Secured Data Transmission Based On Audio Waves

Anshu Fulekar[1] , Tejal Jhambulkar[2] , Umadevi Chute[3], Gaurav Malode[4] , Minal Ukinkar[5]
[1, 2, 3] Dept of I.T.
[4, 5]Assistant Professor, Dept of I.T.
[1, 2, 3, 4, 5] Gurunanak Institute of Engineering and Technology, Nagpur, India

Abstract- *Drastic increase in the usage of electronic communication needed security of data being transmitted. Steganography is one such technique of hiding the message in a chosen carrier such that no one except the intended receiver is aware of its existence and hence prevents unauthorized access. The goal of Audio steganographic technique is to embed data in audio cover file that must be robust and resistant to malicious attacks. This paper discusses various audio steganographic methods like LSB, echo hiding, spread spectrum .The basic idea proposed in this paper is replacement of the bits according to the distortion afforded, with lossy or lossless hiding and recovery. Numbers of bits of the samples in cover file are replaced in accordance with the message bits and size of the message file to be embedded. By using reverse algorithm embedded message file is recovered. Proposed method is a novel for wave steganography for 8 bit/16 bit mono/stereo wave files.*

Keywords- Audio steganography, steganalysis, HVS, HAS, embedding capacity, robustnes

I. INTRODUCTION

Rapid and sudden increase in the Transmission of digital data over the Internet forced researchers for enhancement in the security system. Various alternatives are presented in this regard like cryptography, watermarking. But steganography has gained much importance in this context. Steganography is the art of 'secret writing'. It conceals the existence of hidden message and allows it to be only extracted by intended recipient. It adds twolayer protection against cryptography because cryptography only changes the message form but its existence is not hidden, while steganography even hides its presence [1]. The sender produces a stego file by embedding the secret message using a key in the digital cover so that an intruder cannot feel the presence of hidden message. The recipient of the message then extracts the hidden message by processing the stego file [3]. Thus, the host message is the one which embeds secret data in it. There are various options which can be used as a cover signal like images, audio signal, video files etc. Embedding secret data in digital audio cover is more challenging than using digital images as a cover since human visual system(HVS) is less sensitive in comparison to human auditory system(HAS) [2]. Figure 1 shows an example of audio steganography, here audio cover file is being used to hide secret data.

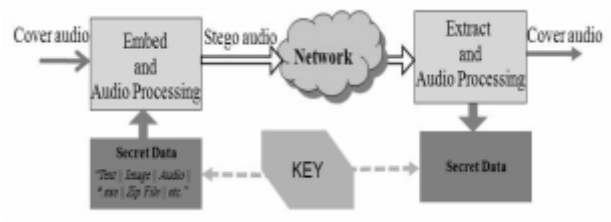

Figure 1.1 Block diagram for audio steganography[9l

There are three major parameters of audio steganography technique as shown in figure 2: Perceptual Transparency: the cover file containing secret data i.e. stego file must be perceptually indistinguishable [4]. Robustness: measures the capability of embedded data how it can face intentional or unintentional attacks. Unintentional attacks could be like conversion from analog to digital format, re-sampling etc. and intentional attack could cover cropping, resizing etc in case of image steganography schemes [5]. Capacity can be defined as the amount of data that can be embedded in the information hiding scheme thereby not disturbing the perceptual transparency so that an observer cannot detect the presence of secret data. In case of audio cover file it measures the amount of data that can be hidden in the cover audio signal. Capacity is measured in terms of percent (%) and even in bits per second audio signal [6]. In this review audio file is used as a cover for secure communication between two parties and various audio steganographic methods have been illustrated in the later sections.

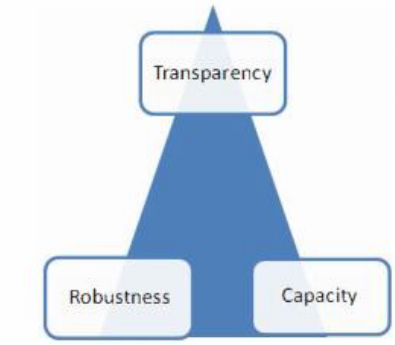

Figure 1.2 Magic Triangle

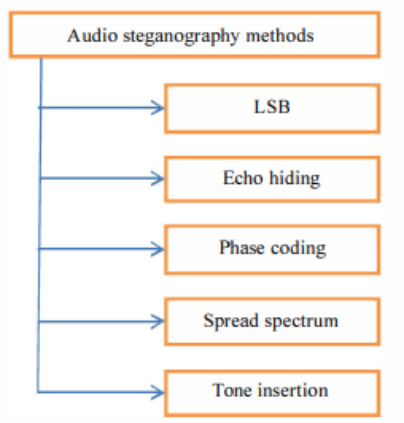

Figure 1.3 Different steganography Techniques

II. AUDIO STEGANOGRAPHY METHODS

2.1 All LOW BIT ENCODING

It is the earliest method used for information hiding [3]. It is a simple method too. LSB is the common name used for it which stands for least significant bit. It works by embedding each bit of the secret message in least significant bit of the cover audio samples. The weightage of LSBs is very small as compared to the weightage of the whole audio sample

