Encrypted Information Hiding using Audio Steganography and Audio Cryptography

Nishith Sinha
B.Tech - Student
CSE Department
MIT, Manipal

Anirban Bhowmick
B.Tech - Student
CSE Department
MIT, Manipal

B. Kishore
Asst. Professor – Sr. Scale
CSE Department
MIT, Manipal

ABSTRACT

With the growing importance of the internet, secure transmission of information is crucial. Steganography and cryptography helps in providing this much needed data confidentiality. Steganography hides secret information into a cover medium and cryptography converts data into an unrecognizable form.

In this paper, the authors proposed a novel approach for concealing data. The proposed algorithm is an amalgamation of text encryption, audio steganography and audio encryption. In the first step, the original text message is encrypted using modified Vigenère cipher algorithm. This cipher text gets embedded into the cover audio using LSB encoding, in the second step. Further, the audio file is then subjected to transposition making use of Blum Blum Shub pseudo random number generator. This scrambled stegno audio is transmitted to the receiver which carries the encrypted secret data.

Keywords

Cryptography, Audio Steganography, Audio Encryption, Modified Vigenère Cipher, Blum Blum Shub, Pseudo Random Number, LSB Coding.

1. INTRODUCTION

When two entities are communicating, security is one of the major concerns. Data needs to be concealed when it is transmitted over the network to protect it from intruders. When it comes to ensuring data confidentiality [1], one can use either cryptography or steganography. In the approach presented in this paper, a combination of the two is proposed. This ascertains greater security of the secret information.

Audio steganography is a technique in which the secret data is embedded into the cover audio, with the secret message invisible to unauthorized users. There are three requirements for any steganographic system - perceptual transparency, hiding capacity and robustness [2]. After embedding the message, the stegno audio is obtained. At the receiver's end the hidden data can be extracted from the stegno signal using the reverse algorithm.

Cryptography is a technique in which the information to be transmitted over the network is transformed into an unreadable form to provide secure communication in the presence of third parties. Cryptography aims at data confidentiality, data integrity and authentication [3] [4]. Encryption and decryption are the two aspects of cryptography.

Further, there are two types of cryptographic schemes [4]:

- Secret key cryptography or symmetric key cryptography
- Public key cryptography or asymmetric key Cryptography

Cryptography and steganography achieve the same goal of data confidentiality via different means. The main difference between steganography and cryptography is that, cryptography concentrates on keeping the contents of a message secret while steganography concentrates on keeping the existence of a message secret [5].

Further, the proposed algorithm makes use of modified Vigenère Cipher [6] and a Blum Blum Shub pseudo random number generator (PRNG) [7]. Vigenère cipher uses polyalphabetic substitution. It is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword.

A pseudo random number generator is a deterministic algorithm which generates a sequence of random numbers with the intent that each number generated is unpredictable. In this paper, the authors use Blum Blum Shub [8] PRNG.

Cryptanalysis [9] [10] and steganalysis [11] is gaining prominence in the field of cryptographic research. Cryptanalysis is the retrieval of original data without the knowledge of the key. Steganalysis is analogous to cryptanalysis. Steganalysis is accessing the hidden information by unauthorized entities.

Continuous research works on new cryptographic and steganographic algorithms are being put forward. This paper makes an attempt to combine cryptography and steganography to enhance the security of vital data.

The rest of the paper is divided into following sections. Section 2 highlights some of the existing work done in this area. Section 3 provides a detailed description of the algorithm proposed. Section 4 contains the waveforms of the audio files at different stages of the experiment. Section 5 concludes the paper.

2. RELATED WORK

All authors in [12] have proposed a two level data security comprising of text cryptography and image steganography. The secret text is encrypted using Blowfish algorithm followed by embedding it into an image using LSB encoding. The carrier image can be then transmitted over the network.

In [13], authors have suggested an algorithm in which the data is first subjected to encryption using Data Encryption Standard (DES). The encrypted message is then passed to embedding phase. In embedding phase the encrypted message will embedded into the cover medium which is either image or audio or video resulting in a stego medium. The embedded stego medium contains the encrypted text message which is extracted at the receiver side. The extracted text is decrypted using decryption module.

Authors in [14] have proposed a combination of cryptography and steganography to provide data confidentiality. AES-128 is used to encrypt the message before it is inserted into image.

After the message is encrypted then it is embedded in to image using pseudo random numbers in LSB of image.

