing the length of the signal segment can increase the transmission rate but this would cause change of phase relations between each frequency component of a segment more excessively, which will help to make embedding easier to detect.

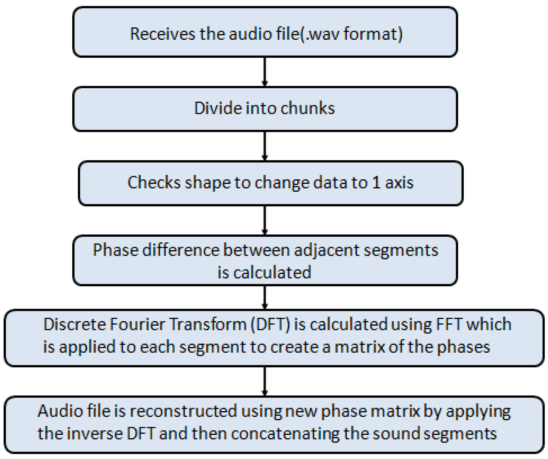


Figure 3. Flowchart for Phase Coding

## IV. SYSTEM IMPLEMENTATION

The proposed system consists of two sections, one at the sender side that is ENCODING and the other at the receiver side that is DECODING. The user should be able to select audio file to encode. The system has options to select steganography techniques then we need to enter text or message to be hidden. After pressing encode button the text is encoded. The stego audio is stored in a folder. The user at the receiver side should be able to extract or decode the secret message from the stego audio by selecting the stego audio, selecting the steganography techniques and press decode button to decode the message.

## A. Interface

The interface for Audio Steganography consists of two columns, the receiver side and sender side. There is an option to select the file to encode, also options to select audio steganography methods.

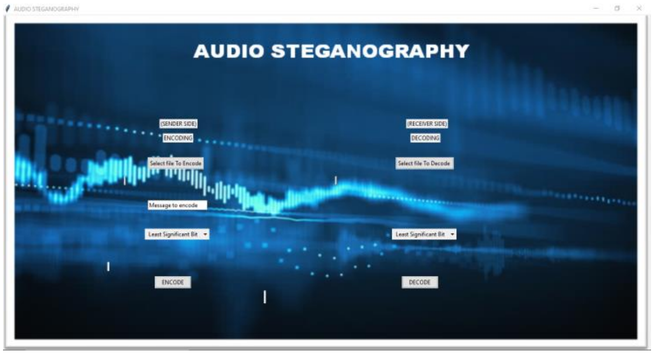


Figure 4. Interface

## B. Encoding

- Select the cover audio from the set of audio files at sender's side.
- Enter the secret message.
- Embed the secret message to generate the stego Audio.

