Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (34-39), Month: May - August 2016, Available at: www.noveltyjournals.com

Embedding of Auricular Sounds Within an Audio Using LSB

[1]Anusha R, [2]Dr. S Bhargavi

[1]Signal processing, M .Tech, SJCIT, Chickaballapur, India
[2]Professor, E&C dept, SJCIT, Chickaballapur, India

***Abstract*: Encryption of Audio Steganography is a challenging task. Computer based audio steganography involves secret message in the form of audio code. In this project the secrecy is done using the LSB technique. The proposed technique consists of two major steps namely Embedding and Extraction. At pre-processing, the target string is converted into Hexadecimal equivalent by considering four bits at a time which affects the capacity of the hidden image/data. Imperceptibility and Distortion are inversely proportional to each other. Challenge is to retrieve the stego audio successfully at the receiving end.**

***Keywords:* Audio Steganography; Modulo operator; Imperceptibility; Stego-Audio.**

I. INTRODUCTION

In today's Digital world, the data hiding is the most important concept. Abundant use of Internet by the public masses has given rise to many issues. Thus, the industry professional, researchers has to keep an eye on data confidentiality. Cryptography, Water marking, Steganography are the methods which leads this responsibility [2].

Cryptography is an art of protecting the primary information by encrypting the data into an unreadable format. Corporate data, E-mail messages, credit card information can be protected using this [3]. Overall Cryptography is time consuming, lengthy process and also fails to ensure safe communication.

Water marking is a process of using transparent image/text to protect the original image. Its wide application is in the field of source tracking. This is a passive protection tool [3] which just marks the data but fail to have the access to the data. In addition to this, it does not provide imperceptibility.

Steganography is an art and science of hiding information by embedding one message within other. The hidden image can be text, audio files, images etc., this secret data is embedded within a carrier file called cover media. Stego file obtained here is impossible to perceive with any of the senses even with the knowledge of exact location of secret data by any other party including the sender and receiver themselves [4]. The main challenges here are imperceptibility, robustness and capacity. All are contradictory to each other.

The primary goal of steganography is to reliably send hidden information secretly, not merely to obscure its presence. In this era, steganography is considered as the sub-discipline of data communication security domain. Lately, new directions based on steganographic approaches started to emerge to ensure data secrecy. Rather than as a substitute to existing solutions, these approaches could achieve better data secrecy if combined with conventional security techniques. Modern techniques exploit the characteristics of digital media by utilizing them as a carrier to hold hidden information.

Steganography can be implemented in four ways: (i) Using text(ii) Using Images (iii) Using Audio files (iv) Using Video files.

In this paper the secret message is covered using the audio files called as Audio Steganography. It uses the cover file which is known as digital audio file. The sender embeds data of any type in a digital audio file using a key to produce a stego-file in such a way that an observer cannot detect the existence of the hidden message. At the other end, the receiver processes the received stego-file to extract the hidden message[1].

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (34-39), Month: May - August 2016, Available at: www.noveltyjournals.com

Although the presence of strong tone in spectral temporal neighborhood, the psychoacoustic masking phenomenon of the Human Auditory System (HAS) renders a weak tone imperceptibility. This unusual property is due to the low differential range of HAS. When frequencies are at low power level or noise like frequencies at higher level, human ear cannot perceive those frequencies [10]. Hence, there is a necessity of frequency masking.

In addition, if the tone occurs at critical band a weak pure tone is masked by wide band noise. Thus there are different ways for embedding information using this inaudibility property of weaker sounds. Audio Steganography itself more challenging task concerned with the hiding of data in audio signal in an imperceptible way. By altering the binary sequence of audio file the secret message is embedded into the corresponding digitized audio signal. Steganography serves as a means for private and secure communications.

Most commonly used methods in Audio Steganography are Least Significant Bit (LSB) Coding: It is the fastest, easiest and the simplest of all. This algorithm replaces the LSB's of digital audio file with the corresponding message bits.

