A Double Layer Protection Transmission Technique Using Cryptography and Steganography

Tanmaiy G Verma, Zohaib Hasan , Dr. Girish Verma

Abstract—**The current era has seen an explosive growth in communications. Cryptography and steganography are the available techniques for network intrusion detection system. However, to match the highly secure requirement for confidential data of today's applications, highly secure and hardware acceleration of the algorithms is a necessity. So to overcome such problem proposed work has come up with the combination of both the methods, i.e. steganography cum cryptography. With these methods the cons of both the methods can be resolved. The problem with cryptography is that it is easy to detect and the problem with steganography is that it is easy to de-crypt. So by using combination of both the cons of each can be used as advantage of each other. Proposed work introduces double layer protection along with a new run time inter-leveling based audio steganography technique.**

Index Terms— **Cryptography, Steganography**

I. Introduction

Due to advances in information coding theory, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. Steganography is a technique of hiding information in digital media. In contrast to cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown.

Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography. All these applications of information hiding are quite diverse.

II. OVERVIEW CRYPTOGRAPHY

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality , data integrity, authentication, and non-repudiation.

III. OVERVIEW STEGANOGRAPHY

Steganography is the art and science of hiding information such that its presence cannot be detected and a communication is happening. Secret information is encoding in a manner such that the very existence of the information is concealed. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed.

The basic model of steganography consists of *Carrier*, *Message* and *Password*. Carrier is also known as *cover-object*, which the message is embedded and serves to hide the presence of the message.

IV. STEGANOGRAPHY VS CRYTPOGRAPHY

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from a malicious people, whereas steganography even conceals the existence of the message. Steganography must not be confused with cryptography, where we transform the message so as to make it meaning obscure to a malicious people who intercept it. Therefore, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system need the attacker to detect that steganography has been used and he is able to read the embedded message.

IV. METHODOLOGY

The communication system consists of two sections, one is the transmitter and the other is receiver. This methodology is

Manuscript received Oct, 2013.

Tanmaiy G Verma, *Deptt. Of Electronics and Communication ,Gyan Ganga Institute of Technology, Jabalpur, India,+91-9425158090*

Zohaib Hasan, *Asst. Professor ,Deptt. Of Electronics and Communication, Gyan Ganga Institute of Technology,*
, Jabalpur, India, +91-9826689969., (e-mail: zohaib166@gmail.com*).*

Dr. Girish Verma, Professor , Deptt. Of Physics , Govt. Home Science College,*Jabalpur, India,+91-9425158090.,*

the over-view of the system employed in the successful transmission of the data. Both of the system are being discussed in the detail in the following section:

Transmitter section:

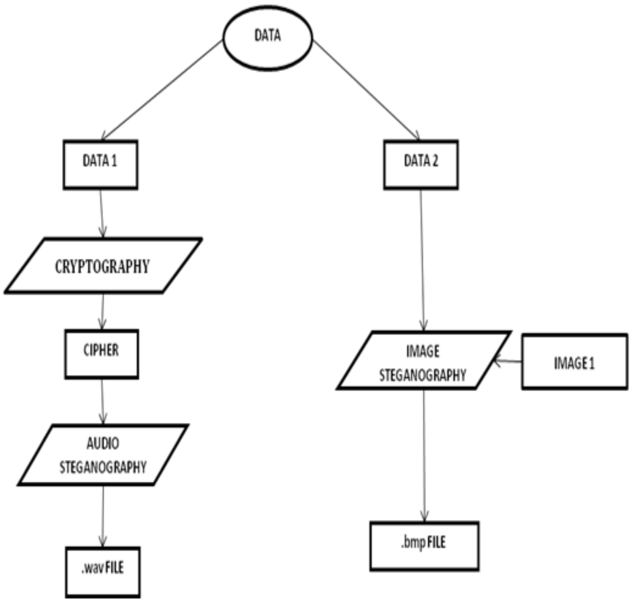

Fig. (a)

The transmitter section is shown in fig (a). Its sub-modules are discussed in details as follows:

Data : Here the data is inserted by the transmitter. In this case the data can be numeric, alpha-numeric or may contain special characters. . This data is divided into sub-parts i.e data-1 and data-2. The data-1 is passed for one process and data-2 is passed for another.

