Review on Audio Steganography by Optimization Approaches

Tabasum kounsar[1], ER sukhvinder Kaur[2]
[12]*Department of Electronics and communication*
Swami Devi Dyalinstitute of Engineering and technology
Barwala, Kurukshetra university, kurukshetra, INDIA

Abstract- In this digital world, huge amount information exchange takes place due to enhanced facilities of networking. Therefore, it is necessary to secure the information which we transmit. The need for secured communication introduces the concept of "Steganography". Steganography, the word itself indicates that information within information; it is the best technique to hide the secret information by using cover objects. Secret information may be a text, image or an audio file. But as per secret information format there are different steganography techniques are availablepower greater than one billion to one and a range of frequencies greater than one thousand to one. Sensitivity to additive random noise is also acute. Perturbations in a sound file can be detected as low as one part in ten million. However there are some "holes" available in this perspective range where data may be hidden. While the HAS consists of a large dynamic range, it often has a fairly small differential range. Asa result, loud sounds tend to mask out quiet sounds. There are some environmental distortions so common as to be ignored by the listener in most cases

Keywords- Steganography, Human Auditory System, Human Visual System

I. INTRODUCTION

The term "Security through Obscurity" is the belief that a system of any sort can be secure so long as nobody outside of its implementation group is allowed to find out anything about its internal mechanisms. Data hiding is considered as security by obscurity system. Number of techniques has been implemented towards improving secure data hiding approaches [9]. Two main considerations in these techniques are the amount of data hidden & the secrecy of the data against the attackers. One of such technique is "Steganography". In steganography techniques, the sender hides the secret message into host file. This produced a stego file then delivers it to the receiver that will de-hide the stego file to retrieve the secret message. The secret data and the host can be any of various file type like text, audio, image and video file [3][13]. If the host file is an audio file then the method is called audio steganography. Embedding secret data in host audio file is more challenging than using images since Human Auditory System (HAS) is more sensitive in comparison to Human Visual System (HVS). Thus, this study focuses on audio Steganography and gives a wide view of trends in this field.

1.1 Steganography

Steganography has proved to be one of the practical ways of securing data. It is used to hide secret data inside other digital mediums. Audio files &signals make appropriate medium for steganography due to high data transmission rate & high level of redundancy. Generally, all digital mediums, signals or files can be used in steganography process as cover media. The choice of cover media depends on the level of redundancy. Redundancy can be described as the bits of media, signals or file that offer accuracy more than needed for the object use. Image, video & audio files fulfil this requirement [13].

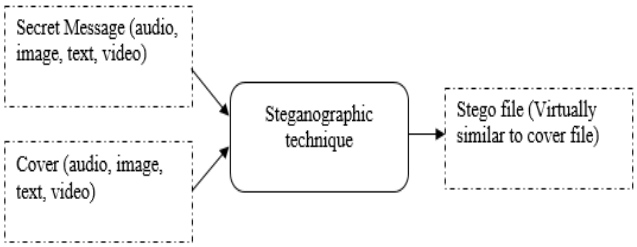

Fig.1: Basic scheme of steganography process

The basic process in steganography involves embedding the secret message in the carrier file & thus the stego file is created. This stego file resembles the carrier file &is transmitted in the transmitter side. It is received at receiver side & the reverse process of extracting the secret information from the stego file is performed.

1.2 Audio steganography

The basic model of Audio steganography consists of Carrier file, given Message and Password which is known as stego-key. Carrier is also known as a cover-file, which hides the secret information. Message is any data that the sender wants to remain it confidential [1, 4]. Message can be plain text, image, audio or any type of file. The password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file [1, 2].

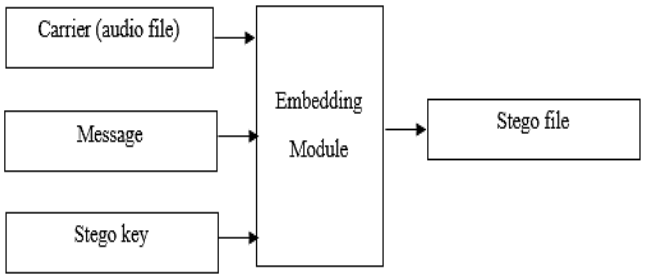

Fig.2: Basic Audio Stenographic Model

The cover-file with the secret information is known as a stego-file. The information hiding process consists of following two steps:

- Redundant bits in a cover-file are identified. Redundant bits are those bits that can be altered without destroying the integrity and exploiting the quality of the cover file.
- To embed the secret information (or data) in the cover file, the redundant bits present in the cover file is replaced by the bits of the secret information.

