Secure Audio Steganography for Hiding Secret information

K.Sakthisudhan
Assistant Professor
Bannari Amman Institute of Technology, Erode- India

P.Prabhu
P.G Scholar
Bannari Amman Institute of Technology, Erode- India

P.Thangaraj
Professor and Head of CSE
Bannari Amman Institute of Technology, Erode- India

ABSTRACT

In present day to day life, effective data hiding methods are needed due to attack made on data communication. This paper presents the technique for the above requirement. In this proposed method, secret message in form of audio file is embedded within another carrier audio file (.wav) .In the transmitter end the output will be similar to the carrier with secret message embedded inside. The hacker will be blinded by the transmitted signal. At the receiver end the original message can be retrieved without any loss. The entire proposed system is simulated and their corresponding waveforms prove the effectiveness of this method.

General Terms

Security, Secret data transmission, steganography.

Keywords

Dual audio steganography, LSB embedding, low complexity.

1. INTRODUCTION

Steganography, coming from the Greek words *stegos*, meaning roof or covered and *graphia* which means writing.It is the art and science of hiding the fact that communication is taking place. Using the steganography, we can embed a secret message inside a piece of unsuspicious information and send it without anyone knowing of the existence of the secret message. Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion while an invisible message will not do so.

Both sciences can be combined to produce better protection of the message. The principle defined once by Kerckhoffs for cryptography, also stands for steganography: the quality of a cryptographic system should only depend on a small part of information, namely the secret key. The same is valid for good steganographic systems: knowledge of the system that is used, should not give any information about the existence of hidden messages.

Finding a message should only be possible with knowledge of the key that is required to uncover it. So, this method will be more effective when compared to the cryptographic methods. In case of pervasive hacking by rapid selection one cannot be able to retrieve its exact message format as the inbuilt cryptography serves for this valuable purpose. Thus, a method called dual steganography serves well for the digital communication fields. The name ‘dual’ itself retrieves its cause such that two methods both combination of cryptography and steganography is used.

In this paper, a secret message of an audio file or a text file is first encrypted and then it is embedded into a carrier audio file. Our assumptions are the audio files are strictly in .wav format and the carrier audio file should be eight times greater than the secret audio message file.

The paper is organized as follows: In section 2 the existing audio steganography methods are discussed. Section 3 deals with the overall system model with the proposed audio steganography technique. In section 4 and 5, the experimental results and conclusion are discussed.

2. RELATED WORKS

There are many papers proposed in this audio steganography with most of the papers embed secret audio file in a carrier audio file. Some of them used cryptography for additional security. The author are mainly concerned with the security of the embedded message. To achieve high robustness and capacity of our steganalysis various methodologies have been implemented and verified their approach.

In [1] *kaliappan gopalan* proposed a steganalysis in audio file with an encryption key for the embedded secret audio file. In [2] *M Asad,J Gilani & A Khalid* proposed a audio steganography with an encrypted audio file using Advanced Encryption Standard(AES). In [3] *Mazdak Zaman, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Farhang Jaryani, Hamed Taherdoost, Akram M. Zeki* proposed a genetic algorithm for the embedding secret audio files for achieving higher robustness and capacity. In [4] *kaliappan gopalan* embed the information of secret message in spectral domain of a cover audio or image files. In [5] *K.B.Raja, C.R.Chowdary, Venugopal K R,& L.M.Patnaik* proposed a work on image steganography where a LSB embedding is used and then DCT is performed followed by a compression technique to provide high security in the hidden data. In [6] *Hossein Malekmohamadi and Shahrokh Ghaemmaghami* proposed an enhancement in image steganalysis of LSB matching by reducing the complexity using gober filter co-officients. In [7] *R Balagi & G Naveen* extended their work towards video steganography by embedding the secret information in some particular frames. In [8] *Andrew D. Ker* derived a mathematical analysis for the steganlysis in last two LSB bits.

