Securing Hill encrypted information With Audio steganography: a New Substitution Method

Enas Wahab Abood 1 Wafaa A. Khudier 1 Rasha Hadi Jabber 1 Dina Adnan Abbas 2
1 University of Basrah - college of Science - Math. Dept
2 Basra Education Directorate
E-mail: enaswahab223@gmail.com

Abstract. Securing data is an essential matter in communication systems, data must be protected from interceptors and eavesdroppers. In this paper, a hybrid system was produced to secure a plain text message encrypted with the Hill encryption method and embedded within an audio file in a random distribution using audio symbol sign to represent message bits. The audio file is restricted to be *.wav stereo file, Two secret keys are needed for this system encryption key and the seed of generating hiding positions. PSNR, MSE, SSIM are calculated between cover before and after embedding and the results reflected the imperceptibility requirement of the system. Also the elapsed time for securing messages was quite low for different sizes of text and the encryption process was less time than hiding.

1. Introduction

Securing data and information of all media is an essential issue that taking enormous attention and studies by researchers and especially for data transmitted over the Internet. These data pass through the net therefor it exposes the risk of third parties to interception [1]. The process of avoiding interception is difficult but, the data still need to be protected either by making it unreadable through encryption or be invisible by hiding it in Innocent other data file (steganography) [2], or even better if both methods have combined in one system [3]. Kerckhoffs defined the principle of cryptography: the cryptographic system quality should only depend on a small but significant part of the information, called a secret key. The same principle is valid for strong steganographic systems: the system knowledge that is used, must not provide any information around the existence of hidden messages [4][5][6]. Audio steganography is the science of hiding a secret message within an audio file called cover file. The secret messages can be any form of data like image, video, text or audio [7][8]. The most known and easy method for steganography is LSB method. It is a technique that allows the secret data to be inserted in the least significant bit of the audio samples of a wav file [9][10][11]. The combination of two techniques empowers the security system and increases its immunity against attackers. Only the authorized person who knows the secret keys for both techniques able to retrieve plain messages. The main goal of this paper is to produce a system that consists of two steps; the first step is cryptography to secure text messages and duplicate the security level by hiding it in a cover file of wav signal using the signal of audio file value with a random distribution. The audio file data are real values in the range [-1,1]. So the values of the wav sample( positive or negative) are taken to hide message bits. A secret text message is encrypted with the Hill encrypted method then embedded within an audio file in a random distribution depending on the sign (negative or positive) of the audio values. The audio file is restricted to be *.wav stereo file, Two secret keys are needed encryption key and the seed of generating hiding positions.

2. Related Work

Audio steganography works were presented by many researchers to discuss the security of information and data file of different forms like text, images, and audio by hiding them within an audio file or the audio embedded in it. The researchers concerned with the combination of encryption and steganography. Many studies take the audio file as a matter of interest either for its importance as a file of big data to be used as a carrier file or secret information needed for protection[10]. Both
frequency domain like DWT and DFT or time domain for an audio file are used for hiding. In time
domain a Least significant Bit (LSB) is an effective method that could be used to insert the
information in a cover file[12]. Researchers like Krishna Bhowal et.al. (2011) produced an audio
Steganography for securing encrypted text messages based on and LSB technique. In their system,
they used the encryption algorithm (RSA) to encrypt the message as the first level of security then, the
encrypted message bits are hidden in random and higher LSB layers that gave their system more
robustness against noise addition and reduce distortion[13]. S.S. Divya and M. Ram Mohan
Reddy(2012) proposed two approaches of replacement techniques for audio steganography that
increases the capacity of cover audio for hiding additional data. In these methods, the message bits are
hidden into a variable and multiple 4 LSBs. They used the RSA algorithm for the encryption
process[14].

S.Hemalatha et.al. (2015 ) proposed an audio steganography system based on Discrete Wavelet
Transform (DWT) for the cover audio file to secure data hiding. The data was an encrypted text
message using a dynamic encryption algorithm. The cipher text is then hidden in wavelet coefficients
of the cover audio signal[15].