1.2.1 Data Hiding in audio files

Encoding secret messages in audio is the most challenging technique to use when dealing with Steganography. This is because the human auditory system (HAS) has such a dynamic range that it can listen over. The HAS perceives over a range of power greater than one billion to one and a range of frequencies greater than one thousand to one. Sensitivity to additive random noise is also acute. Perturbations in a sound file can be detected as low as one part in ten million. However there are some "holes" available in this perspective range where data may be hidden. While the HAS consists of a large dynamic range, it often has a fairly small differential range. Asa result, loud sounds tend to mask out quiet sounds. There are some environmental distortions so common as to be ignored by the listener in most cases. There are two concepts to consider before choosing an encoding technique for audio. They are the digital format of the audio and the transmission medium of the audio [5, 8].

Digital audio formats

- *Sample Quantization:* A 16-bit linear sampling architecture used by popular audio format such as .WAV and .AIFF.
- *Perceptual Sampling:* changes the statistics of the audio drastically by encoding only the parts the listener perceives, thus maintaining the sound but changing the signal. This format is used by the most popular digital audio on the Internet today in ISO MPEG (MP3).
- *Temporal Sampling:* It uses selectable frequencies (8, 9.6, 10, 12, 16, 22.05and 44.1 kHz.) to sample the audio. Sampling rate puts an upper bound on the usable portion of the frequency range.

Transmission audio format

- *Increased/decreased resampling environment*: In thisenvironment, a signal is resampled to a higher or lowers sampling rate, but remains digital throughout. Although the absolute magnitude and phase of most of the signal are preserved, the temporal characteristics of the signal are changed.
- *Over the air'' environment:* This occurs when the signal is ``played into the air'' and ``resampled with a microphone''. The signal will be subjected to possible unknown nonlinear modifications causing phase changes, amplitude changes, drifting of different frequency components, echoes, etc.
- *Digital end-to-end environment:* If a sound file is copied directly from machine to machine, but never modified, then it will go through this environment. As a result, the sampling will be exactly the same between the encoder and decoder. Very little constraints are put on data hiding in this environment
- *Analog transmission and resampling:* This occurs when a signal is converted to an analog state, played on a relatively clean analog line, and resampled. Absolute signal magnitude, sample quantisation and temporal sampling rate are not preserved.

1.2.2 Hidden and extraction of data in sounds

1. Hide secret information into carrier audio file: To hide secret information into audio file, do the following steps [14]:

- Choose the carrier audio file and make sureits format is one of them flac, wav, wma, mp3, ape.
- Click encode and the file will be encoded and then you can click 'Add files' to add secret files into the panel on the right side of application.
- You can choose output audio format (wav, flac or ape). DeepSound does not support wma output format. If you desire to hide secret information into wma, hide secret information into wav file and then use external software such as Windows Media Encoder for change wav to wma lossless.
- In the settings you can select to turn On/Off encrypting and set password. New audio file will be saved to the output directory. Select Ok to start hiding secret files into carrier audio file.

DeepSound: Deep sound is audio stenography software for windows and can be used to create secret message via audio file. It is information security solutions freeware and supports all kinds of audio files.

2. Extract secret data from audio file: As per information and data security solutions experts, to remove secret data from audio file, follow the following steps [14]:

- In the file explorer, choose the audio file, which encloses secret data. If the secret files are encrypted, input password.
- DeepSound examines the selected file and exhibits secret files. Click the right mouse button and press F4 key or select extract secret files.
- Open the Audio Converter.To add input files select 'Add files' button and the supported input audio formats are: Free Lossless Audio Codec (.flac), Windows media audio lossless (.wma), MPEG audio layer-3 (.mp3), and Monkey's Audio (.ape)

1.3 Audio steganography Methods

This section presents some common methods used in audio Steganography [5][6]:

1.3.1 LSB Coding

It is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded.

