ISSN No. 0976-5697

Volume 4, No. 9, July-August 2013

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Development of Semantic Analyzer for Audio Steganography Using Spread Spectrum Technique

Anamika Sharma* Pushpinder Singh
M.tech Computer Science*, AP,M.tech Computer Science,
Department of CSE,Rbiebt,Kharar
Punjab Technical University, India.
anamikasharma379@gmail.com*, pushpinder01@yahoo.com

Abstract: In the current world of information technology, the sending and receiving of digital data through network is not secure up to the extent. There is a need to maintain the robustness and imperceptibility property of the data. So a technique is used, that fulfill these requirements is audio steganography that take the advantages of human auditory system to hide the digital data. In this research work, I have proposed two step audio steganography technique. In the first step spread spectrum technique is used that spread secret information across the audio signal's frequency spectrum as much as possible and in the second step semantic analyzer is used to check whether the data received on the recipient side is semantically correct and in order. The end result will show the amount of data embedding, quality and compression of the audio file at 32kbps, 64kbps and 128kbps and the data received is in order and semantically correct.

Keywords: Audio Steganography, Information Hiding, Security, Spread Spectrum, Semantic Analyzer

I. INTRODUCTION

With the advent of the Internet, computer users started to distribute, share, and transmit their private data online in a complete overt manner. As a result a technique steganography is used [1]. Steganography is an art and a science of communicating in a way, which hides the existence of the communication. It is also called as "covered writing", because it uses a "cover" of a message for sending any important secret message. Steganography serves as a means for private, secure and sometimes malicious communication. Steganography is a powerful tool which increases security in data transferring and archiving. In the steganography scenario, the secret data is first concealed within another object which is called "cover object", to form "stego object" and then this new object can be transmitted or saved [3]. Using different techniques, we can send secret data in the form of an image, a music file or even a video file by embedding it into the carrier, forming a stego signal. At the receiver's end, the secret data can be recovered from the stego signal using different algorithms. Basically, audio steganography is a type of digital steganography that hides digital data into digital audio files such WAV, MP3, and WMA files. Audio steganography takes advantage of the Human Auditory System (HAS) which cannot hear the slight variation of audio frequencies at the high frequency side of the audible spectrum; and thus, audio steganography can exploit and use this type of frequencies to hide secret data without damaging the quality of the audio file or changing its size [2].

A. Audio Steganography:

Audio steganography is the art and science of hiding digital data such as text messages, documents, and binary files into audio files such as WAV, MP3, and RM files. The output audio file is called the carrier file and is the only intermediate to be sent to the receiver [4]. Imperceptibility is the property of steganography and it refers to the fact that no one apart from the original sender and the intended receiver can suspect the presence of secret data into the carrier file being communicated. Steganography can be achieved by means of three types of techniques: injection, substitution, and generation.

Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. In this research work I have used spread spectrum technique.

B. Spread Spectrum Technique:

Spread Spectrum Steganography is a relatively new technology that can provide enhanced levels of security over and above ordinary steganographic techniques. Increasingly, audio media are being used for steganographic purposes. Spread Spectrum Technology forms the basis of Spread Spectrum Steganography. It is a form of Radio Frequency communication. Spread Spectrum techniques intentionally spread the transmitted data signal over a wide frequency range. The bandwidth used is in excess of the minimum bandwidth required for the data being sent. By Increasing the bandwidth improvements in the signal-to-noise performance are obtained [5]. The fundamental idea behind this process is that, in channels with narrowband noise, increasing the transmitted signal bandwidth results in an increased probability that the information received will be correct. The increase in performance for very wideband systems is called the process gain.

In order to be considered as a Spread Spectrum system, the system must meet the following criteria:

a. The transmitted signal bandwidth is much greater than the information bandwidth.

b. Some function other than the information being transmitted is employed to determine the resultant transmitted bandwidth.

C. Spread Spectrum Technique:

There are several techniques currently in use for generating Spread Spectrums. These include:

a) Direct Sequence Spread Spectrum (DSSS)
b) Frequency Hopping Spread Spectrum (FHSS)
c) Time Hopping Spread Spectrum

a. Direct Sequence Spread Spectrum (DSSS):

The basic principle behind the Direct Sequence Spread Spectrum (DSSS) technique is the modulation of the RF carrier with a digital code sequence. A two-stage process is used to produce the DSSS.

During the first stage, data is spread across the spectrum. This is achieved by dividing the data stream into a symbol stream (small pieces of one bit or more) and then allocating each part of the divided data to a frequency channel across the spectrum.