Mazhar Tayel et.al. (2016) used the LSB method for embedding data in an audio file and stated
that the sound quality of the cover file depends on its size and length of the hidden message [16]. Samah M. H. Alwahbani and Huwaida T. I. Elshoush (2017) also proposed new chaos steganography
and cryptography for audio files. They applied an (LSB) layers method for the plain message to
crypt it by a one-time pad algorithm. They used two chaotic sequences of Piecewise Linear Chaotic
Map (PWLCM), one for generating the encryption key while the other to generate a random sequence
for steganography process that used to embed the encrypted message in randomly selected audio
samples [3]. While Jibran Hashim et.al. (2018) invested the AES encryption method as a backup in
case the steganography algorithm has been broken, They used Least Significant Bit (LSB)
mofification technique as random bit spreading wise for secret message bits on different bits of the
sample [9].

Some researchers tended to study encryption and try to improve encryption algorithms to get more
immune systems, B. Ravi Kumar and Dr.P.R.K.Murti(2011) produced a Bit Shifting and Stuffing
(BSS) methodology for encryption the text messages . The printable character needs 7 bits and the last
bit value is 0 which is wasted in the character. In the BSS method, they are stuffing a new bit in the
place of the wasted bit which is shifting from another printable character because the computer system
requires one byte to represent a printable character i.e. 8 bits. After encryption, for every 8 bytes of
plain characters, it will generate 7 bytes cipher characters and in decryption, Every 7 bytes of cipher
characters will reproduce 8 bytes of plain characters[1].

3. **Proposed System**

The proposed system is a hybrid system aims to secure text messages through two security
schemes: Encryption and Steganography. The text is encrypted by the Hill Encryption algorithm then
hidden within a sound file in the time domain by changing the sign of the cover file values. The
system consists of two phases illustrated in Figure(1):
3.1. **Cryptography Phase**

The security first step is to encrypt the plain message by using a Hill algorithm which is a symmetrical key algorithm that uses a matrix(n×n) as a key and multiplies it by the ASCII code of the characters of the plain text, the encryption is done by the sender as follows:

a) Choosing an appropriate key which is a square matrix of n×n of an integer number and its inverse should be integer too for decryption phase.

   ex: key=[1 5 3; 2 11 8; 4 24 21].

b) Let M_plain is a plain text message needed to be secured, converted to ASCII code:

   M_plain='God pleas u!'

   asci_M=[71 111 100 32 112 108 101 97 115 32 117 33].

c) Reshape the asci_M to (m×n) Matrix. 

   A_M= [71 111 100; 32 112 108; 101 97 115; 32 117 33].

   Note: if the the A_M can’t be m×n dimension, It should be completed with zero’s to make the multiplication done.

d) Multiply the asci_M with Key matrix to get Cipher_text by transforming ASCII to characters:

   A= mod( A_M * Key,128).

   A = [30 20 35 76; 115 112 13 79; 56 92 27 45].

   Cipher_text=[-#Lsp← O8-]

e) Hide the Cipher_text in a wav file and send it to the receiver.

f) end

At the receiver side, He extracts (unhide) the Cipher_text from cover file and decrypts it by reversing encryption steps means, multiplying the asci_code of Cipher_text by the inverse matrix of the encryption Key to get ASCII code of plain text and transforms it to characters then reconstructs a plain message again.

3.2. **Steganography**

The second step of the system is hiding Cipher_text in a cover file that is a wav file of two channels (stereo), using a substitutional method for hiding the Cipher_text in random positions in the second channel of the cover wav file, the steps of hiding algorithm is done as follows:

a) Taking the Ascii code of Cipher text and transform it to binary code:

   [30 20 35 …]=[01110010100100011… ]

b) Calculating the number of bits of the cipher message and using a seed number (as a hiding key) exchanged between the sender and receiver to generate a number of random locations equal to the number of message bits to hide in.
c. The message bits are spread randomly in generated positions in such a way that:

\[ y(i) = \begin{cases} 
-|y(i)|, & \text{bit}(h) = 0 \\
|y(i)|, & \text{bit}(h) = 1 
\end{cases} \]

\( y(i) \) is the original sample of the cover file, \( i \) is randomly generated positions, \( h = 1,2, \ldots \text{No. of bits} \).