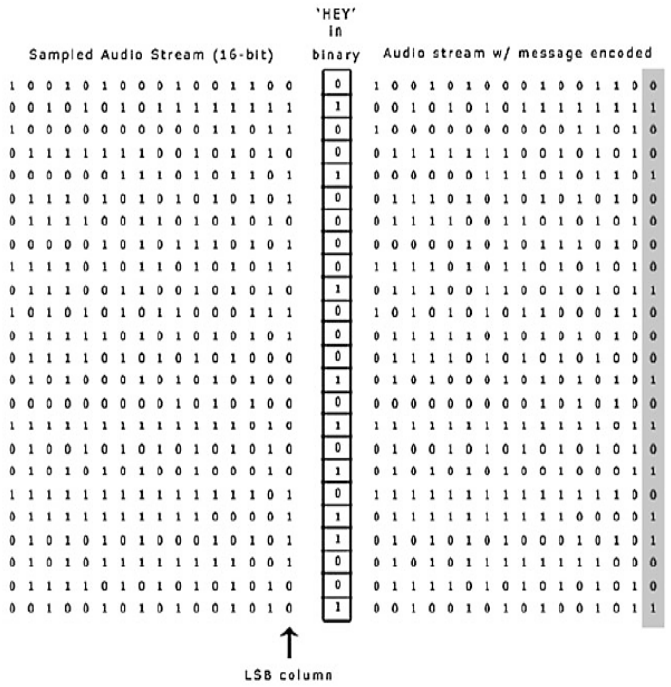

Fig.3: Coding of LSB [5][9]

Figure 3 illustrates how the message 'HEY 'is encoded in a 16-bit CD quality sample using the LSB method. In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo [9].

- *Advantage:* Low computational complexity
- *Disadvantage:* LSB coding increases or, equivalently, depth of the modified LSB layer becomes larger, probability of making the embedded message statistically detectable increases and perceptual transparency of stego objects is decreased. Low Bit Encoding is therefore an undesirable method.

1.3.2 Phase Coding

Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio.

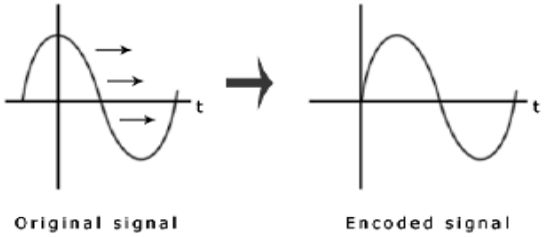

Fig.4: Phase Coding

The phase coding method breaks down the sound file into a series of N segments. A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phase and magnitude. The phase difference between each segment is calculated, the first segment (s0) has an artificial absolute phase of p0created, and all other segments have newly created phase frames. The new phase and original magnitude are combined to get the new segment, Sn. These new segments are then concatenated to create the encoded output and the frequency remains preserved. In order to decode the hidden information the receiver must know the length of the segments and the data inter valued [10, 11] [12]. The first segment is detected as a 0 or a 1 and this indicates where the message starts.

- *Advantage:* Low Bit Encoding being undetectable to the human ear.
- *Disadvantage:* Lack of robustness to changes in the audio data.
-

1.3.3 Spread Spectrum

Spread spectrum techniques can be used for watermarking by matching the narrow bandwidth of the embedded data to the large bandwidth of the medium. Two versions of SS can be used in audio Steganography: the direct-sequence and frequency hopping schemes.

1. Direct-Sequence SS: The secret message is spread out by a constant called the chip rate and then modulated with a pseudorandom signal.
2. Frequency hopping SS: The audio file's frequency spectrum is altered so that it hops rapidly between frequencies.

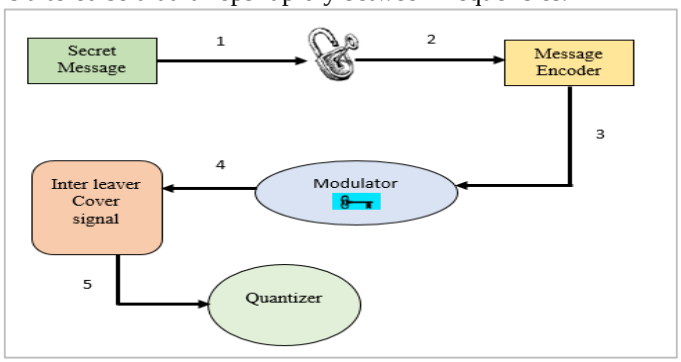

Fig.5: Spread Spectrum (SS)

Steps of Spread Spectrum

The spread spectrum methodology relies on the following represents steps:
1. Secret message encrypted using a symmetric key, k1.
2. Encrypted message is encoded using a low rate error-correcting code. This increases the robustness of the system.
3. The message encoded is then modulated with a pseudorandom signal that was generated using a second symmetric key, k2, as a seed.
4. The resulting random signal that contains the message is interleaved with the cover signal.
5. The final signal is quantized to create a new digital audio file that contains the message.
6. This process is reversed for message extraction.