Data 1: The data-1 undergoes the process of cryptography. The process which is used in this thesis work for cryptography is the ‘modulo-approach’. Now as per the modulo-method the cipher is generated.

Data 2 : This part of the data undergoes image steganography and the resultant output is a .bmp file.

Cipher : This is the output of cryptography. This portion is inserted into audio recorded by the transmitter.

Audio- steganography: In this part the cipher is inserted into audio file and the resultant output is a .wav file. In this case the audio file acts as a cover-object. The process which is being used here for steganography is called ‘substitution method ’. This process is also called noise insertion method.

Receiver section:

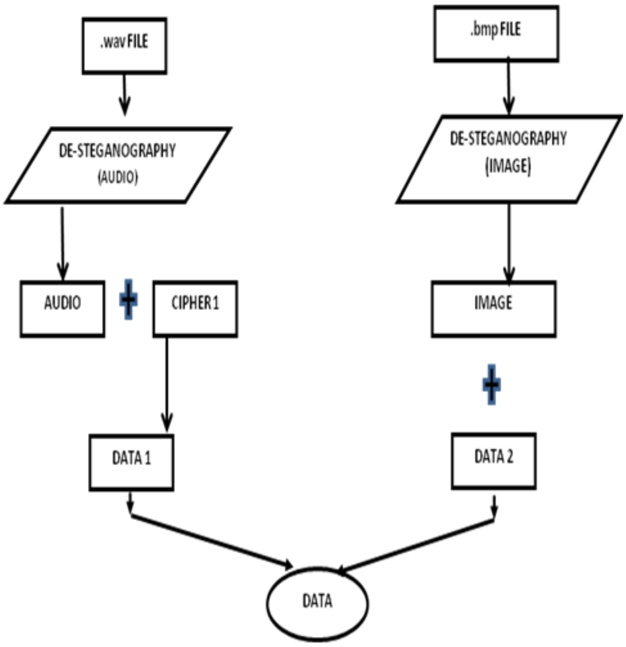

Fig. (b)

The receiver section is shown in fig (b) Its sub-modules are discussed in details as follows:

De-Steganography (Image) : The de-steganography which is the reverse process of steganography. Since we have used LSB method of data insertion hence in the reverse process the data in LSB are extracted to recover half portion of the data.

Data -2 : This is the message extracted from the cover-object (In this case image).

De-Steganography (Audio) : In this case the audio and cipher are separated from the cover-object (In this case audio).

Cipher -1 : The output of de-cryptography yields the half of the original data i.e. data -1.

After this extraction both the outputs are added to recover the original data.

Algorithm used for cryptography:

1. Get the data from the user(Data)
2. Transpose the given data to obtain a transposed matrix(Tdata)

   Tdata = transpose (data)
3. Divide the Tdata by any numerical value say ‘200’

   M = Tdata / 200
4. The ‘Cipher’ so generated can be obtained by calculating the modulo

   Cipher = M % 13

Algorithm used for audio steganography:

1. ‘X’ represents ciphered data
2. ‘W’ represents wave signal
3. ‘Y’ represents wave sound stegano-object
4. Then

Y = [W_0(----),x(0), W_1(----),x(1), W_2(----),x(2), W_3(----),x(3),-------------------]

5. The range of block of ‘W’ is decided at run time as per size of ‘X’

V. SIMULATIONS

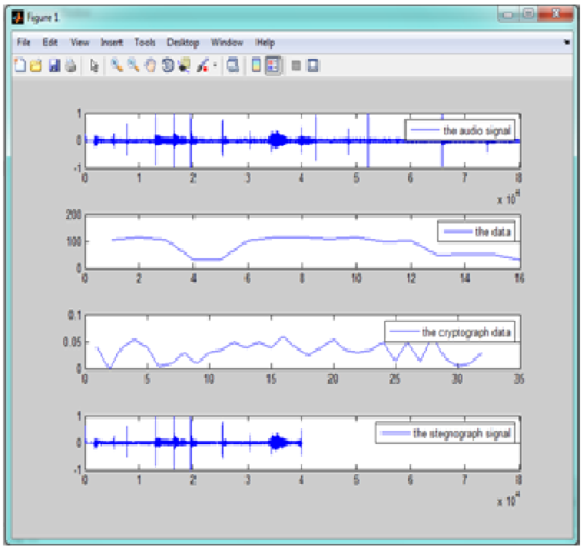

Fig. (c)