3. SYSTEM MODEL

3.1 Overview

Steganography is an art of hiding a secret information inside a carrier file, such that the representation of carrier file wont be altered. Figure-1 shows the basic process involved in steganography, the secret message is embedded(mostly LSB method) in the carrier file and the stego file is created. This stego file resembles the carrier file and is transmitted in the transmitter side and is received at the receiver and the reverse process of extracting the secret information from the stego file is performed as in figure-2.

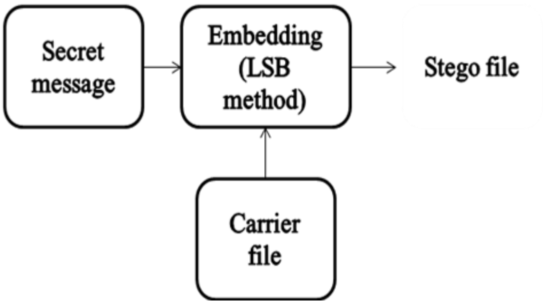

Figure 1 basic steganographic process at transmitter

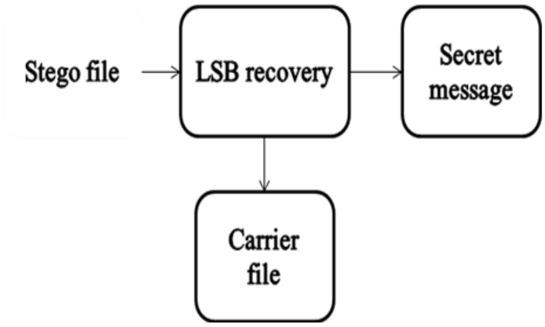

Figure 2 de-steganographic process at receiver

3.2 Existing Methods

In [1] the secret message and carrier files are taken as audio files. Before performing the embedding process the secret message is encrypted using a private key cryptography. Then the stego object is created. Thus using the key the secret information is retrieved at the receiver side. In [2] audio files are taken and the AES of 256 bits key length is used for the encryption of secret audio file to ensure the security.

3.3 Proposed Method

In the proposed method the carrier file is taken as audio format and the secret message may be a text or audio format files. Here a key is taken at the transmitter with that a pseudo sequence is generated and this sequence is performed a logical operation with the secret message. Then the embedding process is carried out with the carrier audio file and is transmitted at the transmitter side as in figure 3.

In the receiver side with the audio stego file the LSB are recovered first and with the known key generated at the transmitter the decryption process is carried out and the secret message is recovered from the stego file. The entire proposed de-steganographic process is shown in figure 4.

The algorithm for our proposed method is followed,

Step 1: Get the carrier file and message file such as the length of carrier file is a1, and message file is a2.

```
y=wavread(a1,'native');
s=dec2bin(y(i),8);
```

Step 2: The key is obtained from the user and thus we generate the PN sequence based on the key value. Let the key value be denoted as r and thus the output will be b.

```
n=input('enter the key for encryption:');
r=dec2bin(n,8);
```

Step 3: Now encrypt the message signal with the generated PN sequence so that it will be difficult for the hacker to trace the original bits even if they had tracked the transmitted signal

```
d=(s~=w);
```

Where “d” has the encrypted value.

Step 4: Embed the encrypted message with the carrier signal

```
s=dec2bin(z1(i),8);
s(7)=p1(i);
```

LSB bits in carrier have been replaced with message bits.

Step 5: Transmit the embedded carrier audio file at the transmitter. In the receiver side the reverse operation is carried out for recovering the secret message.

The main assumptions in the proposed method are,

- The secret and carrier audio files taken are strictly in .wav format.
- The carrier file should be eight times greater than the secret audio file.

