IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. V (Mar – Apr. 2015), PP 55-60
www.iosrjournals.org

Adaptive Steganography Based Enhanced Cipher Hiding Technique for Secure Data Transfer

Sudipta Sahana[1], Goutami Dey[2], Madhurhita Ganguly[2], Priyankar Paul[2], Subhayan Paul[2]

[1](*Asst. Professor, Dept. of Computer Science and Engineering, JIS College of Engineering, West Bengal, India)*
[2](*B.Tech. Dept. of Computer Science and Engineering, JIS College of Engineering, West Bengal, India)*

Abstract:*There have been enormous number of attacks recorded during electronic transmission of information between the source and intended receiver and indeed this has called for a more robust and efficient method for secured data transfer and making it more credible. Cryptography and Steganography are the widely used techniques that manipulates and conceal the information in order to cipher and hide their existence. These two techniques share the common goals and services of shielding the confidentiality, integrity andprevent the access of information by unauthorized users. In this project, a data hiding system which is grounded on audio steganography and cryptography is proposed for authenticateddata transfer. Steganographic medium used in this project is the audio medium. The encryption and decryption methods of cryptography used in developing this system make the surety of the proposed system more efficient in securing the data from unauthorized access. The system thus proposed is therefore recommended for use by the Internet users for founding a more safe and secure system. In this project, an audio medium is used as the steganographic and an advanced algorithm is applied for encoding the private data into the audio file.The goal of this research is to combine both cryptography and steganography in order to develop a better and credible communication in this unsecured open network.*

Keywords:*cryptography, decryption, encryption, Internet, steganography.*

I. Introduction

Steganography is an art of hiding information. The steganographicsystem embeds secret content in a cover media and makes it unremarkable for the eavesdropper. Earlier people used invisible ink or hidden tattoos to transmit steganographic content. The information embedding process in a steganographic system starts by identifying the redundant bits of the cover medium. The embedding process results in a stego medium by replacing the redundant bit of the cover medium with the data of the secret message. The main aim of using such a technique is to make the secret message undetectable to the unauthorized users. There is one more technique used to cipher the existence of the secret message which is cryptography. Cryptography scrambles a message so that it cannot be understood whereas steganography is a technique that is used to hide the secret message so that it is undetectable by the unintended users.

Basically, the purpose of cryptography and steganography is to provide secret communication. Steganography can be used to cloak hidden messages in image, audio, video and even text files. The two most common methods used for hiding information inside a picture, audio and video files are LSB (Least Significant Bit) and Injection.In this paper, audio medium is used for steganography and a modified LSB algorithm is used to embed the secret message.

II. Related Works

Vivek*et al.* (2012) [1] proposed a method to implement the steganography and cryptography for concealing the data into a medium. The steganography medium used in this data hiding system is audio and Least Significant Bit (LSB) algorithm is used for encoding the message in the cover medium. The encryption and decryption algorithm thus used makes the security of the system more efficient in concealing the data.

Abikoye*et al.* (2012) [2] proposed a system that integrated both cryptography and steganography where audio file is used as cover medium for steganography and a more powerful and qualified LSB algorithm is applied in order to achieve security of the information to be transmitted.

Jayaram*et al.* (2011) [3], presented the different types of audio steganographic methods, its advantages as well as disadvantages. This paper has proposed an efficient and robust method of unperceivable audio data hiding. Thus we conclude that audio data hiding techniques can be used for a list of other intents than covert communication or deniable data storage, tamper detection, finger printing and information tracing.

Raphael *et al.* (2011) [4], discussed how combining both steganography and cryptography will provide better security and confidentiality.Cryptography makes the information incomprehensible so that no intruder can

interpretthe original information. However, steganography focuses on hiding the existence of the secret information.