Advantage: Capacity for hiding data is significant in LSB method.

Disadvantage: In addition to low robustness, it is also not immune to manipulation. Message can be extracted easily.

2.2 ECHO HIDING

In order to embed data in the audio signal a short echo is introduced to the audio signal. It exploits human perception by adding echo to parts of cover audio signal. In echo hiding method there are three parameters that are to be manipulated for hiding data in the echo signal and these are: decay rate, offset and amplitude so that echo is inaudible [8].

Advantage: HAS is not easily able to detect the presence of additional data.

Disadvantage: Embedding capacity is less and this method is Less secure too. Therefore, this method is not much used in recent researches.

2.3 PHASE CODING

This method is based on selecting the phase components within the original speech spectrum and replacing the components by the data to be hidden. Phase components modification must be kept small to ensure inaudibility [12]- [15]. This method is resistant to signal distortion as compared to other data hiding techniques [3]. Authors in [12] have used a strategy known as multiband phase modulation to insert data within phase components.

Advantage: Tolerates better signal distortion. Resistant to compression.

Disadvantage: Not immune to low-pass filtering and low Capacity

2.4 SPREAD SPECTRUM

Spread spectrum method makes use of a code which does not depend on the original signal and spreads the secret message along the frequency spectrum of the audio signal [9]. Even if there is interference on some frequencies this method permits signal reception. Spread spectrum is of two types namely, frequency hopping spread spectrum and direct sequence spread spectrum and audio steganography can use both of these [16]. In case of frequency hopping method the frequency spectrum of the audio signal can be altered in order to rapidly hop between frequencies [17].

Advantage: Provides better robustness.

Disadvantage: Vulnerable to time scale modification.

2.5 TONE INSERTION

Tone insertion method takes advantage of limitations in human auditory system, i.e. low power tones are inaudible in light of louder ones [19]. This audio steganographic method operates by inserting the weak power tones in presence of higher tones such that the lower power tones cannot be heard [7].

Advantage: Concealed data is not easily perceivable.

Disadvantage: It is less secured technique.

III. METHODOLOGY

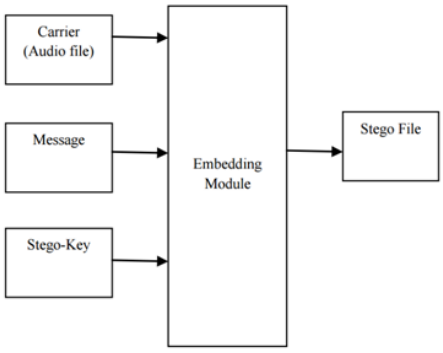

Figure 3.1 Basic Audio Steganographic Model

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. 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. The cover-file with the secret I nformation is known as a stego-file.

The information hiding process consists of following two steps:

Firstly, 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.

3.1Proposed Work

Problem Definition:

The basic aim of problem analysis is to obtain a clear understanding of the needs of the client and end users, what exactly is desired from software, and what are the constraints on the solutions. A good problem statement should be short succinct – 1 or 2 statements is best. It is a good idea to define the problem and scope as early as possible, before getting deeper into analysis of the detailed requirements. In today's society the most practical implementation of steganography is used in the world of computers.

Data is the heart of computer communication and over the year a lot of methods have been created to accomplish the goal of using steganography to hide data. The trick is to embed the hidden object into a significantly larger object so the change is undetectable by the human ear. The best object up to this writing is probably a digital audio. It is important to understand the process by which digital steganography takes place, and to make sure your cover audio is large enough to support the byte manipulation.

The basics of embedding data rely on three different facts. These three items are capacity, security, and robustness. Capacity means the amount of data that can be hidden in the cover audio. Security is the interceptor's ability to decipher the data hidden inside the cover audio. Finally, robustness means the amount of manipulation a cover audio can handle before it is obvious a change has taken place. Among different information hiding techniques proposed to embed secret information within audio file, Least Significant Bit (LSB) coding method is the simplest way to embed secret information in a digital audio file by replacing the least significant bit of audio file with a binary message. Hence LSB method allows large amount of secret information to be encoded in an audio file.

