Overcoming Audio Steganography limitations and increase capacity

Gaytri Tanwar[1], Sarika Rana[2]
[1]*M.Tech (CS), DITMR Faridabad, INDIA*
[2]*Asst. Prof., DITMR Faridabad, INDIA*

Abstract- **In this paper, an attempt is done to implement audio steganography technique. The technique will provide higher data embedding capacity. The increase in capacity will not compromise with the robustness of the technique to various intentional as well as unintentional attacks.**

Index Terms- **Robust, audio sample, capacity, attacks.**

I. INTRODUCTION

The increasing rate of usage of internet and the revolution that occurred in digitization of information; the overall structure of modern communication is changed. The revolution in software industry and semiconductor industry made it feasible that hardware as well as software are more user-friendly and flexible and enables consumers to communicate multimedia data. Peoples are now able to transmit large multimedia files through broadband connection. Moreover, the transmission thus done is almost errorless [2]. Security of data to transmit is of high concern in today's communication system. Data hiding is a technique of providing data security.

Steganography is the art and science of hiding information such that its presence cannot be detected[1]. The secret information is hidden in some carrier file and then transmitted. The carrier file can be an image, Audio file, text file, video file, etc. Due to real time availability and efficiency of HAS, audio is used as carrier in proposed method. The secret message is hidden in an audio file by doing negligible alterations in the audio file. In history, several algorithms were proposed for the embedding and extraction of message in audio signals.

All the algorithms developed are based on the fundamental idea of masking effect possessed by Human Auditory System (HAS). The message thus hidden in audio signal in transparent manner[3].
Using audio file as a cover medium instead of image is more tedious [8], as Human Auditory System (HAS) is more sensitive than Human Visual System (HVS). As the HAS is more sensitive and encoding and decoding of audio is more complex, thus there are not algorithms and techniques as much as exist for image; However audio files are available anywhere. Thus working on audio and improvement in related techniques is needed[8].

Mainly 3 formats of audio files are popular: Sample Quantization, Temporal Sampling Rate and Perceptual Sampling[11].

Sample Quantization which is 16-bit linear sampling architecture used by popular audio formats such as (.WAV and .AIFF).

Temporal Sampling Rates uses selectable frequencies (in the KHz) to sample the audio.

The last audio format is Perceptual Sampling [2]. In this format, only those parts of the audio are encoded which are perceived by the listener. Thus the statistics of the audio are changed drastically and the signal gets changed. This format is used by the most popular digital audio on the internet today in ISO MPEG (MP3) [2].

II. RELATED WORK

K.P. Adhiya and Swati A. Patil 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. In the method 16bit WAV and 8bit WAV audio file are supported. The proposed algorithm gives better result for 16 bit wave audio as compared to 8 bit [4].

Prof. Samir Kumar Bandyopadhyay and Barnali Gupta Banik give an overview of two primitive techniques to get an idea of how steganography in audio file works. LSB modification and Phase Encoding techniques are very primitive in steganography. This method is easy to implement but is very susceptible to data. This method can be used only when a small amount of data needs to be concealed [5,7].

Jayaram P, Ranganatha H R, Anupama H S discuss different type of audio steganographic methods, advantages and disadvantages. They proposed that audio data

hiding techniques can not only be used for secure communication but also for some other purposes like data storage, tracing information, finger printing and tamper detection, etc [6].

R Sridevi, Dr. A Damodaram and Dr. SVL. Narasimha give basic idea behind to provide an efficient method for data hiding. The data will be secure from hackers and send to the destination in a more secure and safe way. The size of cover audio does not change after encoding even the system supports so many formats. The quality of sound was a consequence of the message length that is to be hidden and the size of the audio file that serves as cover [9].