Sujay*et al.* (2010) [5] proposed a technique where cryptography and steganography is combined to encrypt the data and hide the data which is encrypted in the cover medium so that the secret data that is being sent is completely concealed.This paper proposes two new methods in which cryptography and steganography are fused to encrypt the data as well as to hide theencrypted data in the cover medium so the fact that amessage that is being transmitted is concealed. One method is to convert image into cipher text by S-DES algorithm using a secret key and hiding this text in another image using steganographic method. Another method is encrypting the image directly by S-DES algorithm with the use of key image and then it is then concealed in another image.

Mohammad *et al*. (2010) [6] proposed a steganography technique used to hide the data in the cover media and a key is used to hide the data and the Diffie-Hellmann exchange Protocol is used to exchange the data between the sender and the receiver. Proposed method that described two steps for hiding secret information by using the public steganography based on matching method. The first step is to find the shared stego-key between the two communication parties (Alice and Bob) over the networks by applying Diffie Hellman Key exchange protocol. The second step in the proposed method is that, the sender uses the secret stego-key to select pixels that it will be used to hide. Each selected pixel is then used to hide 8 bits binary information.

Dipti*et al.*(2011) [7], cryptography entirely is not enough for secure and credible communication. Both cryptography and steganography provides security and confidentiality in its own way.

Srideviet *al.* (2011) [8] presented that the goal of the steganography is in concealing the secret data by beclouding. The secret data is hidden in the cover medium. Steganography is different from cryptography in an aspect that cryptography is used to make the data unreadable for the unwanted users but at the same time it cannot prevent the unwanted user from learning about their existence whereas steganography hides the very existence of the secret message. The success of the steganography depends holistically on the ability to conceal the secret data in the cover media such that observe do not suspect its existence. Steganography must ensure that the message is invisible until the receiver knows what to look for and how. The process of hiding the data depends upon the medium used for hiding the information. Capacity of hiding information or the amount of information that can be concealed in the medium before it becomes detectable, can be measured.

Niel*et al.* (2003) [9], presented subsistingsteganographicsystems and presents the current research in observing them through statistical steganalysis. This paper discussed about the practical applications and mechanisms of detection algorithms. This article discusses existing steganographic systems and presents recent research in detecting them viastatistical steganalysis. Other surveys focus on the general usage of information hiding and watermarking orelse provide an overview of detection algorithms. The article presented recent research and discussed the practical application of detection algorithms and the mechanismsfor getting around them.

Mark *et al.* (2003) [10] presented an image steganography software named "Chameleon". It features an encoding algorithm for 24 bit true color images. This software for 24-bit true-colorimages features a novel adaptive encoding algorithm founded on the steganographic model conceived by Yeuan-Kwen Lee and Ling-Hwei Chen for grayscale images.

