Literature Review on Audio Steganographic Techniques

Jithu Vimal[1]

[1]PG Student, Dept. of ECE, Mar Baselios College of Engineering and Technology, Trivandrum, Kerala, India

***Abstract*— Steganography is the technique of hiding secret message in a cover medium in such a way that only the sender and the intended recipient knows the existence of communication. Audio steganography is concerned with hiding information in a cover (host) audio signal in an imperceptible way. The main challenge in audio steganography is to increase the capacity of steganographic system. In this paper, we discuss different audio steganographic techniques, their potentials and limitations to ensure data security.**

***Keywords*— Steganography, Audio Steganography, Data Security.**

I. INTRODUCTION

Digital communication has become an essential part of infrastructure nowadays and also lots of applications are internet based. So the communication made must be secret. Techniques such as cryptography are being used on a large scale for transmitting information secretly. Steganography is a new approach of providing secure data transmission. The term steganography is derived from two greek words, “stegano” means “secret” and “graphy” means “writing”. So steganography literally means secret writing hide the secret message in a cover medium so that it cannot be seen. Audio Steganography hides the secret message in an audio signal called cover audio. Once the secret message is embedded in the cover audio, the resulting message is called stego message and stego message is transmitted to the receiver side.

For any audio steganographic technique to be implementable it must satisfy three conditions [1]:

Capacity means the amount of secret information that can be embedded within the host message

Transparency evaluates how well a secret message is embedded in the cover audio

Robustness measures the ability of secret message to withstand against attacks

The basic block diagram of a steganographic system is shown in Fig.1. The secret message to be transmitted is embedded inside a cover file. Cover file could be images, videos or audio. A stego key is also used to provide security. Using a suitable embedding algorithm secret message is embedded into the carrier object. The resultant file is called stego file and this stego file is transmitted to the receiver side. At the receiver side stego file is decoded using the stego key

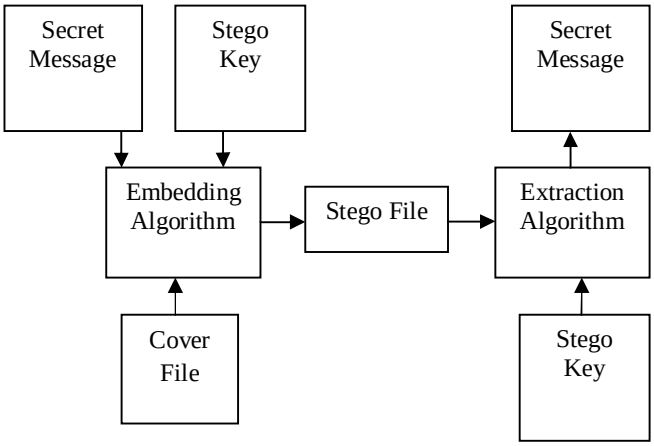

Fig. 1 Steganographic System

to extract the secret message. In the case of an audio steganographic system cover file is an audio file

While hiding the secret data one has to be keep in mind that the header part of the wave file ie. first 44 byte [2] should be unaltered because in case the header gets corrupted, the audio file will also corrupt. Another consideration that should be made is not to embed data into the silent zone [3] as that might cause undesirable change to the audio file

At present, there is lot of research is being made on audio steganography. This paper presents literature review of few of the methodologies of audio steganography.

Figure 2 shows the wave file format.

II. HISTORY

The first steganographic technique was developed in ancient Greece around 440 B.C. The Greek ruler Histaeus employed an early version of steganography. He shaved the head of a slave and then tattooed the message on the slaves scalp, waited for the hair to grow to cover the secret message. Once the secret message is covered he sent the slave on his way to deliver the message. The recipient shaves the slave’s head to read the message.

Null ciphers were also used to send secret messages. Null ciphers are messages which contain secret messages embedded in the current text. An example of null cipher is:

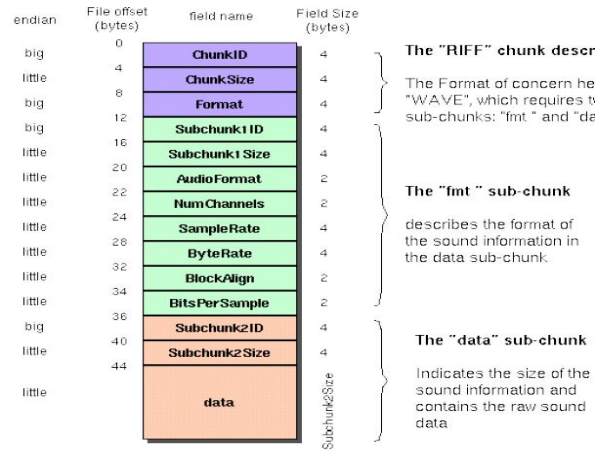

Fig 2. Wave File Format [2]

"Missing feel mind and boat strength admit masterful transparent randomness side moment proposed many step way."