Authors in [15] have put forward an algorithm in which the secret data is first encrypted using AES algorithm. This encrypted data is then embedded into an audio file. The authors then encrypt the audio file using Spread Spectrum technique before transmitting it over the network.

In [16], authors have proposed two methods of hiding data into an audio signal using LSB coding. One is considering parity of the digitized samples of cover audio in which the parity of the samples are checked before data embedding. The other approach is considering the XOR operation. This method performs XOR operation on the LSBs and then depending on the result of XOR operation and the message bit to be embedded, the LSB of the sample is modified or kept unchanged.

3. PROPOSED TECHNIQUE

3.1 First Phase

The first phase is related to encrypting the secret data by the modified Vigenère cipher algorithm. The primary weakness of classical Vigenère cipher is the repeating nature of its key and this loophole was exploited by Kasiski and Friedman. Cryptanalyzing Vigenère cipher [17] is possible. Thus, a modified Vigenère cipher algorithm is proposed in [6] that provides resistance to Kasiski attack [6].

In this method, the original plain text is subjected to classical Vigenère cipher followed by double columnar transposition.

Example
Original Text – CRYPTOGRAPHYANDNETWORKS

Keyword - SECURITYSECURITYSECURIT

Key – 253146

Encrypting using Vigenère cipher, the intermediary cipher text obtained is as follows

C_1 = UVAJKWZPSTJSRVWLWXYIISL

The intermediary cipher text (C_1) is then subjected to double columnar transposition

2	5	3	1	4	6
U	V	A	J	K	W
Z	P	S	T	J	S
R	V	W	L	W	X
Y	I	I	S	L	

The second intermediary cipher text (C_2) is obtained is reading the text column by column, the order decided by the column numbers.

C_2 = JTLSUZRYASWIKJWLVPVIWSX

The final encrypted cipher text is obtained by subjecting C_2 to columnar transposition

2	5	3	1	4	6
J	T	L	S	U	Z
R	Y	A	S	W	I
K	J	W	L	V	P
V	I	W	S	X	

C = SSLSJRKVLAWWUWVXTYJIZIP.

3.2 Second Phase

In the proposed technique, the second phase of data concealing uses Least Significant Bit (LSB) encoding technique in which the encrypted message (C) is embedded into the cover audio making use of the LSB of the audio frames in the audio file.

In this phase, each character of the encrypted message (C) is extracted and the ASCII value of the character is used to generate the corresponding bit pattern. Each bit of this pattern replaces the last bit of an audio frame. Each character is represented by an 8 bit binary number. Thereby, for each character, 8 consecutive audio frames will be needed. Further, the next character will be embedded in the next 8 audio frames and so on.

Example
Character to be embedded – ‘A’

ASCII value of ‘A’: 65

8 bit binary representation of the ASCII value: 01000001

8 consecutive audio frames in binary format (consider 8 bit)

10010010 01010101 10010101 11101010 10000100

11110011 10100000 11010101

Each Bit to be Embedded	**8 consecutive Audio Frames**	
	Before Embedding	**After Embedding**
0	10010010	1001001**0**
1	01010101	0101010**1**
0	10010101	1001010**0**
0	11101010	1110101**0**
0	10000100	1000010**0**
0	11110011	1111001**0**
0	10100001	1010000**0**
1	11010101	1101010**1**

The LSB encoding algorithm is presented below

Algorithm: Encode text message into audio file

Input: Text message, Audio file

Output: Stegno audio file

Initialize: i ← 0, k ← 0,

A ← audio frames of the audio file

```
while i < Length (text message) do
    c ← Get the $i^{th}$ character of text message
    asc ← Get ASCII value of c
    bin ← Get binary value of asc
    j ← 0
    while j < Length (bin) do
    AFbin ← Get the binary pattern of $k^{th}$ audio frame
    in A
```

```
        S [j] ← Store the last bit of AFbin
        Replace the last bit of the audio frame with bin [j]
        j ← j+1
        k ← k+1
    end
    i ← i+1
end
```

Security of the data transmitted is further enhanced by encrypting the audio file thereby making steganalysis difficult. The encryption technique makes use of pseudo random numbers generated through Blum Blum Shub random number generator algorithm.

Blum Blum Shub (BBS)
Blum Blum Shub [8] is a pseudorandom number generator proposed in 1986 by Lenore Blum, Manuel Blum and Michael Shub. Blum Blum Shub takes the form

$$\boxed{X_{n+1} = X_n^2 \bmod M}$$

where M = p x q is the product of two large primes p and q. At each step of the algorithm, some output is derived from x_{n+1}. The initial seed x_0 should be an integer that is co-prime to M (i.e. p and q are not factors of x_0) and not 1 or 0.