III. Methodology

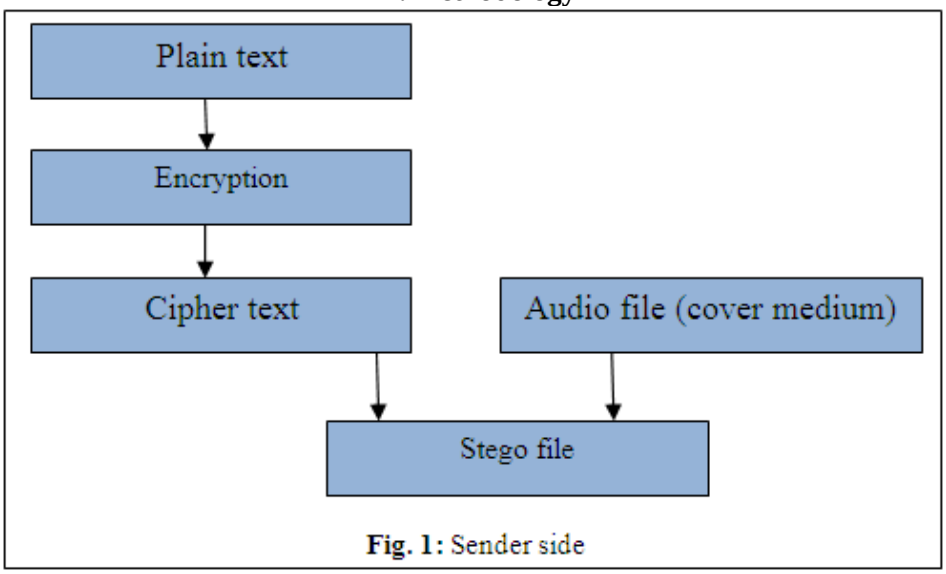

Fig. 1: Sender side

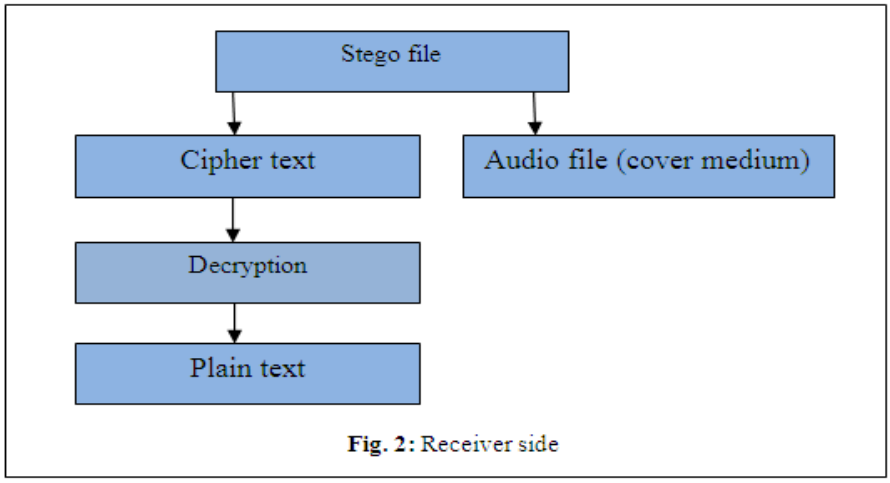

Fig. 2: Receiver side

3.1 Sender side

3.1.1 Take the secret message that we want to hide as an input string called as plain text. Determine the ASCII value of each of the character and convert the ASCII value of each character of the secret message into binary. Each character is 8 bit binary; hence its value ranges from 0-255.

3.1.2 Let the length of the input string be len, then considering the input string defined as Message [8xlen] 2-D array. Let each row be called as BitStream.

3.1.3 Conducting the following steps on the first row of the Message[8xlen]:
As already known each row is of 8 bits, this BitStream is to be converted into 2's complement which comprises of following steps:

a. Complementing each bit in the row.
b. Then binary addition of 1 is done to the BitStream. The result obtained is the 2's complement of the BitStream of the row.

Similarly finding 2's complement for each of the row of the array

3.1.4 Now conduct XOR operation between consecutive rows of the array, replace the even row with the result of the XOR.
If length of the message is odd i.e. len%2=1, then leave the last row as it is.

3.1.5 Converting the audio file into bit stream and sampling it in 16 bits.

3.1.6 Store the LSB of the sampled audio stream in the array namedLSBarray.

3.1.7 For each BitStream in the Message

Embedding (BitStream ,LSBarray)
If BitStream exists in the LSBarray as a substring
Return the starting and the ending row number of the substring in the LSBarray.
Else
The BitStream is divided as the left part and the right part and
stored in Left_BitStream and Right_BitStream.
Embedding (Left_BitStream, LSBarray)
Embedding (Right_BitStream, LSBarray)
Return output and store it in the Key_Array.

3.2 Receiver side

3.2.1 The elements received by the receiver is the audio and the Key_Array.

3.2.2 Forming the array of the LSB of the audio received by the sender and naming it LSB_Array.
For (no. of iteration)<= (size of the Key_Array)

Examining each value in the LSB_Array where the even indices including 0 are the starting indices and the odd indices are the ending indices.
i.e. examining values Stored in Key_Array[0] and Key_Array[1], those values are the indices in the LSB_Array which has common substring as the BitStream or the decomposed BitStream , similarly in Key_Array[2] and Key_Array[3], so on and so forth. Thereby extracting the encrypted message in the audio.