\[ y = [0.002 - 0.0019 - 0.0018 0.0016 0.0015 ...] \]

\[ y = [-0.002 - 0.0019 0.0018 0.0016 0.0015 ...] \]

d. Reconstruct the wav file samples and send it to receiver.

e. End

The capacity of wav file to hide messages varies depending on sampling rate of the audio file. Each character needs 7-bits to be represented so, if the sampling rate for a wav file is 48000 samples/second that means each second of wav file can carry over than 6000 characters, but in proposed system, the bits of the Cipher message are distributed randomly thus, they can’t be noticed, hard to collect and arrange as well as the noise in sound file undetected, Figure(2) shows the wav file before and after hidden process.

![Figure(2) A cover wav file channel two that carry a cipher message with lengths: (a) has 1308 characters and (b) 444 characters](image)

At a receiver side, the seed number is used to generate the locations of the message bits, collect them and form the ASCII code of the cipher text then decrypt it as in algorithm 3.1.

4. Results Analysis

The cover file in this paper restricted to be an audio (.wav) file format and the secret message is a text file. The system was tested for many sizes of audio files and message files, each time the size of cover file should be at least 7 times of text message file for ensuring the reliability of the system. The simulation is implemented with MATLAB R2018a software with core™ i7-3520M CPU@2.90GHz.

The measures PSNR, MSE, SSIM are calculated between cover file before and after embedding to ensure the imperceptibility requirement the results are shown in Table (1).
Table (1) PSNR, MSE, SSIM between the same cover before and after embedding

| Size of message (character) | PSNR   | MSE          | SSIM |
|-----------------------------|--------|--------------|------|
| 444                         | 75.782 | 3.6657e-06   | 1.0  |
| 1308                        | 61.4373| 7.0823e-05   | 1.0  |
| 2170                        | 60.67  | 9.8428e-05   | 1.0  |
| 2500                        | 89.6534| 9.9987e-09   | 1.0  |

As in Table (1) The system approved its efficiency in securing data and hiding it with least noise in the cover file.

The two important keys of the system are the encryption key that responsible for message distortion and the seed number that used for generating a series of random numbers to create locations for spreading message bits. To expose the message by the receiver he should know these two keys, otherwise, the mission is impossible. The sender and receiver exchange the keys between them either by dealing before or sending it secretly.

The time consumption for steganography and cryptography vary proportionally to messages length, and the time for decryption is less than that consumed in encryption for the same length of message. On the other hand the time needed for hide the same message is longer than its encryption time, as shown in Table (2).

| Size of message (character) | Encryption time | Decryption time | Hiding | Unhide |
|-----------------------------|-----------------|-----------------|--------|--------|
| 444                         | 0.011           | 0.0128          | 0.027  | 0.069  |
| 1308                        | 0.0208          | 0.066           | 0.091  | 0.0822 |
| 2170                        | 0.0273          | 0.0715          | 0.159  | 0.106  |
| 2500                        | 0.095           | 0.099           | 0.18   | 0.12   |

5. Conclusion

The security of the data is the most important issue in the digital world; Both Steganography and cryptography are together forming an integral system for security purposes. In our proposed system, the audio file is used as a cover file for securing an encrypted message. A Hill encryption method was used to encrypt the message, while audio steganography uses a new technique for hiding the message bits without changing cover values. It takes the signal of the audio samples (negative or positive) to act like 0 or 1 and randomly spreading the bits through a position generator seed as a hiding key. Both the keys must be private between the sender and receiver. This method is appropriate for securing any type of data like text or image with a minimum rate of distortion to the original sound wav and completely retrieving for the hidden messages and it was good in minimizing the noise in the cover file as measured by PSNR, MSE and SSIM for different lengths for tested messages with less time consumption.

References

[1] B. Ravi Kumar, Dr. P. R. K. Murti, (2011),” Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS) Methodology”, International Journal on Computer Science and
Engineering (IJCSE), Vol. 3 No. 7, pp: 2818:2827

[2] Huda adel ali, Enas wahab Abood and Wafaa A. Khudhair, (2019), “Using LSB Method For Hiding Hill Encrypted Grayscale And RGB Images In RGB Image”, Journal of University of Garmian, Special Issue Conference paper SCPAS-2019, pp:46-53.