- *Advantage:* Moat secure and offers a moderate data transmission rate while also maintaining a high level of robustness.
- *Disadvantage:* It can introduce random noise resulting in data loss

1.3.4 Eco Hiding

Echo hiding embeds its data by creating an echo to the source audio. Three parameters of this artificial echo are used to hide the embedded data, the delay, the decay rate and the initial amplitude. As the delay between the original source audio and the echo decrease it becomes harder for the human ear to distinguish between the two signals until eventually created carrier sound's echo is just heard as extra resonance. In addition, offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero. If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal [7] [9].

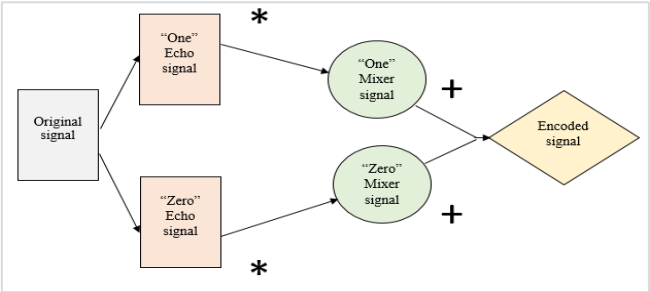

Fig.5: Echo Hiding

The "one" echo signal is then multiplied by the "one" mixer signal and the "zero" echo signal is multiplied by the "zero" mixer signal. Then the two results are added together to get the final signal. The final signal is less abrupt than the one obtained using the first echo hiding implementation. This is because the two mixer echoes are complements of each other and that ramp transitions are used within each signal. These two characteristics of the mixer signals produce smoother transitions between echoes. To extract the secret message from the stego signal, the receiver must be able to break up the signal into the same block sequence used during the encoding process. Then the autocorrelation function of the signal's spectrum (the spectrum is the Forward Fourier Transform of the signal's frequency spectrum) can be used to decode the message because it reveals a spike at each echo time offset, allowing the message to be reconstructed.

- *Advantage:* It allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods.
- *Disadvantage:* The transmission of audio files via e-mail or over the web is much less prolific than image files and so is much more suspicious in comparison.

II. RELATED WORK

Vijay R. Arjunan, et.al [1] presented a novel approach with a randomized embedding scheme for audio steganography, which absolve the lack of security, and the localized nature of the distortions produced in the stego object. The main advantage of a randomized embedding scheme is that, the data values can be stored at any random position in the audio data set. This protects the stego object against an unauthorized breach by unwanted entities. Although the random number generation increases the overall computational complexity of the entire process, the resultant improvement in security and dataset integrity is certainly worth it. Experimental results indicate that the proposed method has an improved security and dataset integrity check with genuine protection for the hidden information, when compared to a basic embedding scheme like the sequential embedding scheme. RuohanMeng,

et.al [2]proposed a new steganography algorithm based on object detection and relationship mapping, which integrates coverless information hiding and steganography. In this method, the coverless information hiding is realized by mapping the object type, color and secret information in object detection method. At the same time, the object detection method was used to find the safe area to hide secret messages. The proposed algorithm can not only improve the steganographic capacity of the two information hiding methods but also make the coverless information hiding more secure and robust. AbdesselamBeroual, et.al [3] highlights the concepts regarding popular steganography techniques and algorithms. There are different types of steganography methods available. The number of methods is not restricted. Here the importance is given to methods focusing on the capacity property, and secondly on imperceptibility. Other properties of a steganogrpahic system "robustness and security" are mentioned briefly in the literature section. According to this paper, the maximum size of embedded data reached by the previous works in this literature review is 55%and 52% in [21] and [17] respectively. This technique consists of transforming the secret data on the base of the cover into a small part considered a sequence of references. Ahmed Hussain Ali, et.al [4] proposed an audio steganography model for secure audio transmission during communication based on fractal coding and a chaotic least significant bit or also known as HASFC. This model contributes to enhancing the hiding capacity and preserving the statistical transparency and security. It manages to embed secret audio into a cover audio with the same size. In order to achieve this result, fractal coding was adopted which produces high compression ratio with the acceptable reconstructed signal. The chaotic map was used to randomly select the cover samples for embedding and its initial parameters are utilized as a secret key to enhancing the security of the proposed model. Shilpi Mishra, et.al [5]focused on the overall standards of concealing mystery facts in sound document utilizing sound information concealing systems, and convey an outline of present strategies and capacities furthermore talk about the favorable circumstances and disservices of diverse sorts of audio steganography method. Mahmoud Mustafa Mohammed Mahmoud, et.al [6] proposed a novel model to hide the very secret and sensitive information within an audio file. The proposed model consists of three stages, the text is first compressed using the Huffman algorithm then encrypted using AES algorithm and finally hide using the novel LSB-Block algorithm. A novel proposed mechanism, Binaries of Message Size Encoding (BMSE), were performed before the hiding process to produce a key, which is used in the hiding process in the proposed enhanced LSB-Block algorithm. The model was applied using the MATLAB program and tested using the Mean Error Square (MSE) operators and the Peak Signal to Noise Ratio (PSNR).Different comparisons were made and the results verified the efficiency and effectiveness of the proposed model.