3.2.3 Now for decrypting, conduct XOR operation between consecutive rows of the array, replace the even row with the result of the XOR. If length of the message is odd i.e. len%2=1, then leave the last row as it is.

3.2.4 Then substracting 1 from each BitStream, resulting in an intermediate message.

3.2.5 Conducting 1's complement on the intermediate message , thereby the resultant message is the original message.

3.3 Example:

Let the original message be "hey" which is to be stored in the 2D array Message[8x len] where len is equal to 3 in this message.
Converting the original message in binary i.e.

Character	ASCII / Decimal	Binary
h	104	01101000
e	101	01100101
y	121	01111001

Therefore the original message, Message[8 x 3] is

0	1	1	0	1	0	0	0
0	1	1	0	0	1	0	1
0	1	1	1	1	0	0	1

Now forming an array of LSB named LSB_array of the sampled (into 16 bits) cover medium i.e.

1	1	0	1	1	0	0	0	1	0	0	1	1	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	0	1

3.3.1 Sender Side:

3.3.1.1 Encryption: First Conducting 2's complement operation on the original message which gives an intermediate message

1	0	0	1	1	0	0	0
1	0	0	1	1	0	1	1
1	0	0	0	0	1	1	1

3.3.1.2 Now, conducting XOR operation as per the algorithm .
Performing XOR operation on the 1st and the 2ndBitStream (comprises 8 bits).

1stBitStream	1	0	0	1	1	0	0	0
2ndBitStream	1	0	0	1	1	0	1	1
Result	0	0	0	0	0	0	1	1

3.3.1.3 Now, replacing the 2ndBitStream with the result of the XOR operation. And the 3rdBitStream is left as it is as per the algorithm because len%2 =1.
3.3.1.4 Encrypted message is

1	0	0	1	1	0	0	0
0	0	0	0	0	0	1	1
1	0	0	0	0	1	1	1

3.3.1.5 Encoding the encrypted message in the LSB_Array. For each BitStream in the Message, Embedding (BitStream, LSB_Array) is called.
Embedding(10011000, LSB_Array), first checking for the 1stBitStream 10011000 in the LSB_Array. The string is found in the index of 8 to 15. Therefore inserting the indices in the Key_Array. Status of the Key_Array is shown below.

8	15				.....						

Embedding(00000011, LSB_Array), checking the 2ndBitStream 00000011in the LSB_Array. The string is not found . Therefore the BitStream is divided into equal left and right substring.

Then Embedding(0000, LSB_Array) is called which returns 17 and 20. Status of Key_Array is

8	15	17	20		.....						

Then Embedding(0011, LSB_Array) is called, which returns 9 and 12. Status of Key_Array is

8	15	17	20	9	12		.....				

Embedding(10000111, LSB_Array), checking the 3rdBitStream 10000111 in the LSB_Array. The string is not found. Therefore the BitStream is divided into equal left and right substring.
Then Embedding(1000, LSB_Array) is called which returns 4 and 7. Status of Key_Array is

8	15	17	20	9	12	4	7			.....	

Then Embedding(0111, LSB_Array) is called, which returns 22 and 25. Status of Key_Array is

8	15	17	20	9	12	4	7	22	25		.....	