Steps to hide secret information using LSB are:

- Covert the audio file into bit stream.
- Convert each character in the secret information into bit stream.
- Replace the LSB bit of audio file with the LSB bit of character in the secret information.

This proposed method provides greater security and it is an efficient method for hiding the secret information from hackers and sent to the destination in a safe and undetectable manner. This proposed system also ensures that the size of the file is not changed even after encoding and it is also suitable for any type of audio file format.

Implementation

The All the Graphical User Interface is created using Swing API.

Figure 4.1Main Application Window

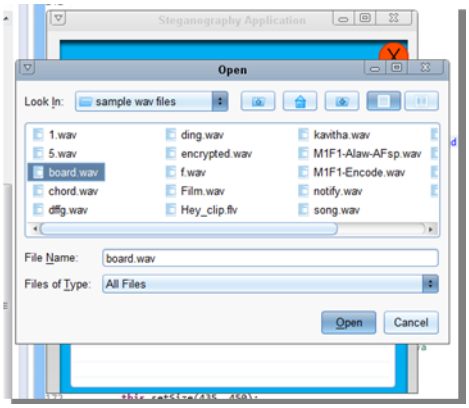

Figure 4.2 Source File Selection Dialog Box

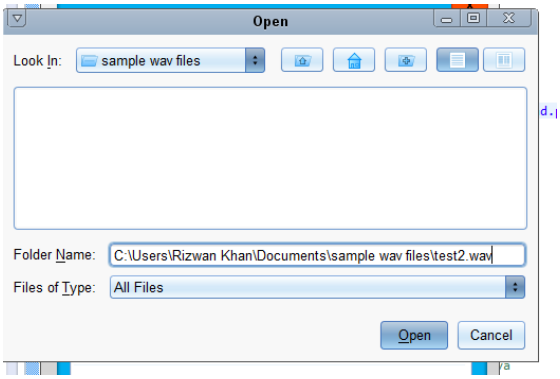

Figure 4.3 Output File Selection Dialog Box

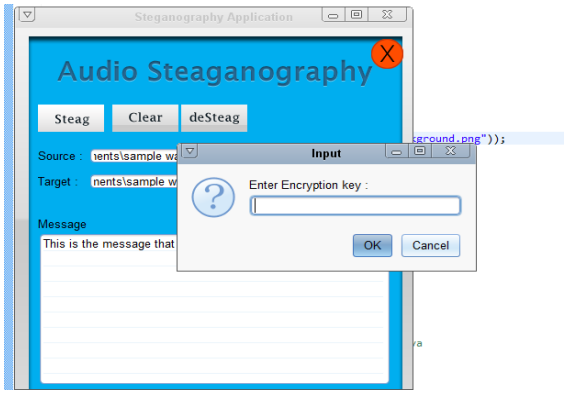

Figure 4.4Encryption Key Dialog Box:

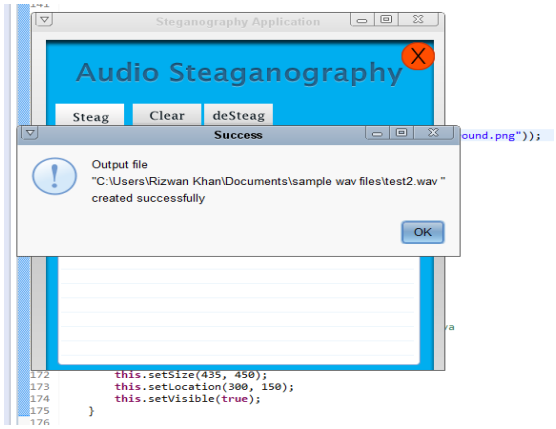

Figure 4.5 Result Dialog Box

The concept of steganography in audio file. Information hiding can be achieved either exploiting loopholes of Human Visual System (HVS) or Human Auditory System (HAS). Steganography of audio signals is more challenging than Steganography of images due to wider dynamic range of the HAS in comparison with human visual system (HVS).

To embed data secretly onto digital audio file there are few techniques introduced earlier. The lists of methods are:

- LSB Coding
- Phase Coding
- Parity Coding
- Spread Spectrum

In LSB coding technique least significant bit is modified to embed data. In phase encoding scheme the phase of carrier file is replaced with reference phase which represents hidden data. In parity coding signals are divided into regions, then parity bit of each region calculated and matched with secret message bit.