Table.1 Existing Scheduling Mode

Author's Name	Year	Methodology Used	Proposed Work
Vijay R. Arjunan, et.al	2019	Randomized Embedding Scheme	Presented a novel approach with a randomized embedding scheme for audio steganography, which absolve the lack of security, and the localized nature of the distortions produced in the stego object.
Mohammed Mahmoud, et.al.	2018	Binaries of Message Size Encoding (BMSE), LSB-Block algorithm	Proposed a novel model to hide the very secret and sensitive information within an audio file.
Namitaverma, et.al.	2013	SB Coding, Phase Coding, Spread Spectrum and Echo Hiding	Presented the major techniques in detail used for data hiding in audio files.
Divya et al.	2012	LSB Coding Method	Reported that compared to standard LSB coding method, embedding data in multiple and variable LSBs depending on the MSBs of the cover audio samples is an efficient approach.

Bandyopadhyay et al.	2011	LSB Modification and Phase Encoding	Provided an overview of LSB modification and phase encoding, two basic techniques to understand the working of steganography in audio files.

SounakLahiri, et.al [7] dealt with the encoding of message bits in a cover audio carrier signal. It applies the basic concepts of audio steganography in transform domain to achieve higher efficiency in data transmission, while preserving the secrecy of the information being transmitted. The proposed model in this paper deals with the application of echo hiding of binary message bits in the carrier signal, in the transform coefficients obtained by applying 2D- discrete Haar Wavelet Transform on the cover signal. Moreover, this algorithm applies pseudorandom sequence to encode the data, which gives the method more efficiency and prevents unauthorized decoding at any moment. Tanwar et al., [8] in 2014 proposed a new approach that addresses the difficulties of substitution techniques in audio steganography. The main issue is less robustness against intentional and unintentional attacks that intend to unmask hidden message. The algorithm will hide the message in deeper layers of audio sample and will modify other bits to minimize the errors. The method currently uses 2 bits per byte of audio sample. This will progress towards achieving higher capacity and robustness. Namitaverma, et.al [9] has looked in detail at the major techniques used for data hiding in audio files. First section gave an overview of Steganography and in particular the concept of Audio Steganography. Second section described in detail, various Audio Steganography algorithms namely LSB Coding, Phase Coding, Spread Spectrum and Echo Hiding. At the end, feasibility of Audio Steganography was evaluated by considering the pros and cons.BandyopadhyayBarnali, et.al [10] studied the method of LSB modification of Steganography is the least secure. This method's security lies on the presumption that no other parties are aware of this secret message. This method is easy to implement but is very susceptible to data loss due to channel noise and re-sampling. Adhiya et al., [11] proposed a steganographic method for embedding textual information in audio. In this method each audio sample is converted into bits and then the textual information is embedded in it. The last 4 bits of this binary is taken into consideration and applying redundancy of the binary code. The prefix either 0 or 1 is used. The main advantage of this method is that 16 bit WAV and 8 bit WAV audio file are supported and the secret message can be hidden

in the audio file with less storage capacity. However, the main disadvantage associated with the proposed algorithm is that it gives better result for 16 bit WAV audio as compared to 8 bit. Divya et al., [12] reported that compared to standard LSB coding method, embedding data in multiple and variable LSBs depending on the MSBs of the cover audio samples is an efficient approach. There is a remarkable increase in capacity of cover audio for hiding additional data and without affecting the perceptual transparency of the text. The main advantage of this proposed method is that they are simple in logic and the hidden information is recovered without any error. Bandyopadhyay et al., [13] provided an overview of LSB modification and phase encoding, two basic techniques to understand the working of steganography in audio files. An effective audio steganographic scheme should possess the following three characteristics: Inaudibility of distortion, Data Rate and Robustness. These characteristics are called the magic triangle for data hiding. The advantage of this method is that it is easy to implement; however, the limitation of the method is that, it can be used only when a small amount of data needs to be concealed.