3.3.1.6 Therefore the elements to be sent to the receiver is the audio and the Key_Array.

3.3.2 Receiver Side:

3.3.2.1 Forming the array of the LSB of the audio received by the sender and naming it as LSB_Array.

1	1	0	1	1	0	0	0	1	0	0	1	1	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	0	1

3.3.2.2 Examining two indices in each iteration where the even indices including 0 denoted starting indices and the odd indices denotes ending indices.
Examining Key_Array[0] and Key_Array[1]. Values stored in them is 8 and 15. Therfore looking for the bits in the index 8 to 15 in the LSB array which gives 10011000, which comprises of 8 bits , hence encrypted 1stBitsream received.
Examining Key_Array[2] and Key_Array[3]. Value stored in them is 17 and 20. So bits in the position 17 to 20 in the LSB_Array is 0000, 4 bits obtained and 4 bits left to obtain the second encrypted character.
Examining Key_Array[4] and Key_Array[5]. Value stored in them is 9 and 12 therefore similarly bits obtained is 0011. Hence the 2nd encrypted BitStreamis 00000011.
Examining Key_Array[6] and Key_Array[7]. Value stored in them is 4 and 7, therefore similarly bits obtained is 1000.
Examining Key_Array[8] and Key_Array[9]. Value stored in them is 22 and 25, therefore similarly the bits obtained is 0111. 3rd encrypted BitStream is 10000111.
Therefore the encrypted message obtained is

1	0	0	1	1	0	0	0
0	0	0	0	0	0	1	1
1	0	0	0	0	1	1	1

3.3.2.3 Now the encrypted message is to be decrypted. So the XOR operation is to be performed on the encrypted message as per the algorithm.

1stBitStream	1	0	0	1	1	0	0	0
2ndBitStream	0	0	0	0	0	0	1	1
Result	1	0	0	1	1	0	1	1

Replacing the 2ndBitStream with the result of the XOR operation. And the 3rdBitStream is left as it is as per the algorithm. Therefore the intermediate message is

1	0	0	1	1	0	0	0
1	0	0	1	1	0	1	1
1	0	0	0	0	1	1	1

3.3.2.4 Nowsubtracting 1 from each of the BitStream. Therefore the intermediate message is

1	0	0	1	0	1	1	1
1	0	0	1	1	0	1	0
1	0	0	0	0	1	1	0

3.3.2.5 Now 1's complement is performed on the intermediate message , which gives

0	1	1	0	1	0	0	0
0	1	1	0	0	1	0	1
0	1	1	1	1	0	0	1

Therefore the original message is extracted from the audio.

IV. Results And Discussion

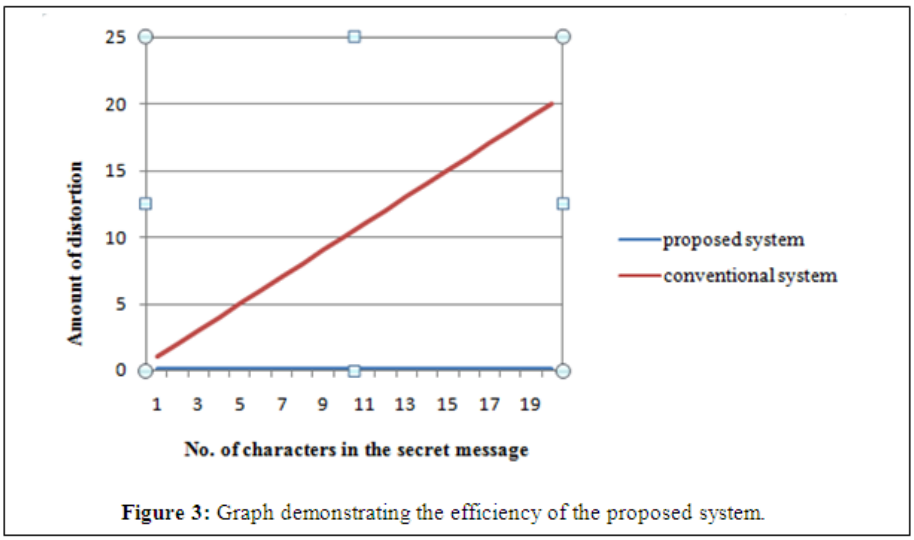

Figure 3: Graph demonstrating the efficiency of the proposed system.