During the second stage, the modulation phase, the DSSS transmitter utilizes a phase varying modulation technique (QPKS – Quadrature Phase Shift Key or BPSK – Binary Phase Shift Key) to modulate each piece of data with a higher data rate bit sequence (chipping code), a code called pseudo-random noise (PN).

DSSS suffers from what is known as a "Near-Far" effect. This effect occurs when an interfering transmitter is much closer to the receiver than the intended transmitter.

b. Frequency Hopping Spread Spectrum (FHSS):

FHSS has an advantage over DSSS in that it is not as affected by the "Near-Far" effect. The basic principle behind the Frequency Hopping Spread Spectrum (FHSS) technique is that the carrier frequency is periodically modified (hopped) across a specific range of frequencies. The frequencies, across which the carrier jumps is the spreading code. Two types of Frequency Hopping signals may be used, slow hopping and fast hopping. With slow hopping, the hopping rate is smaller than the message bit rate, meaning that in one hop, one or more data bits are transmitted. While in fast hopping, one data bit is divided over more than one hop (the hopping rate is greater than the message bit rate).

c. Time Hopping Spread Spectrum:

The third Spread Spectrum technique is Time Hopping. Time Hopping and FHSS are somewhat similar, but in Time Hopping, the transmitted frequency is changed at each code chip time. Time Hopping can be implemented in two ways. In the first technique, each binary is transmitted as a short pulse, known as a chirp. In the second technique for implementing Time Hopping, each chirp has a different duration.

D. Use of Spread Spectrum Technique with Audio Files:

During this research I have analyzed Spread Spectrum that data transmitted in this manner is difficult to detect, can be immune from eavesdropping and jamming, and is very difficult to decode by anyone other than the intended recipient. The techniques described can be used to embed data in audio files relatively easily and these audio files can subsequently be broadcast or passed on using compact discs or other recording media. It would be possible to add another layer of security to the data embedded in the audio file by encrypting it prior to applying the spread spectrum.

E. Semantic Analyzer:

Computational power is increasingly able to analyze more and more complex linguistic structures. Semantic analysis is the process of relating syntactic structures, from the levels of phrases, clauses, sentences and paragraphs to the level of the writing as a whole, to their language-independent meanings. More sophisticated approaches use context-free grammars to generate syntactically correct cover text which mimics the syntax of natural text. None of these uses meaning as a basis for generation, and little attention is paid to the semantic cohesiveness of a whole text as a data point for statistical attack [6].

F. Objective of the Research:

a. To maintain the robustness during the substitution of bits.
b. To maintain imperceptibility of secret data in carrier file during the communication.
c. The clarity of digital audio signal should not be harmed.
d. To analyze the features of audio file that can be used to implement the high rate data hiding.
e. The data received on the receiver side should be grammatically and semantically correct.

II. LITERATURE REVIEW

Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly [4]: in this paper, the growth of high speed computer networks and that of the Internet, in particular, has increased the ease of Information Communication. Ironically, the cause for the development is also of the apprehension - use of digital formatted data. In comparison with Analog media, Digital media offers several distinct advantages such as high quality, easy editing, high fidelity copying, compression etc. But this type advancement in the field of data communication in other sense has hiked the fear of getting the data snooped at the time of sending it from the sender to the receiver. So, Information Security is becoming an inseparable part of Data Communication. In order to address this Information Security, Steganography plays an important role. Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message.

Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar [7]: Audio steganography is concerned with hiding information in a cover (host) audio signal in an imperceptible way. Hidden information from the stego, or data-embedded audio signal, is retrieved using a key similar to the one that was employed during the hiding phase. Least Significant Bit (LSB) modification technique is the most simple and efficient technique used for audio steganography.. The technique uses the fact that most of the information in a sample in any audio file is contained in the MSBs rather than LSBs. If one has to hide any speech signal inside a music file which is also called as "carrier", it can be done by replacing consecutive LSBs in each sample of the carrier with the message bits. Such a bit replacement is very simple & safe.

R Sridevi, Dr. A Damodaram, Dr. Svl.Narasimham [9]: In the current internet community, secure data transfer is limited due to its attack made on data communication. So more robust methods are chosen so that they ensure secured

data transfer. One of the solutions which came to the rescue is the audio Steganography. But existing audio steganographic systems have poor interface, very low level implementation, difficult to understand and valid only for certain audio formats with restricted message size. Enhanced Audio Steganography (EAS) is one proposed system which is based on audio Steganography and cryptography, ensures secure data transfer between the source and destination. EAS uses most powerful encryption algorithm in the first level of security, which is very complex to break. In the second level it uses a more powerful modified LSB (Least Significant Bit) Algorithm to encode the message into audio. It performs bit level manipulation to encode the message.