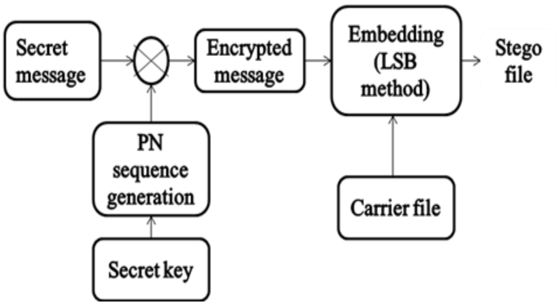

Figure 3 proposed steganographic approach at transmitter

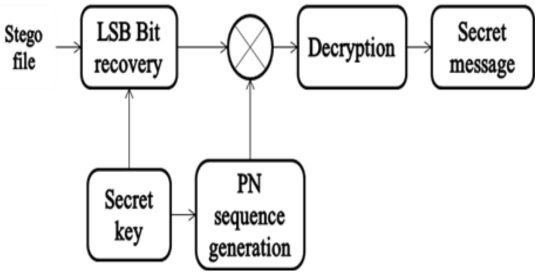

Figure 4 proposed de-steganographic approach at receiver

Thus providing a low complexity encryption and decryption process with security proves the efficiency of the proposed method.

3.4 Flowchart

The proposed flow chart is shown in figure 5. The steps are as follows,

1. Get the carrier audio signal and calculate the length it is noted as A1.
2. Get the secret audio or text file and calculate the length, it is noted as A2.
3. As per the assumption check whether the L1 is eight times greater than A2.
   3.1 If it is greater than proceed with the proposed algorithm.
   3.2 Else display the message as secret message is too large and initializes the process from starting.
4. Get the secret key and with that a pseudorandom sequence is generated and is performed logical operation with the secret message and is then embedded using LSB method in the carrier audio file.
5. The stego file is created and is transmitted from the transmitter side.

The reverse operation is performed at the receiver side for retrieving the secret message embedded in the transmitted stego audio file.

4. EXPERIMENTAL RESULTS

The carrier file should be strictly audio (.wav) file format and the secret message may be of audio (.wav) or text file. And here for our experimental scenario the carrier audio file is '*one.wav'* of 27.5 KB size and the secret audio file is '*hi.wav'* of 1.57 KB size. Thus the carrier file is eight times greater than the secret message file ensuring the assumptions made. The full details about the audio files taken are shown in the table 1.

The secret text file chosen is '*rajeswari V'*. As per the proposed method a text file can also be embedded in the carrier audio file. Thus the chosen secret messages of audio or text files are embedded in transmitter side and are recovered at the receiver side as shown in the following figures. The simulation is carried out in MATLAB R2010a software.

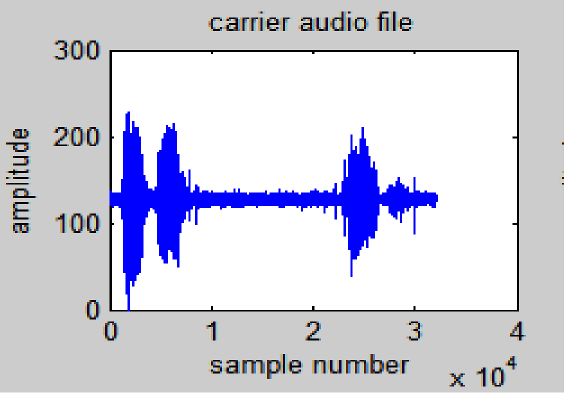

Figure 6 carrier audio file

Figure 6 shows the carrier audio file 'bond.wav' representation. Figure 7 & 8 shows the secret audio and text file to be embedded in the carrier audio file. Figure 9 shows the stego audio file after embedding the secret audio file. Figure 10 shows the comparison of the carrier audio file and stego file. We can infer that there is no major difference in the signal representation ensures the security. Figure 11 & 12 shows the recovered secret audio and text files at the receiver side.