[3] Samah M. H. Alwahbani and Huwaida T. I. Elshoush, (2017), “Hybrid Audio Steganography and Cryptography Method Based on High Least Significant Bit (LSB) Layers and One-Time Pad—A Novel Approach” Proceedings of SAI Intelligent Systems Conference, Intelligent Systems and Applications, pp: 431-453.

[4] K. Saktisudhan, P. Prabhu and P. Thangaraj, (2012), “Secure Audio Steganography for Hiding Secret information”, International Conference on Recent Trends in Computational Methods, Communication and Controls (ICON3C 2012) Proceedings published in International Journal of Computer Applications® (IJCA), pp:33-37.

[5] Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim and Hassanain Mahdi Alzuabidi, (2019), “Combination of Steganography and Cryptography: A short Survey”, 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019), IOP Conf. Series: Materials Science and Engineering 518 (2019) 052003, IOP Publishing, doi:10.1088/1757-899X/518/5/052003, pp: 1-13.

[6] Hashim M, Rahim M, Shafry M and Alwan A A, (2018), “A review and open issues of multifarious image steganography techniques in spatial domain”, Journal of Theoretical & Applied Information Technology 96.

[7] Chua Teck Jian, Chua Chai Wen, Nurul Hidayah Binti Ab. Rahman, Isredza Rahmi and Binti A. Hamid, (2017), “Audio Steganography with Embedded Text” International Research and Innovation Summit (IRIS2017) IOP Publishing, IOP Conf. Series, Materials Science and Engineering 226 (2017) 012084 doi:10.1088/1757-899X/226/1/012084.

[8] Mohammed Pooyan, Ahmed Delforouzi, (2007), “LSB based steganography method based on lifting WaveletTransform”, IEEE international symposium on signal processing and information technology.

[9] Jibran Hashim, Arsalan Hameed, Muhammad Jamshed Abbas, Muhammad Awais, Hassaan Aziz Qazi and Sohail Abbas, (2018), “LSB Modification based Audio Steganography using Advanced Encryption Standard (AES-256) Technique”, 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), IEE, DOI: 10.1109/MACS.2018.8628458.

[10] Rina Mishra and Praveen Bhanodiya, (2015), ”A Review On Steganography And Cryptography “, International Conference on Advances in Computer Engineering and Applications, IEEE, DOI: 10.1109/ICACEA.2015.7164679.

[11] Pooja P. Bulguri and Sonal K. Jagtap, (2013),” Audio Steganography Used for Secure Data Transmission”, Aswatha Kumar M. et al. (Eds.): Proceedings of ICAdC, AISC 174, Springer India, pp. 699–706.

[12] K. Thangadurai; G. Sudha Devi (2014),” An analysis of LSB based image steganography techniques”, International Conference on Computer Communication and Informatics, IEEE Xplore, Coimbatore, India, DOI: 10.1109/ICCCI.2014.6921751.

[13] Krishna Bhowal · Debnath Bhattacharyya · Anindya Jyoti Pal · Tai-Hoon Kim, (2013), ”A GA based audio steganography with enhanced security”, Springer Science+Business Media, LLC, Telecommun Syst (2013) 52 pp:2197–2204, DOI 10.1007/s11235-011-9542-0.
[14] S.S. Divya and M. Ram Mohan Reddy ,(2012),”Hiding Text In Audio Using Multiple Lsb Steganography And Provide Security Using Cryptography”, International Journal Of Scientific & Technology Research Vol. 1, Issue (6), ISSN 2277-8616.

[15] S. Hemalatha, U. Dinesh Acharya, A. Renuka, S. Deepthi and K. Jyothi Upadhya,(2015),” Audio steganography in discrete wavelet transform domain”, Journal of International Journal of Applied Engineering Research,Vol.10, Issue (16), pp: 37544-37549.

[16] Mazhar Tayel , Ahmed Gamal and Hamed Shawky, (2016),” A proposed implementation method of an audio steganography technique”, 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, South Korea ,IEEE Xplore INSPEC Accession Number: 15824048 ,DOI:10.1109/ICACT.2016.7423320 .