III. SUBSTITUTION TECHNIQUES OF AUDIO STEGANOGRAPHY

Initially steganographic systems were developed for digital images and video files. Later on with the tremendous increase in use of digital audio for multimedia communication the interest moved towards audio steganography. There are so many attacks that are malicious against

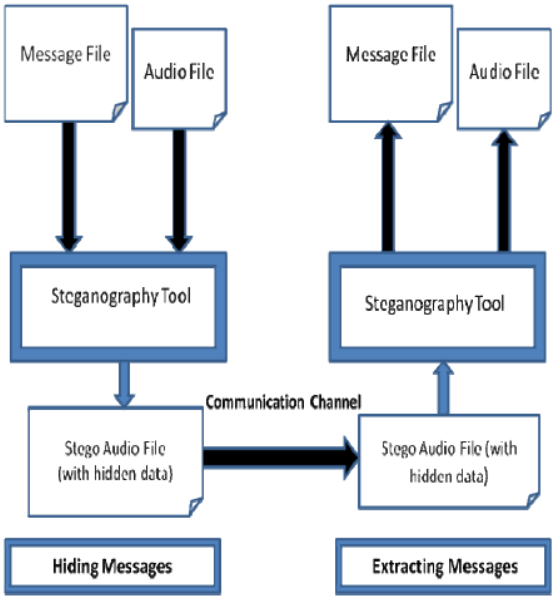

Figure 1. Audio Steganography Process

image steganography algorithms (e.g. geometrical distortions, spatial scaling, etc.) but when these attacks are tested against audio steganography techniques, they were not as much effective. Moreover there are not so many steganalysis techniques that can be used by attackers against audio steganography.

The substitution technique is based on the idea that if a single bit or a few bits in each audio sample are replaced with the message bits then the change thus occurred will not be noticeable to the human ear (type of file matters). The capacity of this method is very high (41,000 bps). The robustness of this method is very low. This method is however easy to implement but susceptible to various attacks.

The prime reason for choosing this technique lies in the advantage of using substitution technique which is a very high capacity for hiding a message. When only single LSB replacement is done per host audio sample a capacity of 44.1 kbps can be achieved. However there are certain other techniques like spread spectrum (4 bps) having lesser capacity but they are more robust. [10].

IV. PROBLEMS IN TRADITIONAL SUBSTITUTION

AUDIO STEGANOGRAPHY TECHNIQUES

A multimedia technique is said to be good if it satisfies three basic requirements: Perceptual Transparency, Capacity of Hidden data and Robustness. The same rule must be hold for audio steganography techniques.

The steganography techniques can be categorized as of two types: one that tries to reveal the message and another one that tries to destroy the hidden message. Substitutions techniques are vulnerable against both types of attacks. The attack that tries to reveal the hidden message must have the knowledge of hiding process. Since the bits of lower layers are the targets for replacement in substitution techniques, it is not much difficult to reveal the hidden message as the suspicious transmission due to low transparency may drive attention.

One more categorization of attacks can be intentional and unintentional attacks. The unintentional attacks like noise, transition distortions could destroy the hidden message without intention. The chances are more if it is hidden in the bits of lower layers in the sample LSBs.

The above discussion can be summarized as following problems of substitution techniques of audio steganography:

1) Low robustness against intentional attacks which try to reveal the hidden message.
2) Low robustness against distortions with high average power (unintentional attacks).

One possible solution to withstand intentional attacks that tries to reveal the message is making more difficult discovering which bits are modified. As it is known that LSBs are more suspicious, thus if the embedding is done in the bits other than LSBs then it would be helpful to increase the robustness against intentional attacks. Furthermore the

statistical values of the sample are changed after embedding process. In order to minimize the changes thus occurred the values of some other bits (other than used for data hiding) are changed willingly. Now the final modified audio file is not as much deviated from the original one.

V. THE SOLUTION

From above discussion, the following two solutions for above mentioned problems can be possible:

1) Making the embedding process more difficult, use bits other than LSB's for substitution.
2) Use bits in deeper layers for substitution and other bits should be altered willingly to decrease the amount of error induced.

Conclusively both the above solutions can be combined by embedding the message bits in deeper layers; that is "modifying the bits else than LSBs in samples". In addition "other bits alteration to decrease the amount of error" should also be adopted.

Audio sample: 1001***11***01 (value 157)
Message bits: 0 and 1
After substitution: 1001***01***01 (value 149)
After modification: 1001***01***11 (value 151)

VI. THE PROPOSED WORK

The proposed work is based on the solutions discussed to avoid common problems in substitution techniques. The work is explained as the steps to be done at sender side and at the receiver side as shown in Figure 2.