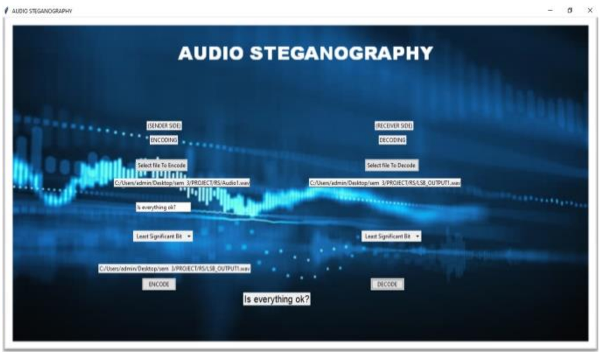


Figure 5. Encoding for audio 1

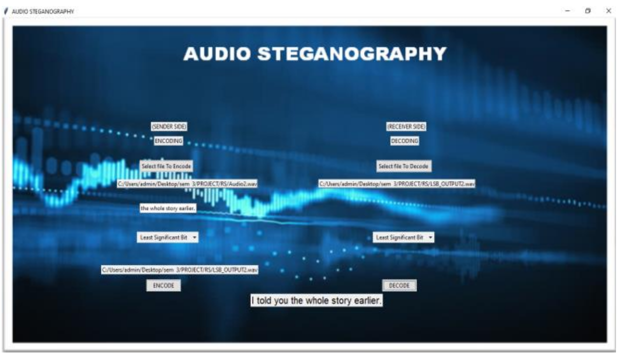


Figure 6. Encoding for audio 2

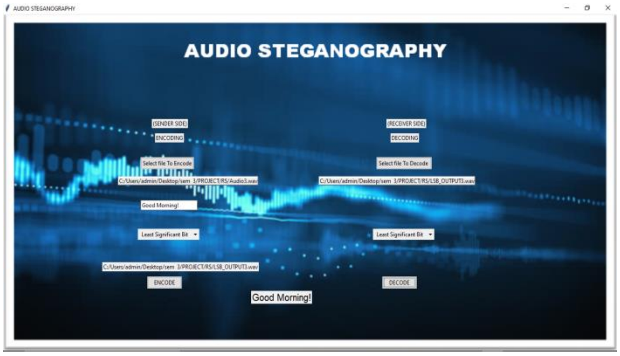


Figure 7. Encoding for audio 3

## C. Decoding

- Select the encoded audio from the set of audio files from the folder.
- Secret message is extracted.
- Later secret message is displayed.