Parity Coding: Here, signals are broken down into the regions of samples instead of individual samples. Thus the each bit can be encoded in the sample region's parity bit from the secret message. If in case the selected region's parity bit does not match with the secret bit which is to be encoded, it can be flipped. Thus the sender have a greater choice of encoding the secret bit.

Phase coding: HAS is sensitive to phase change in audio signal in comparision to the signal noise. The secret message is encoded as phase shift in the phase spectrum of digital signal from which we achieve inaudibility encoding in terms of SNR.

Spread Spectrum: In this technique, the secret message is spread over all the frequencies evenly as much as possible. It is almost similar to LSB coding where the secret message bits are randomly spread over the entire sound file but, in SS the bits are spread over the sound file's frequency spectrum using the code which is independent of actual signal. The resultant signals occupies the wider bandwidth area for the transmission.

Echo Hiding: By introducing an echo into the discrete signal the information is embedded in a sound file. The advantage of this is high transmission rate like SS method and robustness against the noise. Only one bit of information can be encoded for one echo produced from the original signal. Hence, here the original signals is divided into number of encoding process. After the successful completion of encoding process it is concatenated back together to create the final signal.

II. LITERATURE SURVEY

Hacking is the popular term we often listen in today's world. Hacking can be described as an unauthorized data access at the time of transmission of data. This problem in steganography can be termed as stegoanalysis. The process in which stegoanalyzer cracks the cover object to get the hidden data is known as stegoanalysis. Thus there are many technique which are evolved and would be developed in future keeping in mind the secrecy of data. There are three prominent data embedding approaches namely hiding in temporal domain, in frequency or wavelet domain and in the coded domain.

Hiding in temporal domain employs low bit encoding techniques. LSB is the oldest method used for this purpose. Each bit of the cover audio is replaced by the message bit in a deterministic way. This allows the high embedding capacity for data. Implementation is simpler in its own way and also it can be clubbed with the other techniques. On the other hand in spacial domain, the secret data is embedded directly on the pixels of an Image.

LSB being the simplest algorithm was widely used for the implementation. But it reduces the security performance because of its low robustness characteristics to noise addition. Henceforth it is vulnerable even for the simple attacks. Stegoaudio are prone to filtration, lossy compression, amplification and noise addition which will very likely destroys the data[4]. Furthermore, the attacker can easily retrieve the secret message by just removing the entire LSB plane.

Amritpal Singh and Harpal Singh proposed Image Steganography for color images [6]. Two files are necessary here, first one is the cover image which is the color image for example scenery/image of any object. Second file is secret message to be hidden. Since, the cover image is color it is necessary to slice into their respective planes and plot the histogram technique for insertion used in LSB. Whre in, the LSB bits of cover image pixels are changed to insert secret message. Capacity is the major issue found here.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (34-39), Month: May - August 2016, Available at: www.noveltyjournals.com

Later the techniques evolved where audio was used to cover or hide secret message. Algorithm evolved to hide text within the cover audio. Prior embedding any text in the audio file, it is important to convert the audio signal into the respective bits and the text ino 5-bit code by checking the redundancy in binary code [7]. Then the text is embedded in audio file using LSB algorithm. Rating is done using 5-point scale. 8 bit WAV and 16 bit WAV audio file are supported but storage capacity of the text within an audio is too less.

Ideal data transmission in LSB Coding is 1kbps per kHz. But in some cases two message bits can be sent by replacing two LSBs. This induces noise in the audio file as well. To overcome this, text file size must be lesser than audio file contents [8]. If condition is not satisfied error occurs else the secret message can be embedded in 4^{th} and 5^{th} LSB bit as proposed.

Gupta Banik et al. proposed Audio Steganography technique using LSB modification technique and Parity technique. Presumption here is that no other third parties are aware of this secret message [8]. This is easy for implementation but induces error due to the loss of data which may occur due to the channel noise and resampling .

