World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 111-114, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.29.csea.2240

Modeling of Steganography with Audio Files Using Matlab

R. Udayakumar, K.P. Kaliyamurthie, Khanaa and A.V.Allin Geo

School of Computing Science, Bharath University, Chennai-73, India

Abstract: The main objective of our project is to enable secure sending and receiving of secret data without a third party reading it. In our project, we hide data contents of a file in to a wave audio file. The audio file does not have change in its quality before and after this technique in implemented. The stego-audio file is send to the destination without any detection from any of external sources. Even if it is detected, the secret data meant for the receiver cannot be read or understood as it is encrypted.

Key words: Audio Steganography · Encryption · Audio processing · Encoding · Decoding · Data security · Data privacy

INTRODUCTION

Steganography is a sub discipline of information hiding that focuses on concealing the existence of messages. Unlike earlier times where message sending required lot of time and there was no assurance for data security. Now, we have lot of message sending techniques by which we can send and receive messages in seconds but data privacy or security is still a question mark [1, 2]. There is an urgent need for secure transmission of data in all areas of information exchange. There are various techniques available for information hiding and secure data transmission. These techniques are devised based on various necessities of information hiding. Indeed, there are many applications and uses of steganography and most experts agree that it will remain an important issue in the coming years [3]. 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. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information [4].

This paper is organized as follows. Section 2 describes the goal of our project. Section 3 and 4 tells about the techniques involved in our work i.e., encoding and decoding parts. Applications of steganography are discussed in section 5. In sections 6 and 7, the experiments performed and the results obtained are discussed. Section 8 concludes the paper.

Description: Our project deals with audio steganography. In this project we have presented a ***novel*** and economic idea of sending and receiving encrypted text messages without any detection as we use audio file which is not prone to privacy attacks [5]. Audio is an integral part of entertainment media and a millions of audio files are shared, uploaded and downloaded daily. The use of audio files will burden up the job of third party people interested in reading confidential messages and is an efficient method of transmission when compared to any other forms of steganographic media. Thus we have presented a simple and secure method of data transfer which can be implemented in a wide area of applications [6].

Encoding: In the encoding part, the audio file selected by the user is first read and stored in a matrix. The chosen secret file is opened and length is calculated [7]. This is stored in a variable, also in a secure position of the resulting steg-audio file. The secret message is encrypted as a precaution so that the original message don't fall into wrong hands even it is intercepted, which is of least probability and is placed in a location which depends on the size of both the secret file and the audio file. The encoded audio file is then saved and is ready to be transported.

Corresponding Author: R. Udayakumar, School of Computing Science, Bharath University, Chennai-73, India.

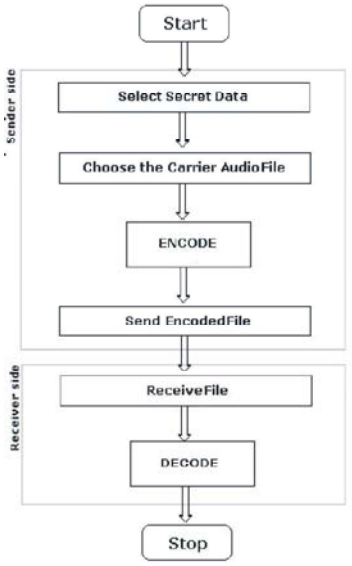

Fig. 1: Steganography Overview

Fig. 2: GUI

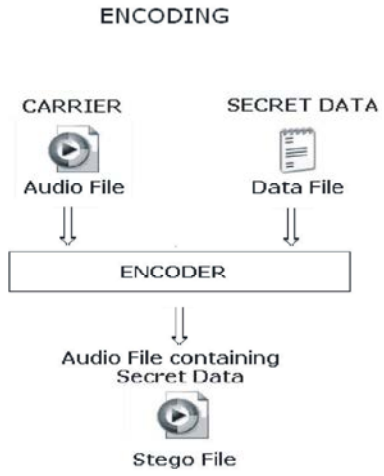

Fig. 3: Encoding Process

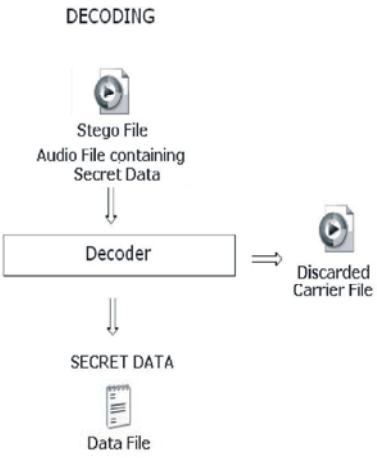

Fig. 4: Decoding Process

Decoding: The secret message from the steg file can be retrieved only using the decoding program. At the receiver end, the length of the secret message is read from the audio file. This will in turn serve the purpose of calculating the starting position of the secret message also. The secret message is then read and decrypted. This is then read to a matrix and saved to the output file and hence the original secret message is obtained [8].

Applications: In recent years there has been an exciting convergence of information protection technologies and the main emphasis is information hiding as oppose to encryption. The more information that is placed on the Internet or public media, the more the owner of the information need to protect themselves from theft and abuse. The advantage of steganography is the fact that, an encrypted data is easily detected by an attacker than information whose existence is unknown. The way forward is to embrace advance technology by blending cryptography with steganography. The principal focus is hiding information [9].

