ISSN 2320-9984 01>
9 772320 998022

Volume 2 Issue 1 | March 2014 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

New Approach for Affine Combination of Steganography with Cryptography for Highly Secure Data Hiding

Vartika Pandya
Research Scholar
Department of Electronics and Communication Engg.
Shriram Institute of Technology, Jabalpur
Engineering, Affiliated to RGPV University, Bhopal
Email : 19vartikapandya@gmail.com

Prof. Meenal Jain
Professor & Guide
Department of Electronics & Communication Engg.
Shri Ram Institute of Technology,
Jabalpur M.P., [INDIA]
Email: meenal086@gmail.com

Prof. Ravi Mohan
Head of the Department & Professor
Department of Electronics & Communication Engg.
Shri Ram Institute of Technology,
Jabalpur M.P., [INDIA]
Email: ravimohan7677@yahoo.co.in

Abstract*—The current era has seen an explosive growth in communications. Applications like online banking, personal digital assistants, mobile communication, smartcards, etc. have emphasized the need for security in resource constrained environments. 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 that is 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.*

Keywords:—*MSE(Mean Square Error),SNR (Signal to Noise Ratio), MaTLAB, LSB(Least Significant Bit).*

1. 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'[6]. In contrast to cryptography, the message or 'encrypted message is embedded in a digital host' [7] 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[1][2][4]. All these applications of information hiding are quite diverse.

1.1 Overview Cryptography:

'Cryptography is the practice and study of techniques for secure communication in the presence of third parties' [7]. 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.

1.2 Overview Steganography:

Steganography is the art and science of hiding information such that its presence cannot be detected and a communication is happening[3]. 'Secret information is encoding in a manner such that the very existence of the information is concealed' [5]. 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[3].

1.3 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'[5], 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.

2. METHODOLOGY

The communication system consists of two sections, one is the transmitter and the other is receiver. This methodology is the over-view of the system employed in the successful transmission of the data. Both of the systems are being discussed in the detail in the following section.

2.1 Process flow of transmitter

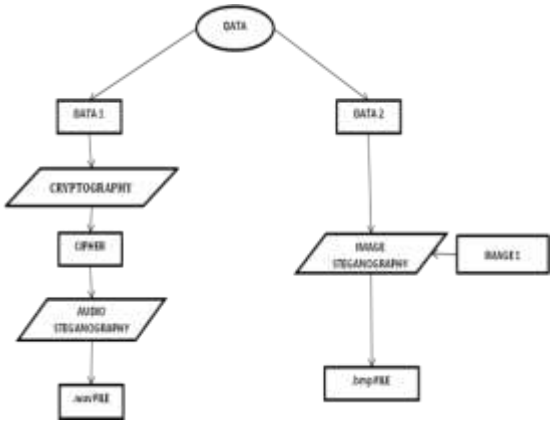

Figure 1 :Methodology Employed in the Transmission of the Data

The transmitter section is shown in Figure 1. 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 will go 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 'interlevel method '.

2.2 Process flow of receiver

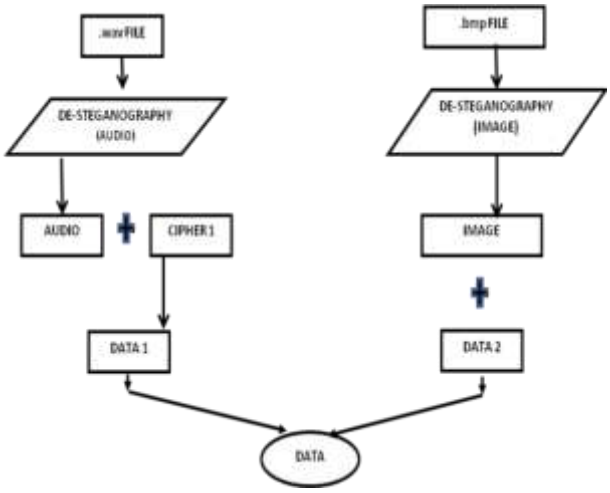

Figure 2: Methodology Employed in the Reception of the Data

The receiver section is shown in figure 2. Its sub-modules are discussed in details as follows:

De-Steganography(Image): The de-steganography will be 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:

Get the data from the user(Data)

Transpose the given data to obtain a transposed matrix(Tdata)

Tdata = transpose(data)

Divide the Tdata by any numerical value say '200'

M = Tdata / 200

The 'Cipher' so generated can be obtained by calculating the modulo

Cipher = M % 13

Algorithm used for audio steganography:

'X' represents ciphered data

'W' represents wave signal

'Y' represents wave sound stegano-object

Then

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

The range of block of 'W' is decided at run time as per size of 'X'.

The approach that will be used here will be "interlevel approach".

3. SIMULATION RESULTS

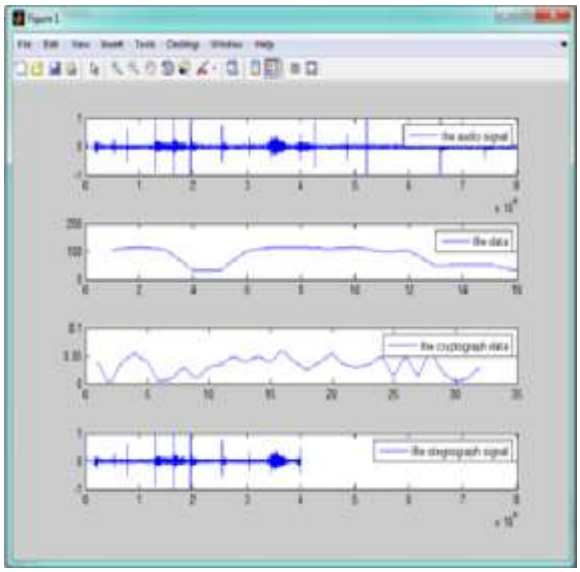

Figure 3: Simulation Results of proposed Audio steganographic signal

The figure 3 represents the data for wave_1.Similarly we have performed for the above wave as well as shown in the table.

Table 1:Result of proposed audio steganography

Audio File	Audio File Size (In KB)	(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

4. CONCLUSIONS

Information security is essential for confidential data transfer. Steganography is one of the ways used for secure transmission of confidential information. Proposed architecture for secure data transmission has achieved it original objective and the overall avalanche has been improved and the MSE has been reduced. 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] V. Saravanan, A. Neeraja, **Security Issues in** Computer **Networks and Stegnography**, Proceedings of7'h International Conference on Intelligent Systems and Control (ISCO 2013), 978-1-4673-4603-0/12,2012 IEEE.

[2] Imran SarwarBajwa, RubataRiasat,**A New Perfect Hashing based Approach forSecure Stegnograph,** 978-1-4577-1539-6/11, 2011 IEEE

[3] 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

[4] ZaidoonKh. 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

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

[6] 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

[7] 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