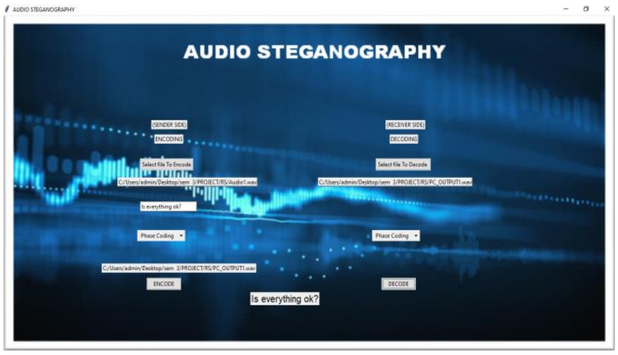


Figure 8. Decoding for audio 1

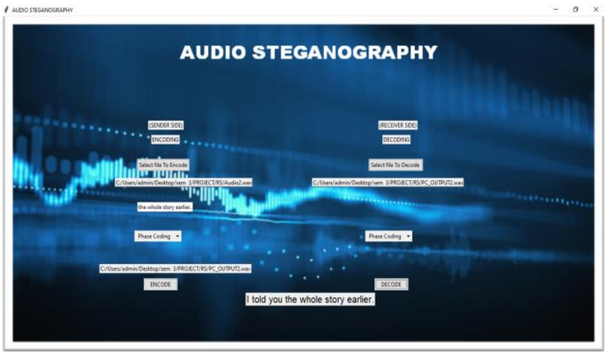


Figure 9. Decoding for audio 2

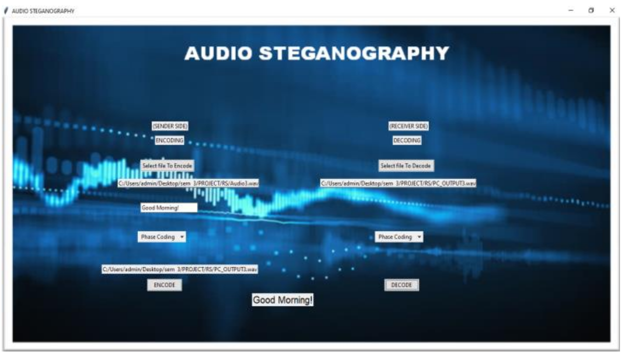


Figure 10. Decoding for audio 3

## V. THE OUTCOME

### A. Numerical

| Method | Audio file | Audio time (secs) | Text size (bits) | Sampling rate (Hz) | RMSE | ZCR | BER | Amplitude envelope | Spectral centroid | Spectral bandwidth | MFCCs |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Audio1.wav | 5.32 | 136 | 44100 | 230 | 230 | 230 | 230 | 230 | 230 | (13, 230) |
| LSB | LSB_OUTPUT1.wav | 5.32 | 136 | 44100 | 230 | 230 | 230 | 230 | 230 | 230 | (13, 230) |
| PC | PC_OUTPUT1.wav | 5.38 | 136 | 44100 | 233 | 233 | 233 | 232 | 233 | 233 | (13, 233) |
| | Audio2.wav | 33.52 | 280 | 8000 | 1445 | 1445 | 1445 | 1445 | 1445 | 1445 | (13, 1445) |
| LSB | LSB_OUTPUT2.wav | 33.52 | 280 | 8000 | 1445 | 1445 | 1445 | 1445 | 1445 | 1445 | (13, 1445) |
| PC | PC_OUTPUT2.wav | 33.79 | 280 | 8000 | 1456 | 1456 | 1456 | 1456 | 1456 | 1456 | (13, 1456) |
| | Audio3.wav | 35.54 | 104 | 44100 | 1531 | 1531 | 1531 | 1445 | 1531 | 1531 | (13, 1531) |
| LSB | LSB_OUTPUT3.wav | 35.54 | 104 | 44100 | 1531 | 1531 | 1531 | 1531 | 1531 | 1531 | (13, 1531) |
| PC | PC_OUTPUT3.wav | 35.57 | 104 | 44100 | 1533 | 1533 | 1533 | 1532 | 1533 | 1533 | (13, 1533) |

Table 1. Shows results for audio feature extraction

### B. Graphical

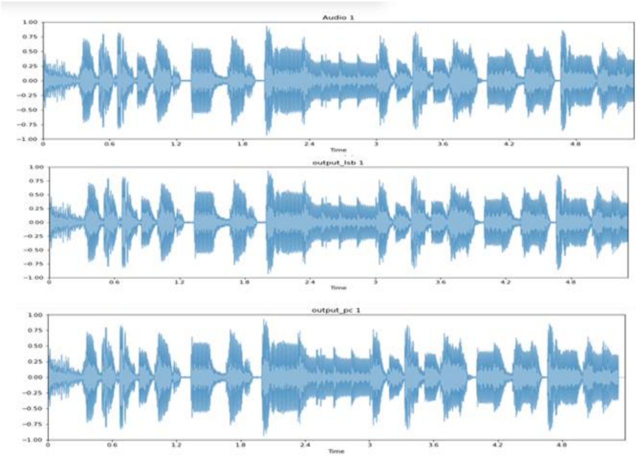


Figure 11. Visualizing audio signal in the time domain for audio 1 and audios after encoding for both methods

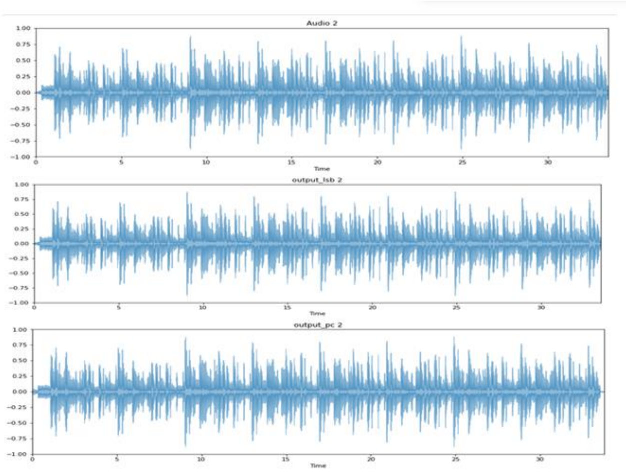


Figure 12. Visualizing audio signal in the time domain for audio 2 and audios after encoding for both methods

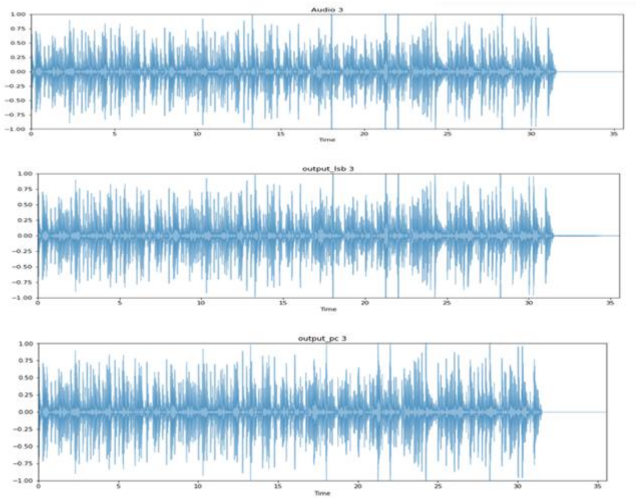


Figure 13. Visualizing audio signal in the time domain for audio 3 and audios after encoding for both methods