The dialog box appears on the screen which displays the amplitude of the following data:

1. The audio signal
2. The data which is to be transmitted
3. The cryptograph data
4. The steganograph signal

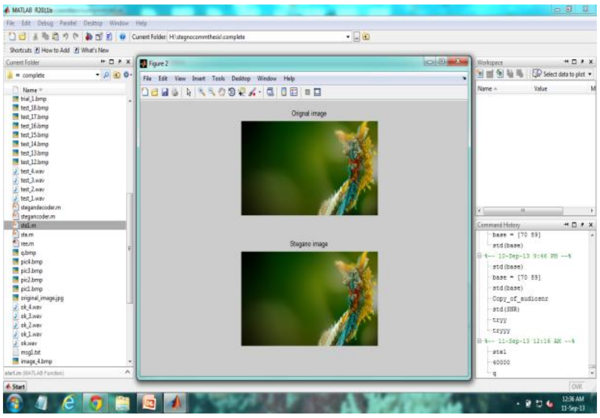

Fig (d)

In the above fig., it can be seen that it is visually impossible to detect the difference between original image and steganographed image.

VI. RESULTS

a. Image analysis:

No. of characters inserted	2	7	12
MSE	0.5787×10^{-5}	0.7716×10^{-5}	0.9645×10^{-5}
PSNR	100.5402	99.2908	98.3217

Here,
MSE is the Mean Square Error
PSNR is Peak Signal to Noise Ratio

b. Audio analysis:

Audio File	Audio File Size (In KB)	Proposed Methodology Results (SNR in db)
Wave_1	390	84.60
Wave_2	490	85.87
Wave_3	590	83.69
Wave_4	680	84.36
Wave_5	830	82.60
Wave_6	940	82.63
Wave_7	1660	84.58
Wave_8	2050	82.86

VII. CONCLUSIONS

Information security is essential for confidential data transfer. Steganography is one of the ways used for secure transmission of confidential information. Hiding information in a photograph is less suspicious than communicating an encrypted file. So steganography can be used for confidential data transfer. On the other hand on focusing on cryptography it is suspicious to the intruder but complex algorithms are available that makes the work of the hacker cumbersome. So combination of both can be used so that confidentiality, data integrity, authentication, and non-repudiation of the data can be maintained.

REFERENCES

[1] Prof. Samir Kumar Bandyopadhyay and Barnali Gupta Banik, “Multi-Level steganographic algorithm for audio steganography using LSB modification and parity encoding technique”, International Journal of Emerging Trends & Technology in Computer Science , Volume 1, Issue 2, July – August 2012

[2] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi , “Overview: Main Fundamentals for Steganography” , Journal of computing, Volume 2, Issue 3, March 2010

[3] Marcelo E. Kaihara and Naofumi Takagi , “A Hardware Algorithm for Modular Multiplication/Division” , IEEE Transactions on computers, Vol. 54, No. 1, January 2005

[4] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath,” A secure and high capacity steganography technique”, Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1, February 2013

[5] Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay, and Tai-hoon Kim,” Text Steganography: A Novel Approach”, International Journal of Advanced Science and Technology Vol. 3, February, 2009

Tanmaiy G Verma has completed his bachelor of engineering from Shri Ram Institute of technology , Jabalpur. He is currently pursuing his masters in technology from Gyan Ganga institute of technology, Jabalpur.

Prof. Zohiab Hasan completed his M.tech from IIIT,Banglore . He is presently working as professor at Gyan ganga Institute of Technology, Jabalpur.

Dr. Girish Verma completed his Ph.D from Rani Durgavati Vishvavidhaya, Jabalpur. He is presently working as Professor in Govt. Home Science College, Jabalpur.