B. Santhi, G. Radhika and S. Ruthra Reka [11]: The most important application of internet is data transmission. Unfortunately this is less secured because of advanced hacking technologies. So, for secured data transmission we make use of steganography. This is the art of hiding information where the existence of data is unknown. Any medium like music, video, text, speech, etc can be used. In this study, the selected medium is audio. This study discusses about the existing audio steganographic techniques along with their advantages and limitations. Also an algorithm implementing parity and LSB methods is proposed. This mitigates the limitations of the existing methods discussed, thus increasing security and reducing computational load and code complexity.

Zameer Fatima and Tarun Khanna [12] In this a novel method for digital audio steganography where data is encrypted using DES (Data Encryption Standard) algorithm and embedded into the host audio signal using LSB algorithm. To avoid data being easily extracted we use 16 sub keys generated from a modified random key to encrypt data. Hence decoding 16 sub keys in a row become quite difficult and provide more robust way of data hiding. Another novel feature of this project includes compressing the data, to hide, before embedding into the audio carrier. The problem with conventional LSB algorithm is that since it embeds each bit of covert data into LSB of the audio file very less data can be hidden, so to increase the amount of data hiding we compress the data first. Experimental results show that proposed method has large payload, high audio quality and full recovery.

III. CONCLUSION

Steganography is a powerful tool for data hiding in audio medium when used in conjunction with spread spectrum technique. In this proposed technique it will become difficult for the eavesdropper to trace the data. Along with semantic analyzer is used that will make data semantically correct at the receiver side. This is a robust method for imperceptible data hiding.

IV. ACKNOWLEDGEMENT

I would like to thank my guide Mr. Pushpinder Singh, Assistant Professor in Department of Computer Science and Engineering at R.B.I.E.B.T. (Kharar), Punjab, India for motivating me to work on Audio Steganography and Semantic Analyzer. I would also like to thank my mother, my father and my brother for their continuous support, cooperation, and guidance throughout my M.Tech. work. Moreover I would also like to thank my Professors who were always there at the need of the hour and provided with all the help and facilities, which I required, for my thesis work.

V. REFERENCES

[1]. Peter Wayner, “Disappearing cryptography: information hiding: steganography & watermarking”, 3rd Edition, Morgan Kaufmann Publishers, 2009.

[2]. Kandel ER, Schwartz JH, Jessell TM, “Principles of Neural Science”, 4th edition, McGraw-Hill, 2000.

[3]. http://en.wikipedia.org/wiki/Steganography.

[4]. Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, “A Tutorial Review on Steganography”

[5]. Nick Sterling, Sarah Summers and Sarah Wahl, “Spread Spectrum Steganography”

[6]. Krista Bennett, Department of Linguistics “Linguistic Steganography:”

[7]. Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar : “ Data Hiding Technique: Audio Steganographyusing Lsb Technique”, Vol. 2, Issue 3, May-Jun 2012.

[8]. Aho, A.V., Sethi, R. and Ullman, J.D. “Compilers: principles, techniques, and tools”, Addison-Wesley Longman Publishing, 1986.

[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”, © 2005 - 2009 JATIT.

[10]. K. Gopalan, “Audio steganography using bit modification”, Proceedings of International Conference on Multimedia, vol.1, pp.629-632, 2003.

[11]. B. Santhi, G. Radhika and S. Ruthra Reka: “Information Security using Audio Steganography -A Survey”, Research Journal of Applied Sciences, Engineering and Technology 4(14): July 15, 2012.

[12]. Zameer Fatima and Tarun Khanna: “Audio Steganography Using DES Algorithm”, Proceedings of the 5th National Conference; INDIACom-2011.

[13]. Mazdak Zamani, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Farhang Jaryani, Hamed Taherdoost, Akram M. Zeki: “A Secure Audio Steganography Approach”, Copyright © 2009 by the Institute of Electrical and Electronics Engineers.

[14]. Mazdak Zamani , Azizah A. Manaf , and Rabiah B. Ahmad: “Knots of Substitution Techniques of Audio Steganography”, 2009 International Conference on Computer Engineering and Applications IPCSIT vol.2 (2011) © (2011) IACSIT Press, Singapore