Advance Encryption standards was used by Aniruddha Kanhe et al. This provides secrecy, robustness and was also tested for about 30 speech files [4]. Cryptography is added in steganography which increases the robustness and also introduces the security to the higher level. This is because of the requirement of the key to decrypt the secret message. Two sets are done where in, first set includes the implementation of LSB algorithm without encrypting the message while the second set of test includes the implementation of LSB algorithm, along with secret message AES encryption and then embedded in the 1^{st} LSB. In the third set of test, the length of the encrypted secret message is placed in 4^{th} LSB in order to introduce the randomness but rest all the other constraints are retained in 1^{st} LSB. Similar procedure is followed in the fourth set of test, 4^{th} LSB position is filled with the entire key and rest retained in 1^{st} LSB. In fifth set of test, the complete set is placed in 4^{th} LSB position [9]. But this propsed technique is purely for the lossless channel.

Ramandeep Kaur et al. proposed an approach where the three messages can be embedded in a single audio file [10]. Three methods are used here namely LSB, Parity and Spread Spectrum technique instead of using the single method. In addiiton to all this BER comparision is also made.

In Audio Steganography technique proposed by Biswajitha Datta et al. modulo operator was used both at embedding and extraction step [1]. Text is embedded within the audio cover. At preprocessing the secret message which is in the string format is converted into multiples of four else the special characters can be added to make sure the condition is satisfied. It is then converted into corresponding ASCII characters and 7-bit binary. Later concatenated to embed using the modulo operator. The exact vice-versa is followed at the extraction process to recover the original signal.

III. PROPOSED METHOD

This can be understood by segregating the transmission and receiving part. On both the ends the simplest LSB technique is implemented.

A. Embedding:

The wave file in which the hidden text must be embedded is selected. Such that, the cover audio which helps in embedding the secret message should be too large. Open the wave file to hide the audio file where in, first 40 bytes make wav header and thus stores the header. The next three samples i.e, 41^{st} to 43^{rd} sample stores the length of the wav data sample.

Copy the 16 bit wav data samples starting from 44^{th} byte. Later, close the file since only wav data samples are sufficient to hide the audio. Hide the identity in first 8 wav data samples and hide binary length of the message from 9^{th} to 28^{th} samples. Hide message binary starting from 28^{th} position of wav data samples. This creates the new wav file in write mode. Copy the original wave file and the wave data samples with hidden audio in new file.

B. Extraction:

To extract the target the process as proposed in embedding is repeated exactly in the reverse order. Open the file with hidden audio (mentioned as in embedding). Read the wave data samples and close the file because only wave data samples are sufficient for extracting the audio.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (34-39), Month: May - August 2016, Available at: www.noveltyjournals.com

Extract the length of audio from 9th to 28th wav data samples. Convert the length to decimal. Extract the LSB from the wave data samples. Open the new wave file again in the write mode. Later copy the header of the original wav file and also the wave data samples with hidden audio in new file

IV. ALGORITHM

A. Algorithm for embedding:

Step 1: Start

Step 2: Read the cover audio file

Step 3: Read the target audio message

Step 4: Normalize the cover audio in 16 bits

Step 4: Store the length of the target message using the standard LSB technique

Step 5: pre-process and embed the target secret message

Step 6: Send the obtained Stego Audio to the receiver

Step 7: End

B. Algorithm for Extraction:

Step 1: Read the stego audio file..

Step 2: Extract the length of the string using standard LSB extraction rule

Step 3: post process the extracted string to get the original target string

Step 4: End

V. RESULT ANALYSIS

In this section the experimental analysis is done as shown in the figure given below. At the embedding, the cover audio is shown in the Figure 1