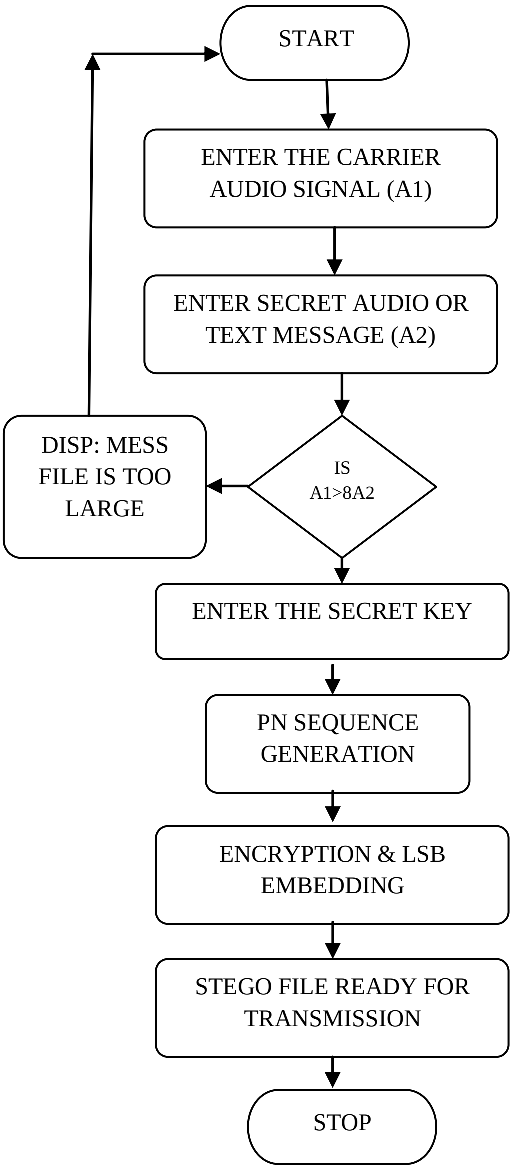
START
ENTER THE CARRIER AUDIO SIGNAL (A1)
ENTER SECRET AUDIO OR TEXT MESSAGE (A2)
IS A1>8A2
DISP: MESS FILE IS TOO LARGE
ENTER THE SECRET KEY
PN SEQUENCE GENERATION
ENCRYPTION & LSB EMBEDDING
STEGO FILE READY FOR TRANSMISSION
STOP