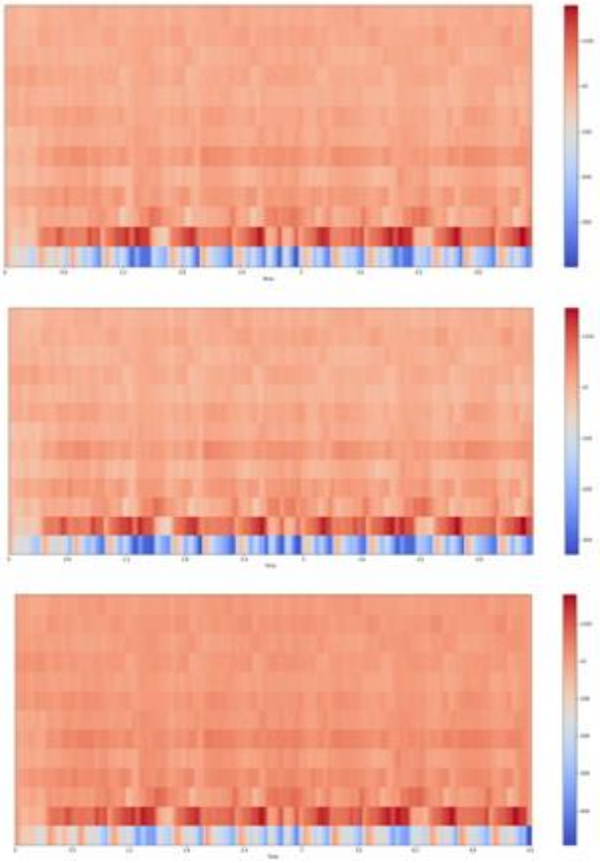

Figure 14. Extracting MFCCs for audio 1 and audios after encoding for both methods

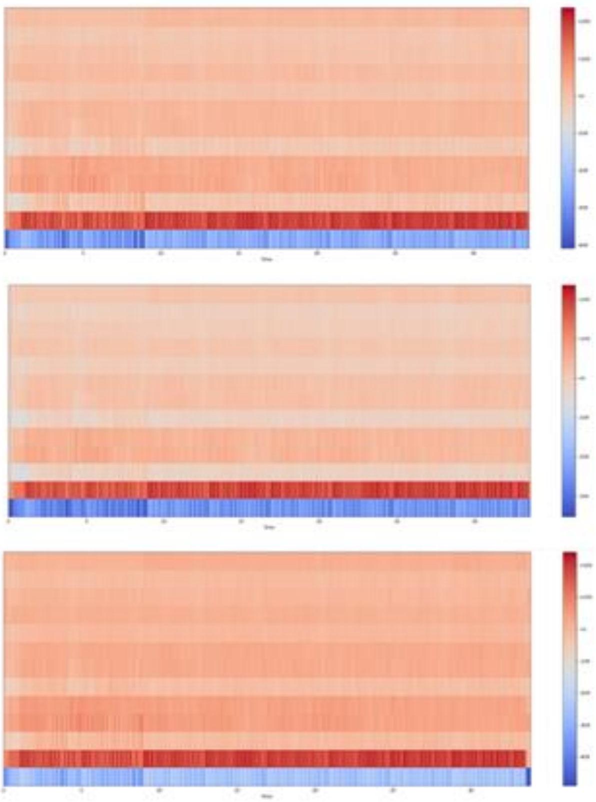

Figure 15. Extracting MFCCs for audio 2 and audios after encoding for both methods