Algorithm: Blum Blum Shub Algorithm

```
Input: p, q, $x_0$
Output: Sequence of pseudo random numbers
Initialize: M ← p x q,
            Num ← (seed x seed) mod M

while Num != 0 and Num is non repeating do
    Used as the next number of the sequence
    Num ← (seed x seed) mod M
end
```

3.3 Third Phase

Please In the third phase, the audio file is subjected to encryption. Encryption is carried out by transposition in which the orders of the audio frames are changed generating a scrambled audio file. This scrambling is carried out by the random numbers generated by Blum Blum Shub pseudo random number generation algorithm.

The random numbers are generated dynamically using BBS algorithm. The first step of encryption is to restrict the magnitude of each random number to the number of audio frames present in the audio by making use of modulo operation. The audio frames are then traversed starting from the very 1st audio frame. Each audio frame is swapped with another; the latter’s frame number being picked by the random number generated at that instant. The procedure is repeated till all the audio frames are exhausted. Subsequently, the encrypted audio file is obtained.

Algorithm: Transposition using random numbers

```
Input: Original audio file, Sequence of random numbers
Output: Encrypted audio file
Initialize: k ← 0
1: while k < number of audio frames do
2:     Extract the kth audio frame
3:     Extract another audio frame, this audio frame
       number decided by the random number generated
4:     Swap the kth frame with the frame having the frame
       number equal to the value obtained in STEP 3
5:     k ← k+1
6: end
```

Once the third phase of the algorithm is completed, the resulting audio can be transmitted over the network. The general outline of the proposed algorithm is diagrammatically represented in Figure 1.

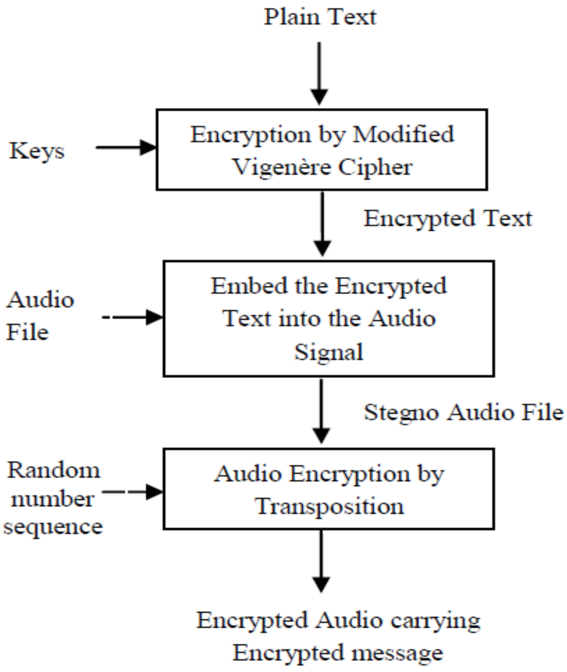

Plain Text
Keys
Encryption by Modified Vigenère Cipher
Encrypted Text
Audio File
Embed the Encrypted Text into the Audio Signal
Stegno Audio File
Random number sequence
Audio Encryption by Transposition
Encrypted Audio carrying Encrypted message

Fig 1: General outline of the proposed algorithm

The encrypted message can be then extracted at the receiver's end after the encrypted audio is subjected to decryption, which is just the reverse of the algorithm previously used for encrypting the audio. The encrypted text can be then decrypted by the receiver to obtain the secret message.

The encryption techniques put forward is symmetric encryption which makes use of private keys. The private keys are known only to the sender and the receiver.