Depending on parity matching result encoding is done. In spread spectrum method secret information is spread over the audio signal's frequency spectrum as much as possible.We observe that the stego-file hasn't been audibly modified. Also the graphical representation shows that there is reasonable no change between input carriers file and output stego-file. The output stego-file is correct and audible. There is no Such discrepancy found compared to the input carrier file.

IV. CONCLUSION AND FUTURE SCOPE

All In this work we have been able to discuss major techniques used for data hiding in audio files. The proposed method has the potential to be a suitable cryptographic

method to secure the embedded data before insertion to a cover medium, and can be put to use as a powerful tool for the transmission of undetectable and secure communication.

FUTURE SCOPE

Our ability to discover hidden information during our investigations is vital, especially as new and innovative methods continue to evolve. Techniques have advanced and every passing day the technology is improving and creating new frontiers to be explored . With the advent of the smart phone and it's ever future is open to modify any of the above techniques individually or in a hybrid way to achieve at the desired results. These new techniques provide hybrid solutions that combine the best of cryptography with the best of steganography. The interest, innovation, and advancement of these threats continue to go unchecked.

REFERENCES

[1] KaliappanGopalan, "A Unified Audio and Image Steganography by Spectrum Modification" ,International Conference on Industrial Technology, 2009, Page(s): 1-5.

[2] Zamani M., Manaf A. A., Ahmad R.B., Zeki A. M., and Abdullah S., "A Genetic-Algorithm-Based Approach for Audio Steganography", World Academy of Science, Engineering and Technology 54, 2009.

[3] Walter Bender, Daniel Gruhl, Norishige Morimoto, Anthony Lu,"Techniques for Data Hiding", IBM Systems Journal, vol. 35, no. 3 and 4, pp. 313-336, 1996.

[4] Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding-ASurvey," Proc. IEEE, 1999, pp. 1062-1078.

[5] Cvejic N. and Seppanen T. "Increasing the capacity of LSB based audio steganography", Proc. 5th IEEE International Workshop on MultimediaSignal Processing, St. Thomas, V I, December 2002, pp.336- 338.

[6] Muhammad Asad, JunaidGilani, Adnan Khalid, "An Enhanced Least Significant Bit Modification Technique for Audio Steganography" ,978-1- 61284-941 6/111 $26.00 ©20 II IEEE.

[7] Pooja P. Balgurgi, PG Student, Prof SonalK. Jagtap, Asst. Professor,"Intelligent Processing : An Approach of Audio Steganograph" 2012 International Conference on Communication, Information& Computing Technology (ICCICT), Oct. 1920, Mumbai,India

[8] D. Gruhl, W. Bender, "Echo hiding", Proceeding of Inforomation Hiding Workshop ,pp. 295315, 1996.

[9] FatihaDjebbar_, BeghdadAyady, Habib Hamamzand Karim AbedMeraimx,"A view on latest audio steganography techniques",201IInternational Conference on Innovations in Information Technology

[10] P.K.Singh, R.K.Aggrawal," Enhancement of LSB based Steganography for Hiding Image in Audio", International Journal on Computer Science and Engineering, Vol. 02, No. 05, 20 10.

[11] K.Geetha And P.VanithaMuthu," Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy", International Journal on Computer Science and Engineering, Vol. 02, No. 04, 20 I O.

[12] Gang. L, A.N. Akansu, M. Ramkumar, "MP3 resistant oblivioussteganography", Proceedings of IEEE International Conference onAcoustics, Speech, and Signal Processing, Salt Lake City, UT, Vol.3,pp.1365-1368, 7-11 May 2001.

[13] X. Dong, M. Bocko, Z. Ignjatovic, "Data hiding via phase manipulationof audio signals", IEEE International Conference on Acoustics, Speech,and Signal Processing (ICASSP), vol. 5, pp. 377-380, 17-21 May 2004.

[14] R. Ansari, H. Malik, and A. Khokhar, "Data-hiding in audio usingfrequency-selective phase alteration", IEEE International Conference onAcoustics, Speech, and Signal Processing, (ICASSP'04), pp. 389-392,Montreal, Quebec, Canada, May 2004

[15] H. M. A. Malik, R. Ansari, and A. A. Khokhar, "Robust Data Hidingin Audio Using Allpass Filters", IEEE Transactions on Audio, Speechand Language Processing, vol. 15, no. 4, pp. 1296 - 1304, May 2007.