According to the result analysis in this figure, we have shownthe comparison between the conventional system and the proposed system that has no distortion in the audio. Conventionally, as the number of characters in the hidden message that is to be embedded increases, distortion in the audio increases. As more the manipulation in the bits of the original audio is going to take place which leads to distortion therefore leads to deterioration of the quality of audio which is quite crucial as the distortion might lead to emergence of suspicion among the intruders about the embedded secret information. The proposed method is robust and efficient as it leads to zero distortion as it has no manipulation in the bits of the original audio. Therefore, the proposed system is recommended for the use of internet user as it provides higher security because there is no manipulation in the bits of the audio so does not bring into the attention of attackers.

V. Conclusion

The proposed system, thus fuses both cryptography and steganography to present a highly efficient system for concealing data from undesirable user. Novel algorithms have been used for implementing cryptography and steganography. The proposed system is highly efficient as far as security and confidentiality of the data transmission is concerned. As only the audio and an array, is sent to the receiver with no sort of embedding and manipulation in the bits of the audio, the audio is absolutely distortion free. As this is an audio, so the quality of the audio is a high concern. The proposed system has no deformation in the bits of the audio using this proposed algorithm therefore there is no distortion so does not bring suspicion in the mind of attackers. Therefore the proposed system is robust and credible for the Internet users.

Reference

[1]. Vivek, J., Lokesh, K., Madhur, M. S., Mohd, S., and KshitizRastogi 2012. Public-Key Steganography Based on Modified LSB Method. Journal of Global Research in Computer Science, 3(4). ISSN: 2229-371X, pp. 26-29.

[2]. AbikoyeOluwakemi, C., AdewoleKayode, S., &OladipupoAyotunde, J. 2012. Efficient Data Hiding System using Cryptography and Steganography. International Journal of Applied Information Systems (IJAIS)–ISSN, 2249-0868,4(11).

[3]. Jayaram, P., Ranganatha, H. R. and Anupama, H. S. 2011. Information Hiding Using Audio Steganography – A Survey. International Journal of Multimedia and Its Application, 3(3), pp. 86-96.

[4]. Raphael, A. J., and Sundaram, V. 2011. Cryptography and Steganography - A Survey. International Journal of Computer Technology Application, 2(3), ISSN: 2229-6093, pp. 626-630.

[5]. Sujay, N. and Gaurav, P. 2010. Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions. Signal & Image Processing: An International Journal (SIPIJ), 1(2), pp 60-73.

[6]. Mohammad, A. A., and Abdelfatah, A. Y. 2010. Public-Key Steganography Based on Matching Method. European Journal of Scientific Research, 40(2). ISSN: 1450-216X. EuroJournals Publishing, Inc., pp. 223-231. Retrieved 21st August, 2012 from http://www.eurojournals.com/ejsr.htm.

[7]. Dipti, K. S. and Neha, B. 2010. Proposed System for Data Hiding Using Cryptography and Steganography. International Journal of Computer Applications. 8(9), pp. 7-10. Retrieved 14th August, 2012 from http://www.ijcaonline.org/volume8/number9/pxc3871714.pdf.

[8]. Sridevi, R., Damodaram, A., and Narasimham, S. 2009. Efficient Method of Audio Steganography By Modified LSB Algorithm and Strong Encryption Key with Enhanced Security. Journal of Theoretical and Applied Information Technology, pp. 768-771. Retrieved 21st August, 2012 from http://www.jatit.org.

[9]. Niels, P. and Peter, H 2003. Hide and Seek: An Introduction to Steganography. IEEE Computer Society. IEEE Security and Privacy, pp. 32-44.

[10]. Mark D. G. 2003. Chameleon Image Steganography- Technical Paper. Retrieved 14th July, 2012 from http://faculty.ksu.edu.sa/ghazy/Steg/References/ref13.pdf.