Figure 5 proposed flowchart

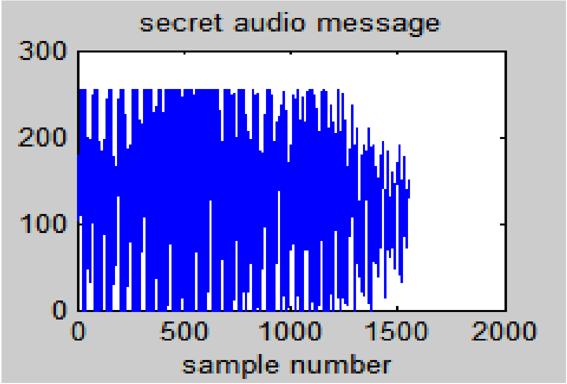

Figure 7 secret audio file

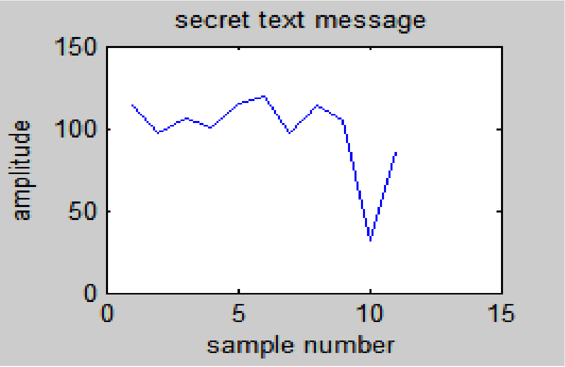

Figure 8 secret text message

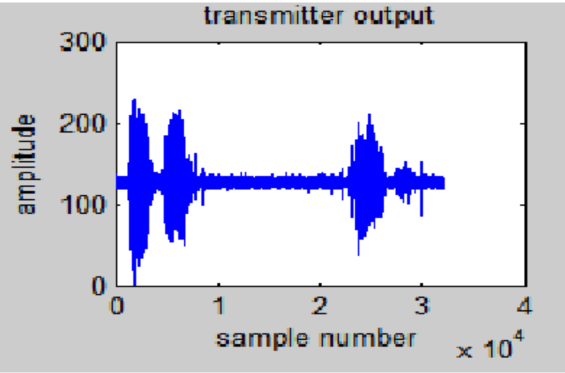

Figure 9 stego audio file to be transmitted

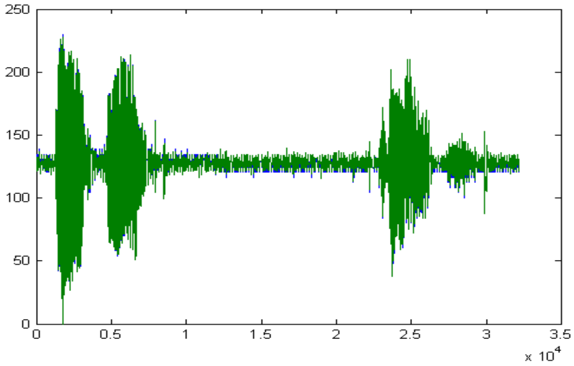

Figure 10 comparison of original carrier audio file and stego audio file(amplitude vs. sample no)

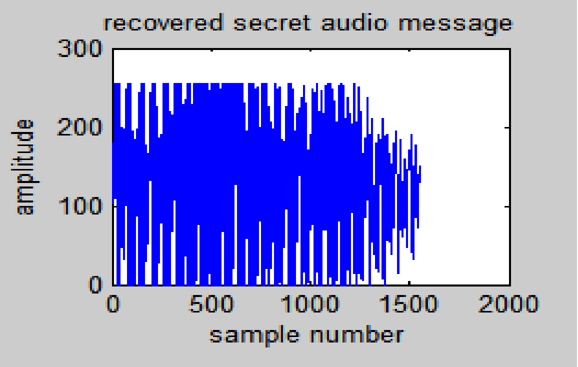

Figure 11 retrieved secret audio message at receiver

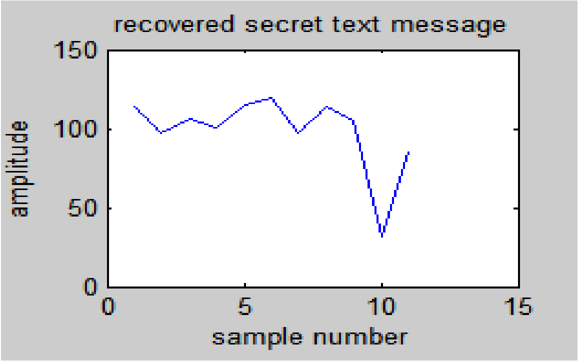

Figure 12 retrieved text message

PARAMETERS	CARRIER FILE	SECRET MESSAGE
NAME	One.wav	Hi.wav
SIZE	27.5 KB	1.57 KB
BIT RATE	88 kbps	64 kbps

Table 1 experimental audio file parameter values

5. CONCLUSION

The steganography is one of the safest forms of data transmissions in this digital world. In our proposed method, audio steganography is enhanced more by means of cryptographic key algorithms. The message signal is transmitted with utmost security and can be retrieved without any loss in transmission in this method. Apart from lossless transmission this method easily blinds the hackers securing from data piracy. The key can be both public and private depending upon the user and serves better in both aspects.

The output waveforms show that the recovered message resembles exactly as that of the transmitted message. Similarly, the carrier and transmitted signal resembles the same. These results shows that this method is lesser prone to error while transmission. Hence, this method is well suited for digital data transmission through internet and other communication systems.