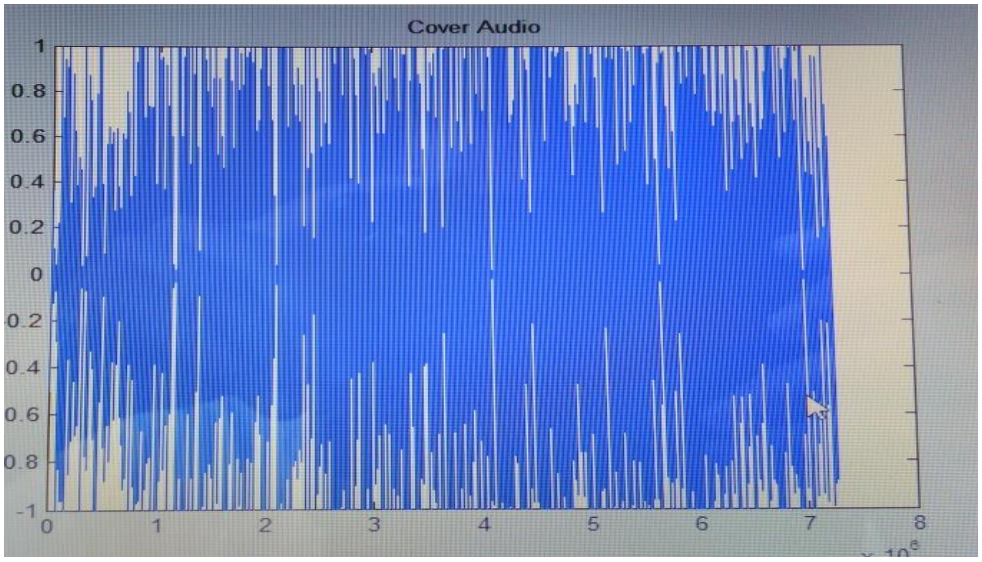

Figure 1

The cover audio in this paper is taken from the English movie clipping. In the cover audio the secret audio /message is hidden. The graph of secret audio of beep is shown in the figure 2.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (34-39), Month: May - August 2016, Available at: www.noveltyjournals.com

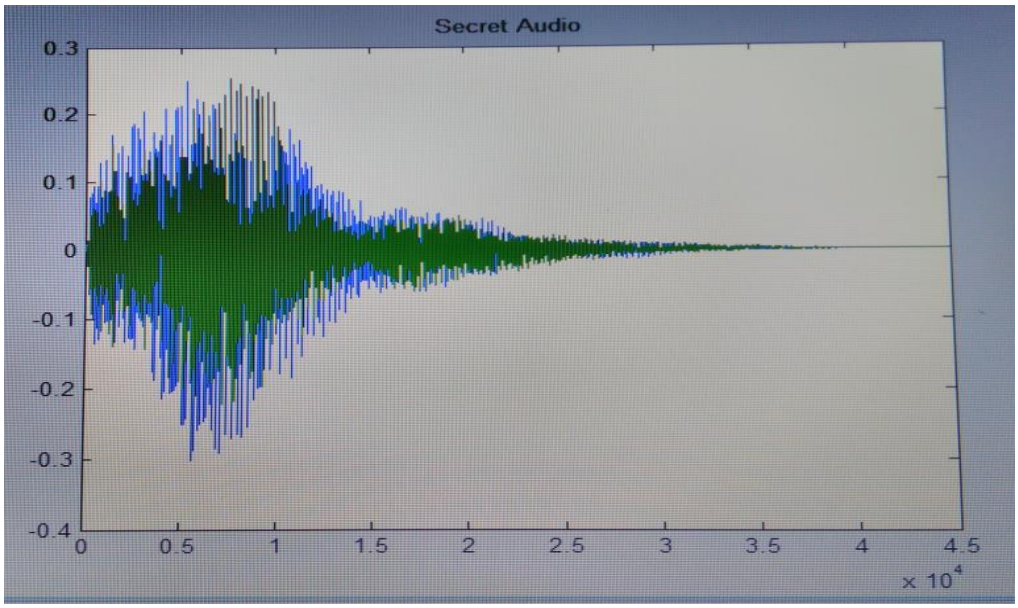

Figure 2

Then we obtain a window as shown in figure 3, which tells the folder name of the secret message that is stored.