III. CONCLUSION

The proposed model consists of three stages, the text is first compressed using the Huffman algorithm then encrypted using AES algorithm and finally hide using the novel LSB-Block algorithm. A novel proposed mechanism, Binaries of Message Size Encoding (BMSE), were performed before the hiding process to produce a key, which is used in the hiding process in the proposed enhanced LSB-Block algorithm. The model was applied using the MATLAB program and tested using the Mean Error Square (MSE) operators and the Peak Signal to Noise Ratio (PSNR).Different comparisons were made and the results verified the efficiency and effectiveness of the proposed model.

IV. REFERENCES

[1]. Arjunan, Vijaya R., and ArunaavAlok. "A Randomized Approach for Data Embedding in Audio Steganography." *Journal of Advanced Research in Dynamical and Control Systems* 11, no. 2 (2019): 6-13.

[2]. Meng, Ruohan, Zhili Zhou, Qi Cui, Xingming Sun, and Chengsheng Yuan. "A Novel Steganography Scheme Combining Coverless Information Hiding and Steganography." *Joural of Information Hiding and Privarcy Protection* 1, no. 1 (2019): 43-48.

[3]. Beroual, Abdesselam, and ImadFakhri Al-Shaikhli. "A Review of Steganographic Methods and Techniques." *International Journal on Perceptive and Cognitive Computing* 4, no. 1 (2018): 1-6.

[4]. Ali, Ahmed Hussain, LoayEdwar George, A. A. Zaidan, and MohdRosmadi Mokhtar. "High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain." *Multimedia Tools and Applications* 77, no. 23 (2018): 31487-31516.

[5]. Mishra, Shilpi, Virendra Kumar Yadav, Munesh Chandra Trivedi, and TarunShrimali. "Audio Steganography Techniques:

A Survey." In *Advances in Computer and Computational Sciences*, pp. 581-589. Springer, Singapore, 2018.

[6]. Mustafa, Mahmoud, Mohammed Mahmoud, HuwaidaTagelsir, and Ibrahim Elshoush. "A Novel Enhanced LSB Algorithm for High Secure Audio Steganography." In *2018 10th Computer Science and Electronic Engineering (CEEC)*, pp. 125-130. IEEE, 2018.

[7]. Lahiri, Sounak. "Audio steganography using echo hiding in wavelet domain with pseudorandom sequence." *International Journal of Computer Applications* 140, no. 2 (2016): 16-19.

[8]. Tanwar R, Sharma B, Malhotra, MS. "A robust substitution technique to implement audio steganography". *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)*, 2014: 290-293

[9]. Verma, Namita, and Vinay Kumar Jain. "Audio Steganography – A Review".*International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Vol 2, no.1 (2013): 2278 – 909X*

[10]. Kumar, Samir, B. Barnali, and G. Banik. "LSB modification and phase encoding technique of audio steganography revisited." *International Journal of Advanced Research in Computer and Communication Engineering* 1, no. 4 (2012): 1-4.

[11]. Adhiya, K. P., and Swati A. Patil. "Hiding text in audio using LSB based steganography." In *Information and Knowledge Management*, vol. 2, no. 3, pp. 8-15. 2012.

[12]. Divya, S. S., and M. Ram Mohan Reddy. "Hiding text in audio using multiple LSB steganography and provide security using cryptography." *International journal of scientific & technology research* 1, no. 6 (2012): 68-70.

[13]. Bandyopadhyay, Samir Kumar. "Genetic Algorithm Based Substitution Technique of Image Steganography." *Journal of Global Research in Computer Science* 1, no. 5 (2011).

[14]. How to hide secret messages in music files. [Online]. Available at: http://www.iicybersecurity.com/audio-steganography.html [Accessed on 11-07-2019]