6. ACKNOWLEDGMENT

I hereby thank my project guide (B.E) Mrs.S.Gayathiri priya and my friends (Naveen.A, Prabhu.C, Prabhakaran.R) for completing this project. And I place my sincere thanks and regards to my project guide (M.E) Mr.K.Sakthisudhan for his excellent support throughout my carrier. I also extend my thanks to all my staffs and my friends for their wonderful encouragement.

7. REFERENCES

[1] Gopalan., “Audio steganography using bit modification”, 2003 IEEE International conference on Acoustic, Speech and Signal Processing page(s): II – 421 -4 vol.2.

[2] Muhammad Asad, Junaid Gilani, Adnan Khalid “An Enhanced Least Significant Bit Modification Technique for Audio Steganography”, 2011 international conference

on Computer Networks and Information Technology (ICCNIT), pages 143-147

[3] Zamani, M., Manaf, A, Ahmad, R.B., Jaryani, F., Taherdoost H., Zeki, AM.,"A secure audio steganography approach", International Conference for Internet Technology and Secured Transactions 2009, Page(s):1 - 6.

[4] Kaliappan Gopalan, "A Unified Audio and Image Steganography by Spectrum Modification", International Conference on Industrial Technology, 2009, Page(s):1 – 5

[5] Raja K B, Chowdary C R, Venugopal K R, Patnaik L M "A Secure Image Steganography using LSB DCT and Compression Techniques on Raw Images" 2005 IEEE International conference on session B-image signal processing.

[6] Hossein Malekmohamadi and Shahrokh Ghaemmaghami Reduced Complexity Enhancement Of Steganalysis Of LSB-matching Image Steganography" 2009 IEEE/ACS International conference on computer system and applications.

[7] Balagi R, Naveen G"Secure Data Transmission Using Video Steganography", 2011 IEEE International conference on electro/information technology (EIT).

[8] Andrew D. Ker, "Steganalysis of Embedding in Two Least-Significant Bits" 2007 IEEE transactions on information forensics and security, vol. 2, no. 1, march 2007.

[9] W. Mazurczyk and Jozef Lubacz, "LACK– a VoIP Steganographic Method", Journal of Telecommunication System, Springer Netherlands, Dec., 2009.

[10] D. LIamas, C Allison and A Miller, "Covert Channels in Internet Protocols: A Survey", 2005 at http://grayworld.net/papers/0506-PGNET-Paper.pdf.

[11] D.V. Forte et al. "SecSyslog: An Approach to Secure Logging Based on Covert Channels," Proc. First Int'l Wksp. Systematic Approaches to Digital Forensic Engineering, Nov. 2005, pp. 248-263.

[12] Wilfrid J. Dixon, Frank J. Massey: Introduction to Statistical Analysis. McGrawHill Book Company, Inc., New York 1957.

[13] Neil F. Johnson, Sushil Jajodia: Steganalysis of Images Created Using Current Steganography Software, in David Aucsmith (Ed.): Information Hiding, LNCS 1525, Springer-Verlag Berlin Heidelberg 1998. pp. 32–47

[14] M. R. Nelson: LZW Data Compression. Dr. Dobb's Journal, October 1989.

[15] Birgit Pfitzmann, Information Hiding Terminology, in Ross Anderson (Ed.): Information Hiding. First International Workshop, LNCS 1174, Springer-Verlag Berlin Heidelberg 1996. pp. 347–350

[16] Robert Tinsley, Steganography and JPEG Compression, Final Year Project Report, University of Warwick, 1996

[17] Terry Welch: A Technique for High-Performance Data Compression. IEEE Computer, June 1984.

[18] http://lifehacker.com/5807289/how-to-hide-secret-messages-and-codes-in-audio-files

[19] Hide and Seek, http://www.rugeley.demon.co.uk/security/hdsk50.zip

[20] S-Tools,ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/s-tools4.zip