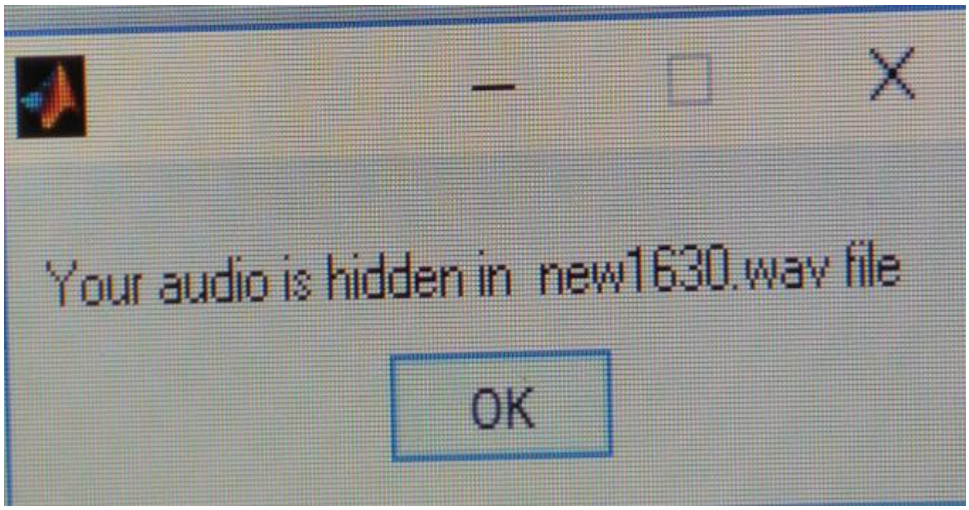

Figure 3

At the decoder the same procedure is repeated. If the secret message is obtained as shown in the figure 2, then the audio streganography is successfull. If the message which is to be hidden is too long then the error occurs.

VI. CONCLUSION

In today's e-world technology steganography place an important role. In this paper audio message/ file is embedded within an audio using LSB coding. The disadvantage of this is that the secret message that is to be embedded must be too short, when compared to the cover audio. This cover image must 11 times larger than the secret audio file. In future this can be increased using modulo operator.

ACKNOWLEDGMENT

Very grateful to VTU and SJC Institute of Technology for providing a helpful environment to make this project successful.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (34-39), Month: May - August 2016, Available at: www.noveltyjournals.com

REFERENCES

[1] Biswajitha Datta, Souptik Tat and Samir Kumar Bandyopadhyay, "Robust High Capacity Audio Steganography using Modulo Operator", IEEE 2015.

[2] Padmashree G, Venugopala P.S, "Audio Steganography and Cryptography using LSB algorithm at 4th and 5th LSB layers", IJEIT, vol 12. Oct 2012.

[3] Prof. Samir Kumar, Bandyopadyay Parbali, Gupta Banik, "LSB modification and Phase encoding technique of Audio Steganography revisited", journal, June 2012.

[4] Aniruddha Kanhe, G Aghila, Hanuma Ramesh, "Robust Audio Steganography based on Advanced Encryption standards in Temporal Domain", IEEE 2015.

[5] Ramandeep Kaur, Abhishek Thakur, Hardeep Singh Saini, Rajesh Kumar, "Enhance steganographic Method preserving Base quality of information using LSB, Parity and spread spectrum technique", IEEE 2015.

[6] Amritpal Singh, Harpal singh, "An improved LSB based Image steganography techniques for RGB Images", IEEE 2014.

[7] K P Adhiya, Swati A Patil, "Hiding text in Audio using LSB based stegabography", ISSN, vol 2, 2012.

[8] "audio steg: methods", Internet publication on http://www.snotmonkey.com/work/school/405/methods..

[9] N. Cvejic and T. Seppänen "Increasing the capacity of LSB based audio steganography", Proc. 5th IEEE International Workshop on Multimedia Signal Processing, St. Thomas, VI, December 2014.

[10] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding - A Survey", in Proc. of the IEEE, special issue on protection of multimedia content vol. 87.