A. Sender side:

a.) Convert the secret message to hide in first in ASCII and then in binary format.
b.) Make a copy of the audio file selected and convert it into binary format.
c.) Check the audio file for its capacity to hide the given message. If it succeeds then move to next step.
d.) Keep the header part intact, read the audio samples bytes from starting and replace their 3rd and 4th LSB's with the two message bits. In order to minimize the distortion thus induced alter the 1st,2nd and 5th bits willingly.
e.) Now read the next audio sample byte and increase the count by two to point to next message bits.
f.) Repeat steps-d and step-e until the count exceeds message length.
g.) Hide the length of the message (already converted into binary) in last 4 bytes of audio samples starting from the 4th last with the same process used for hiding message bits.
h.) The stego file thus obtained differs negligible in statistical values from the original audio file in sample values
i.) The file is now ready for transmission.

B. Receiver Side:

a.) Last 4 bytes of the audio file received are read starting from the 4th last. The 3rd and 4th LSBs of each byte are collected to finally calculate the length of the message.
b.) Now start reading the audio samples from first byte (excluding the header). The 3rd and 4th LSBs of each byte are copied in some data structure until the number of bits copied equals to number of bits equivalent to the length of the message.
c.) The bits thus obtained are first converted to ASCII and then finally into characters to form the secret message.
d.) The bits thus obtained are first converted to ASCII and then finally into characters to form the secret message.
e.) The message that was hide by the sender is now obtained by the receiver.

VII. RESULT ANALYSIS

The result can be analysed using following figures. Fig 3 compares the frequence spectrum while figure1and 2 gives the histogram.