One of the most widely used applications is for so-called *digital watermarking*. The entertainment industry is particularly very nervous due to the ease at which exact copies of digital music and video can be made. A solution using steganography can be done by hiding notices or serial numbers or other copyright details inside the media which can later be made use of. It is used in military applications for transfer of sensitive data. Steganograhic implementations can allow communication within an underground community. These systems and techniques

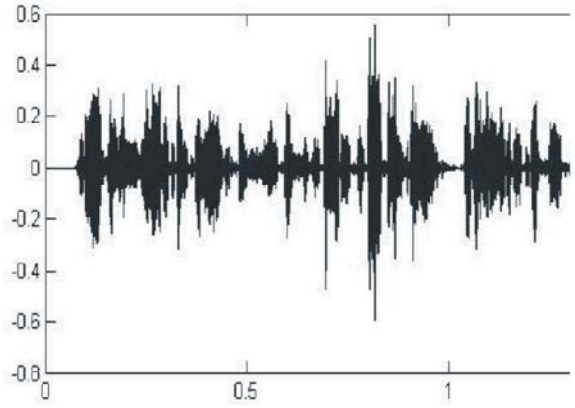

Fig. 5: Sample before encoding (Carrier Audio File)

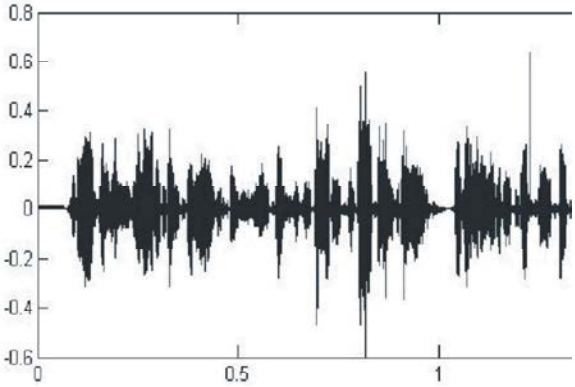

Fig. 6: Encoded sample (Steganographed Audio File)

Table 1: Experimental results on *wav* audio file

	Size of files tested	
Noise Duration	Data File	Carrier File
nil	Up to 10 KB	215 KB and above
1 sec	10 – 70 KB	

that can be used for hiding information which will be useful in computer forensics and digital traffic analysis. Hidden data within Web pages allows secret transfer of information [10].

Experiments and Results: We have currently tested the system on two audio formats: ***wav*** and ***au***. Carrier and data files of different magnitudes were used. Different test cases were formed based on the carrier-data file size ratio. Better accuracy levels were shown by those with bigger file size ratios. Data files with different sizes were tested on the same Carrier file to find out its maximum holding capacity. The quality of encoded carrier file was compared with the original audio file to find out the noise distortion levels caused due to the hidden data file.

Similar results were obtained for ***au*** format Carrier Files [11]. Samples of the carrier file before and after encoding in a ***wave*** format file are shown in Figure 5 and 6 respectively. By trial and error analysis method, we have found out that 100% accuracy is achieved when data file size is not more than 10KB. Minimum size of carrier wave used was 215 KB. Data Files in the range 10 to 70 KB adds a noise of 1 second. File sizes above 70 KB is not suitable for encoding as it introduce higher noise levels making the audio file unfit for listening [12].

Following are the sample wave forms obtained on a carrier file of 215KB encoded with 10KB of data.

CONCLUSION

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. But it is also quite real; this is not just something that's used in the lab or an arcane subject of study in academia. Steganography may, in fact, be all too real — there have been several reports that the terrorist organization behind the September 11 attacks in New York City, Washington, D.C. and outside of Pittsburgh used steganography as one of their means of communication.

This work can be extended to support various kinds of Carrier and Data file formats i.e., from the existing *wav* and *au* Carrier file formats to mp3, mpeg and other video formats. Data File support can be made for images, videos etc.

REFERENCES

1. Stefan Katzenbeisser Fabien and A.P. Petitcolas, 2000, Information Hiding Techniques for Steganography and Digital Watermarking
2. Neil F. Johnson, 2002. Steganography: Art & Science of Hidden Communication, Office of Naval Research (ONR) Naval-Industry Partnership Conference, Washington, DC, USA.
3. Stephen Mahoney, 2002. Audio Steganography and Steganalysis, Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection, Johns Hopkins University
4. Sushil Jajodia, 1998. Steganography: Seeing the Unseen. IEEE Information Technology Conference.
5. Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding, IBM Systems Journal, pp: 35.

6. Cox *et al*., 1995. Secure Spread spectrum Watermarking for Multimedia, NEC Research Institute Technical Report.
7. Dr.-Ing, XXXX. Claus Vielhauer supported by Christian Krätzer, Steganography and Digital Watermarking, Seminar: Otto-von-Guericke University Magdeburg, Germany.
8. Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. Detection of Material hardness using tactile sensor, Middle-East Journal of Scientific Research, ISSN:1990-9233 15(12): 1713-1718.
9. Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. Blue tooth broad casting server, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1707-1712.
10. Saravanan, T., V. Srinivasan and R. Udayakumar, 2013. Images segmentation via Gradient watershed hierarchies and Fast region merging, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1680-1683.
11. Saravanan, T., V. Srinivasan and R. Udayakumar, 2013. A Approach for Visualization of Atherosclerosis in Coronary Artery, Middle-East Journal of Scientific Research, ISSN:1990-9233, 18(12): 1713-1717.
12. Udayakumar, R., V. Khanna, T. Saravanan and G. Saritha, 2013, Cross Layer Optimization For Wireless Network (Wimax), Middle-East Journal of Scientific Research, ISSN:1990-9233, 16(12): 1786-1789.