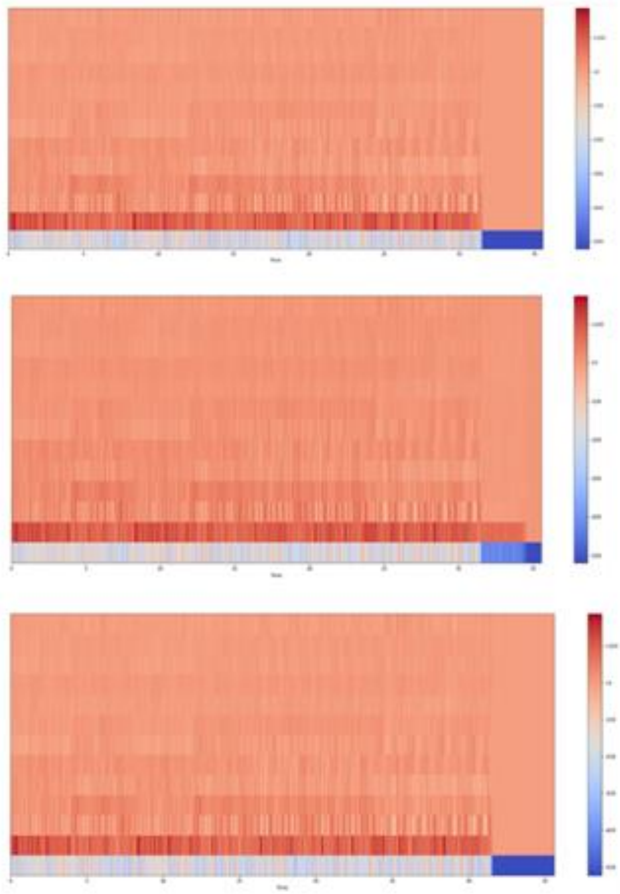

Figure 16. Extracting MFCCs for audio 3 and audios after encoding for both methods

## IV. CONCLUSION

A system was implemented to perform audio steganography using LSB and Phase encoding techniques. Comparison has been performed between these techniques. From the experimental results, it has been observed that Phase encoding is more secured than LSB method. From the survey, it is clear that the spatial domain maximizes the data hiding capacity whereas the transform domain focuses on masking properties to make the noise generated by embedding data imperceptible. In addition, it can be concluded that the transform domain is preferred over the spatial domain although this method has been designed for wav format; the method can be extended for any other type of audio file format.

Also audio feature extraction are performed with visualization like amplitude envelope, Root-mean-squared energy, Zero-crossing rate, Band Energy Ratio, Spectral centroid, Spectral bandwidth and Extracting MFCCs.

## V. REFERENCES

[1]. Binny, Anu; Koilakuntla, Maddulety (2014). Hiding Secret Information Using LSB Based Audio Steganography [IEEE 2014 International Conference on Soft Computing & Machine Intelligence (ISCMI)]

[2]. Vimal, Jithu; Alex, Ann Mary (2014). Audio Steganography Using Dual Randomness LSB Method [IEEE 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)

[3]. Mrs. Namita Verma, Mr. Vinay Kumar Jain. Audio Steganography – A Review, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 2, Issue 1, January 2013 .

[4]. Manisha Verma, Hardeep Singh Saini, Analysis of Various Techniques for Audio Steganography in Data Security-IJSRNSC.

[5]. Souvik Bhattacharyya, Arko Kundu, Gautam Sanyal -A Novel Audio Steganography Technique by M16MA, International Journal of Computer Applications 2011.

[6]. Prof. Samir Kumar, BandyopadhyayBarnali, Gupta Banik-LSB Modification and Phase Encoding Technique of Audio Steganography Revisited, International Journal of Advanced Research in Computer and Communication Engineering 2012.

[7]. Bilal, Ifra; Kumar, Rajiv; Roj, Mahendra Singh; Mishra, P K Mishra -Recent advancement in audio steganography [IEEE 2014 International Conference on Parallel, Distributed and Grid Computing (PDGC).

**Cite this article as :**

Vaibhavi P. Naik, Dr. Aisha C. F. Fernandes, "Audio Steganography", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 3, pp. 196-201, May-June 2022. Available at doi : https://doi.org/10.32628/CSEIT5228368
Journal URL : https://ijsrcseit.com/CSEIT5228368