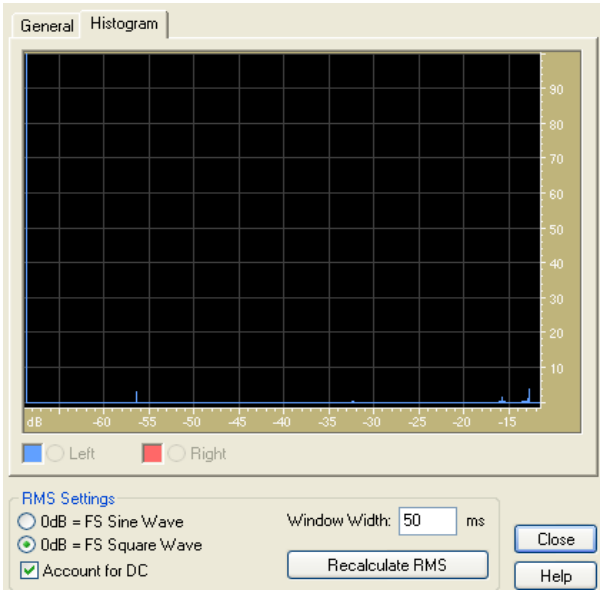

Fig 1. Cover Audio Histogram

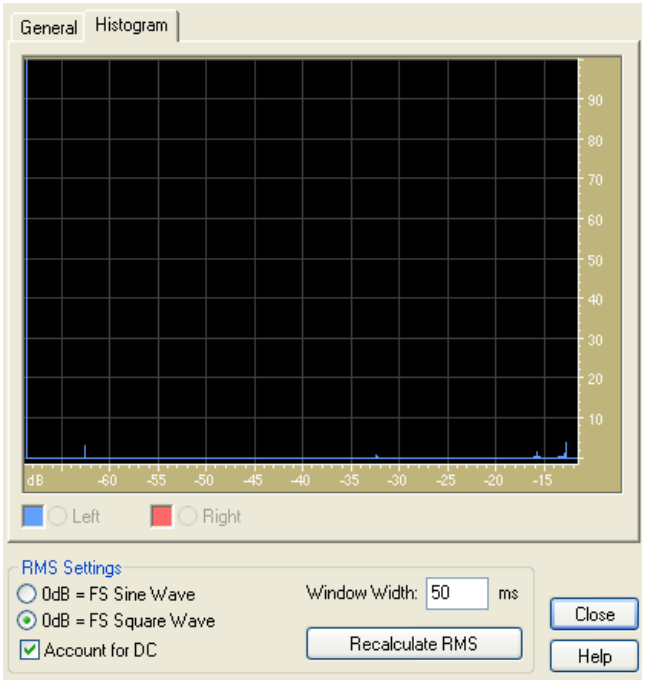

Fig 2. Stego Audio Histogram

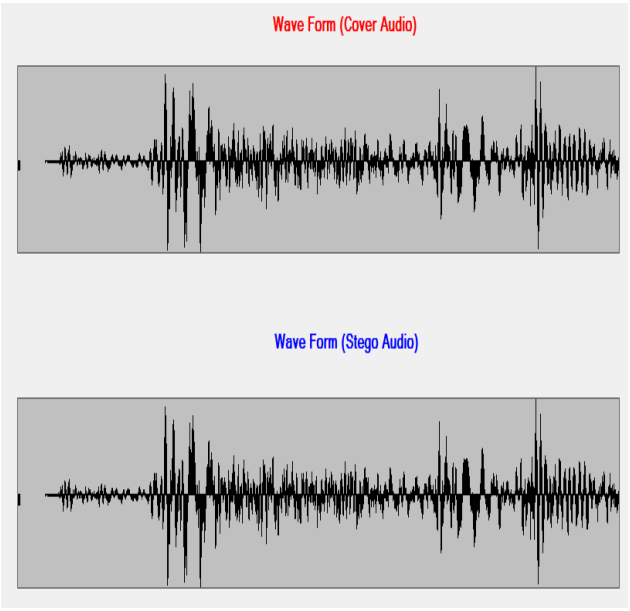

Fig 3. Wave Forms comparision

VIII. CONCLUSION

The basic problems in using substitution techniques are identified and the possible solutions are then proposed too. This paper proposes a new approach that overcomes the problems of substitution techniques in audio steganography. One problem is that they are less robust against intentional attacks that try to reveal hidden message and second problem is having low robustness against unintentional attacks like distortions with high average power. The algorithm will hide the message as per the proposed solution (in deeper layers of audio sample and will modify other bits to minimize the error). The method currently uses 2 bits per byte of audio sample. This will progress towards achieving higher capacity and robustness.

REFRENCES

[1]. Rohit Tanwar, Sunil Kumar, Narender Gautam, Ravinder Gautam," A Spatial Domain Steganography Technique Based on Optimal Solution Using Genetic Algorithm", January 2013,Page(s):228-232.ISBN:978-93-81583-82-1

[2]. Gunjan Nehru, Puja Dhar,"A detailed look of audio steganographic techniques using LSB and Genetic Algrithm approach", IJCSI Vol.9, Issue1, No.2, January 2012 ISSN(online): 1694-0814.

[3]. Juhi Saurabh, Asha Ambhaikar,"Audio Steganography using RPrime RSA and GA Based algorithm to enhance security", IJSR (online) ISSN:2319-7064, Vol-1,Issue-2, November 2012.

[4]. K.P.Adhiya and Swati A. Patil, " Hiding Text in Audio Using LSB Based Steganography" in Information and Knowledge Management Vol. 2, No.3, 2012.

[5]. Prof. Samir Kumar Bandyopadhyay and Barnali Gupta Banik , "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited" in International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012.

[6]. Jayaram P, Ranganatha H R, Anupama H S, " INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY" in The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.

[7]. Samir Kumar Bandyopadhyay and Biswajita Datta" Higher LSB Layer Based Audio Steganography Technique" in IJECT Vol. 2, Issue 4, Oct . - Dec . 2011

[8]. Zamani, M. Manaf, A.A. , Ahmad, R.B., Zeki, A.M., & Abdullah, S."A genetic algorithm based approach for audio steganography", World Academy of Science, 2009

[9]. R SRIDEVI, DR. A DAMODARAM, DR. SVL. NARASIMHAM, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security", in Proc. JATIT PP:768-771,2005-2009.

[10]. Bret Dunbar, "A Detailed Look at Steganographic Systems and their Use in Open-Systems Environment" in SANS Institute Infosec Reading room, August 01, 2002,url:http://www.sans.org/readingroom/whitepapers/c

overt/detailed-steganographic-techniques-open-systems-environment-677

[11]. Pal S.K., Saxena P.K. and Mutto S.K, "The Future of Audio Steganography", Pacific Rim Workshop on Digital Steganography, Japan, 2002.