4. RESULTS

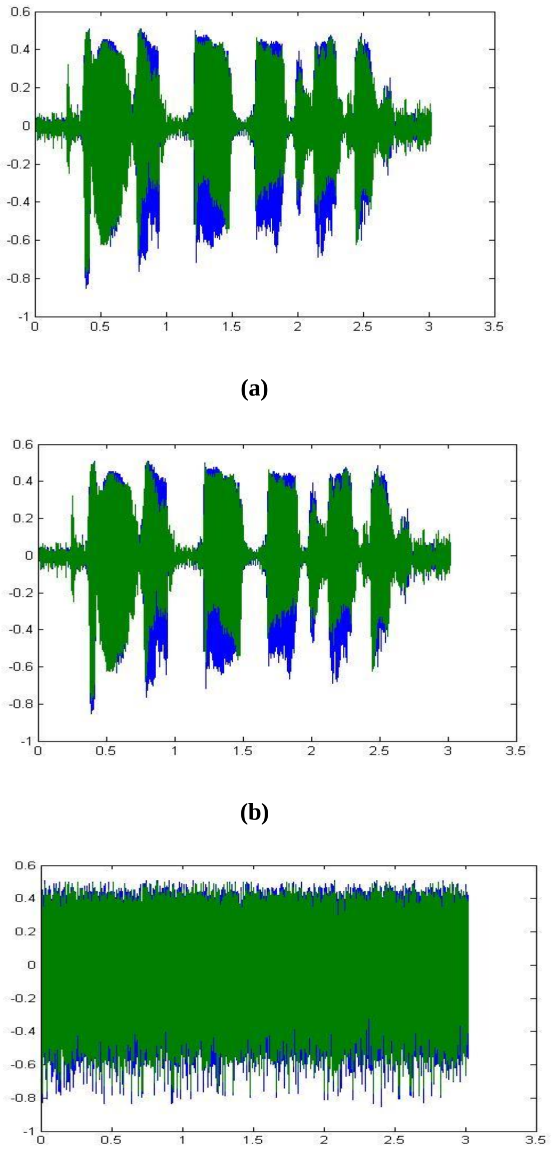
This section highlights the waveforms of the original audio file, the stegno audio file and the encrypted audio file. The authors have subjected the proposed algorithm on two audio files to test the suitability and efficiency of the algorithm. The results obtained at each step have been presented in this section.

The two cases discussed below represent the waveforms of the two audio files and the waveforms generated at each intermediary step of the algorithm. The y-axis of the waveforms represents the sampled audio data and the x-axis represents the time axis.

CASE 1

Specifications of the Audio File

Type	Wave Sound (.wav)
Size	130 KB
Length	3 seconds
Bit Rate	352 Kbps



(a)

(b)

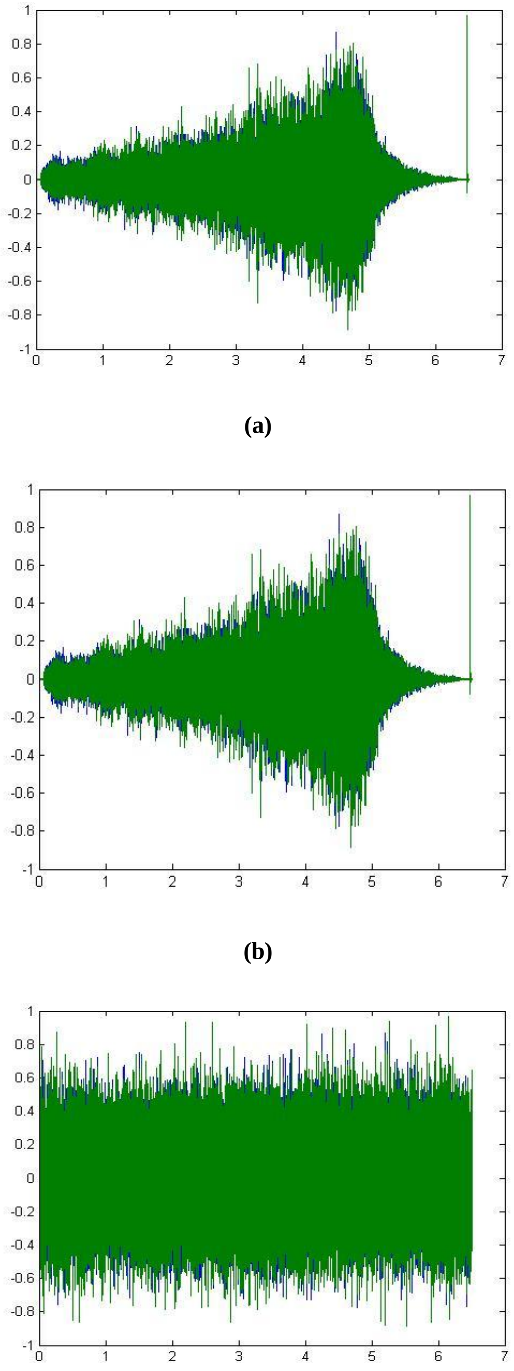
(c)