By taking the third letter in each word we get the secret message as follows:
Send arms and money.

III. LITERATURE REVIEW

1. Muhammad Asad, Junaid Gilani, Adnan Khalid proposed a three layered model for audio steganography based on least significant bit replacement [1]. The secret message to be transmitted is passed through two layers before it is embedded within the cover message in the third layer. The stego message is transmitted over the network to the receiver side and the secret message is recovered by performing reverse operations in reverse order. The objective of the paper is to make sure the confidentiality of the secret message. They also discussed the implementation issues of the three layered model with respect to different parameters like capacity, transparency and robustness. Experimental results have shown that three layer model achieved a signal to noise ratio of 54.78dB in comparison to 51.12 dB of conventional LSB method.
2. Lovey Rana, Saikat Banerjee implemented an audio steganographic system that provides improved security [4]. To achieve this, dual layer randomization approach is used. First layer of randomization is achieved by randomly selecting the byte number or samples. An additional layer of security is provided by randomly selecting the bit position at which embedding is done in the selected samples. Using this proposed algorithm the transparency and robustness of the steganographic technique is increased.
3. Kirti Gandhi, Gaurav Garg introduced a method which is a variant of well-known LSB method [5]. Due to less robustness and more vulnerability to be attacked LSB method is not preferred. Instead two bits (2nd and 3rd LSB's) are used for hiding message. This will increase the data hiding capacity also. A filter is designed to minimize the changes occurred in stego file. The stego file along with the filtered file thus obtained is used to generate a unique key. The filtered file and the generated key will be transmitted to receiver. The key will derive to extract the correct message at receiver's end.
4. Bankar Priyanka R., Katariya Vrushabh R., Patil Komal K. presented a novel approach of submission technique of audio Steganography [6]. Using genetic algorithm, message bits are embedded into multiple and higher LSB layer values, resulting in increased robustness. The robustness would be increased against those intentional attacks which try to reveal the hidden message and also some unintentional attacks like noise addition as well.
5. Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar presented a method known as Least Significant Bit (LSB) method [7]. In LSB method consecutive LSB's in each sample of cover audio is replaced with secret message bit. LSB method is very easy to implement but have low robustness. The paper also compares the spectra of original audio signal before embedding and audio signal after embedding.
6. S.S. Divya, M. Ram Mohan Reddy discussed a method of hiding text in audio using multiple LSB steganography and provide security using cryptography [8]. For 16 bit per sample audio sequences the maximum number of bits that can be altered for LSB audio steganography without affecting the quality of host audio signal is 4 LSBs. The research has proposed two novel approaches of substitution technique of audio steganography that improves the capacity of cover audio for embedding additional data. Here message bits are embedded into multiple and variable LSBs. These methods utilize up to 7 LSBs for embedding data. From the results these methods improves the capacity of data hiding of cover audio by 35% to 70% as compared to the standard LSB algorithm which uses 4 LSBs for data embedding.
7. Gunjan Nehru and Puja Dhar studied a detailed look of audio steganography techniques using LSB and genetic algorithm approach [9]. This research has study of various techniques of audio steganography using different algorithms like genetic algorithm approach and LSB approach. It has tried some approaches that help in audio steganography. It has the art and science of writing hidden messages in such a way that only the sender and intended recipient suspects the existence of the message.
8. Ajay.B.Gadicha explored a new 4th bit rate LSB audio Steganography method that reduces embedding distortion of the host audio [10]. Using the proposed algorithm, Message bits are embedded into 4th LSB layers, resulting in increased robustness against noise addition. Hearing tests showed that perceptual quality of audio is higher in the case of the proposed method than in the standard LSB method.
9. Mazdak Zamani *et.al* described the problems faced by substitution technique and solution to the problems [11].

The main problem is low robustness against attacks. Two types of attacks are there. One type of attack tries to reveal the hidden message and other tries to destroy the hidden message. In conventional LSB method secret message is embedded in the least significant bit. This method is more vulnerable to attack. So by embedding message in bits other than LSB more security can be achieved. More robustness can be achieved if message is embedded into deeper bits. But the problem is that as one move into the MSB's the host audio signal gets altered. This problem can be solved by an intelligent algorithm which embeds the message bits in the MSB and alter other bits to decrease the error. Using this intelligent algorithm message bits can be embedded into multiple MSB's to achieve higher capacity and robustness.

10. R. Sridevi, Dr. A Damodaram and Dr. SVL. Narasimham proposed an efficient method of audio steganography by modified LSB algorithm and strong encryption key with enhanced security is proposed [12]. Enhanced Audio Steganography (EAS) is a combination of audio Steganography and cryptography. EAS proceeds in two steps: it uses most powerful encryption algorithm in the first level and in the second level it uses a modified LSB (Least Significant Bit) algorithm to embed the message into audio.

IV. APPLICATIONS

Audio steganography is use in wide range of applications. Few applications are discussed below:

1. Secret Communication: To maintain patient's medical records secrecy, [13] proposed multilevel-access control audio steganography system to telemedicine users for secure transmission of medical images. The system embeds medical images in audio files which is send to different recipients such as doctors' in-charge of the corresponding patient. For more security, only intended recipients having the knowledge of a key will be able to extract the medical images.

2. Data Storage: Audio Steganography could be used in subtitled movies where actors' speech, film music, background sounds could be used to embed the text needed for translation [14].

V. CONCLUSION

Communicating secretly without giving away any kind of crucial information is very important now a days in many fields. In this paper we presented some audio steganographic systems. Hence, up to date the main challenge in digital audio steganography is to obtain robust high capacity steganographic systems. So the objective of designing an audio steganographic system that ensures high capacity and security of embedded data has led to great diversity in the existing steganographic techniques.

ACKNOWLEDGMENT

I would like to thank the almighty for giving me the strength to work on this subject and coming up with this literature review paper. I am grateful to my family for supporting me and praying for me. I would like to express my gratitude towards the professors of Mar Baselios College of Engineering and Technology for their valuable guidance..

REFERENCES

[1] Muhammad Asad, Junaid Gilani, Adnan Khalid, "Three Layered Model for Audio Steganography", 2012 International Conference on Emerging Technologies (ICET)

[2] https://ccrma.stanford.edu/courses/422/projects/WaveFormat/ (last accessed on 20th February 2013).

[3] Masahiro Wakiyama, Yasunobu Hidaka, Koichi Nozaki, "An audio steganography by a low-bit coding method with wave files", 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 530 - 533.

[4] Lovey Rana, Saikat Banerjee, "Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding" , International Journal of Engineering and Innovative Technology, Volume 2, Issue 8, February 2013

[5] Kirti Gandhi, Gaurav Garg, " Modified LSB Audio Steganography Approach" International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6, June 2012, pp 158-161

[6] Bankar Priyanka R., Katariya Vrushabh R, Patil Komal K, "Audio Steganography using LSB'', International Journal of Electronics, Communication and Soft Computing Science and Engineering, March 2012, pp 90-92

[7] Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar, "Data Hiding Technique: Audio Steganography using LSB Technique", International Journal of Engineering Research and Applications, Vol.2, No.4, May-June 2012, pp 1123-1125

[8] S.S. Divya, M. Ram Mohan Reddy, "Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography", International Journal of Scientific &Technology Research, Vol. 1, pp. 68-70, July 2012.

[9] Gunjan Nehru and Puja Dhar, "A Detailed Look Of Audio Steganography Techniques Using LSB And Genetic Algorithm Approach", International Journal of Computer Science (IJCSI), Vol. 9, pp. 402-406, Jan. 2012.

[10] Ajay.B.Gadicha, "Audio wave Steganography", International Journal of Soft Computing and Engineering (IJSCE), Vol. 1, pp. 174-177, Nov. 2011.

[11] Mazdak Zamani *et.al* , "A Secure Audio Steganography Approach", International Conference for Internet Technology and Secured Transactions 2009.

[12] R Sridevi, Dr. A Damodaram and Dr.Svl. Narasimham, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key With Enhanced Security", Journal of Theoretical and Applied Information Technology, pp. 771-778, 2009.

[13] J. Nafeesa Begum, K. Kumar, Dr. V. Sumathy, "Design And Implementation Of Multilevel Access Control In Medical Image Transmission Using Symmetric Polynomial Based Audio Steganography", Int. J. Comput. Sci. Inf. Security **7**, 139–146 (2010).

[14] **Fatiha Djebbar** *et.al* , "Comparative Study of Digital Audio Steganograhic Techniques", *EURASIP Journal on Audio, Speech, and Music Processing* 2012