Fig 2: (a) Original audio file (b) Stegno audio file containing the encrypted text (c) Encrypted stegno audio file

CASE 2

Specifications of the Audio File

Type	**Wave Sound (.wav)**
Size	**1.09 MB**
Length	**6 seconds**
Bit Rate	**1411 Kbps**



(a)

(b)

(c)

Fig 3: (a) Original audio file (b) Stegno audio file containing the encrypted text (c) Encrypted stegno audio file

5. CONCLUSION AND FUTURE WORK

As discussed earlier, security of information over the internet is becoming a major concern. In this paper, the authors made an effort to safeguard this information from intruders using an amalgamated approach of cryptography and steganography. The secret data is first encrypted which is embedded into an audio file and then this audio file is encrypted before being transmitted over the network. This combination of cryptography and steganography ensures that even if the audio file is intercepted by an unauthorized person, the person doesn't discover the secret information.

The difference in the frequency time analysis waveforms of the original audio, the stego signal and encrypted audio signal has also been represented in Section 4. Figure 2c and 3c clearly suggest that the encrypted audio is completely different from the original audio. The lack of difference between figures 2a and 2b or 3a and 3b proves that there is almost no distortion created in the audio file by the embedded text.

As a part of future work, the authors recommend more secure encryption algorithms to be utilized for text encryption. Further, different steganographic techniques can also be used. In this paper, the audio is encrypted only using transposition [18]. To enhance the resistance of the audio file, the audio file can be further subjected to substitution [18] encryption.

6. REFERENCES

[1] Behrouz A. Forouzan, “Cryptography and Network Security” special Indian Edition 2007, Tata McGraw-Hill Publishing Company Limited, New Delhi.

[2] S. Das, B. Bandyopadhyay and S. Sanyal, “Steganography and Steganalysis: different approaches”, Cornell University Library, 2011.

[3] Nigam Sangwan, “Text Encryption with Huffman Compression”, International Journal of Computer Applications (0975 – 8887) Volume 54– No.6, September 2012

[4] Ayushi, “A Symmetric Key Cryptographic Algorithm” International Journal of Computer Applications (09758887) Volume 1 – No. 15

[5] Wang H and Wang S, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM, vol. 47, no. 10, 2004

[6] Forman, Nishith Sinha, Kishore Bhamidipati, “Improving Security of Vigenère Cipher by Double Columnar Transposition”, International Journal of Computer Applications (0975 – 8887) Volume 100 – No.14, August 2014.

[7] “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”, National Institute of Standards and Technology, Special Publication 800-22 Revision 1a.

[8] Divyanjali, Ankur, Vikas Pareek, “An Overview of Cryptographically Secure Pseudorandom Number generators and BBS”, International Journal of Computer Applications (0975 – 8887).

[9] M U Bokhari, Shadab Alam, Faheem Syeed Masoodi, “Cryptanalysis techniques for Stream Cipher: A Survey”, International Journal of Computer Applications (0975 – 8887) Volume 104 – No 15, October 2014

[10] Andrew S Tanenbaum, “Computer Networks”, 4th Edition

[11] Yambem Jina Chanu, Kh. Manglem Singh, Themrichon Tuithung, “Image Steganography and Steganalysis: A Survey”, International Journal of Computer Applications (0975 – 8887) Volume 52– No.2, August 2012

[12] Komal Patel, Sumit Utareja, Hitesh Gupta, “Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm”, International Journal of Computer Applications (0975 – 8887) Volume 63– No.13, February 2013

[13] V. Lokeswara Reddy, A Subramanyam , P Chenna Reddy, “A Novel Approach for Hiding Encrypted Data in Image, Audio and Video using Steganography”, International Journal of Computer Applications (0975 – 8887) Volume 69– No.15, May 2013

[14] Unik Lokhande, A. K. Gulve, “Steganography using Cryptography and Pseudo Random Numbers”, International Journal of Computer Applications (0975 – 8887) Volume 96– No.19, June 2014

[15] Md. Shafakhatullah Khan, V.Vijaya Bhasker, V. Shiva Nagaraju, “An Optimized Method for Concealing Data using Audio Steganography”, International Journal of Computer Applications (0975 – 8887) Volume 33– No.4, November 2011

[16] H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, “Information Hiding in Audio Signals”, International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010

[17] D R Stinson, “Cryptography Theory and Practice”, 3rd Edition

[18] William Stallings,” Cryptography and Network Security”, 5th Edition