ANALYSIS OF COMBINED IMAGE STEGANOGRAPHY AND CRYPTOGRAPHY TECHNIQUES

Rashmi Naveen
Dept of Information Science & Engineering, NMAM Institute of Technology, Nitte-574110
rashmin@nitte.edu.in

Abstract

As real time applications in today's century, makes use of digital data, security of this data becomes important and essential. Different aspects to be considered while dealing with such digital data are preserving authenticity, make sure that data is not modified in transit and no one else other than intended user can read this data. To fulfil these requirements, many techniques are available to protect this data. Cryptography is to jumble the original information so that unauthorized person can't see it and that of steganography is to hide the original information. These techniques have their respective pros and cons. The main intention of the presented technique is to re-conciliate cryptography with steganography and give better protection.

Index Terms— AES, Blowfish, Random padding, RDH.

I. INTRODUCTION

An innovative technique used in multimedia information management and transfer plays a very important role in today's era. The goal of Communication is that the information should not be revealed and the existence should be hidden as well [1]. Steganography [2] is a Greek word specifies steganos means covered and graphy means writing. Steganography is described as the camouflaging the information within the other object viz text, image, audio, video etc. Cryptography described as an encryption technique in which the message is disorganized into some particular form so that third party other than authorized user cannot read and process it. Encryption is the process of converting original contents to cipher contents and Decryption is the reverse of it. Steganography in image exploits the weakness of the human visual system (HVS) while steganography in audio [3] relies on the imperfection of the human auditory system (HAS). But every object has pros and cons associated with it. Many cryptanalytic attacks are present today which can recovers the plain text from cipher text [4] as well as many stego-techniques are easily discernible. Extra security can be provided by unifying these two techniques. In this case, even if intruder identifies the existence of message within an object, the message is unreadable as the message is in the encrypted form. Steganography is not a substitution for cryptography but rather add-on. Different cover objects used to conceal the confidential information are text, audio, images, video. Integrity, confidentiality and availability are the main objectives of any security algorithm.

The rapid development of information technology makes it easier to leak the information on the Internet, various intelligent terminals and portable storage devices, and the leakage might have a great influence on the safety for individuals, enterprises and the state. Owing to these information security issues, how to deal with these challenges becomes an important problem.

In the Random based approach for secure communication [4], secret data (text, image or audio file) is encrypted using SHA-1 algorithm and then embedded the encrypted data in an audio file using random based approach. In this technique, the measured speech has seen some sort of distortion when compared with the original sound.

In the Audio steganography with the embedded text [5], confidential information is encrypted with the RC4 algorithm and embedding is done using LSB approach of audio steganography. In this method, destruction of data has been observed. Also the process of extraction is easy as the least significant bit has been used for embedding.

In the proposed algorithm, the destruction of data is reduced which is observable by calculating the PSNR values. And more complex algorithm than the LSB is used so that it becomes difficult to extract the data.

The intention of this paper is to combine multiple mitigating security controls along with the better imperceptibility level [6]. The paper is organized as follows:

Second section gives the detailed description of the Existing Techniques, third section defines the Methodology, fourth section briefs about Result and Analysis, and fifth section illustrates the Conclusion.

II. EXISTING TECHNIQUES

A. Cryptography

Cryptography is the study of mathematical methods regarding information or data security such as secrecy, entity authentication, integrity of data and message's original authentication [3]. The main objective is to make information impossible to read by an eavesdropper. Cryptographic algorithms are divided into symmetric and asymmetric network cryptographies [3]. Symmetric algorithms are used to convert the plaintext to cipher text and cipher text to original messages (plaintext) by using the same secret key. While Asymmetric algorithms uses public-key to exchange key and then uses the secret key algorithms to ensure secrecy of stream of data [3]. In asymmetric cryptography, there is are two kinds of keys, one key is public-key which is known to public, and is used to encrypt data to be sent by the sender to a receiver who owns the respective secret-key. In order for transmission to occur, secret and public keys are both different and they need to be exchanged between the sender and the receiver.

B. Steganography

Steganography is derived from Greek language which means "secrecy writing" [4]. The main objective of steganography is to send sensitive information under the cover of a carrier signal. It is generally known that any steganographic method must have these two properties: good imperceptibility and enough data capacity [5]. The property ensures that the secret messages that are embedded are difficult to discover, and the second implies effective secret communication. Even though Steganography and cryptography both aim at security, but they are different. The goal of cryptography is to communicate securely by changing the data into an unreadable form that an intruder cannot understand

III. METHODOLOGY

The proposed technique provides the security in two ways, first using symmetric cryptography and second using image steganography. The work is divided into four steps, two steps at sender and two steps at receiver. Encryption of plain text to cipher text and embedding cipher text into selected image is done at sender side while extraction of cipher text from stego-image and decryption of cipher text to obtain original text is carried out at receiver end. Mentioned encryption techniques convert the plain text into a cipher text, after which the cipher is embedded into the cover file to hide its presence.

In the traditional Reversible data hiding (RDH) technique, the message is embedded in the encrypted image. First the compressible features of original cover are extracted and again compression carried out to save spare space for embedding secret data.

In the proposed work, the confidential text will be encrypted with the AES & Blowfish encryption and the key, which will be used for decryption. Resultant cipher text will be inserted into the cover object with steganography using RDH algorithm & random padding. The image will be inserted chosen by the user. Stego object will be transmitted over the network. Stego object received by the user will be processed to get cipher text. Using key, cipher text will be decrypted to obtain the original text.

The proposed algorithm first converts the secrete message into cipher using one of the mentioned algorithm AES or Blowfish. Two image steganography algorithms are analyzed on the respective cipher text- reversible data hiding and random padding. Reverse procedure is applied at the receiver end.

Random padding is a technique in which the image is converted in to flat array of pixels and the text is hidden in between them. We have made use of python for the implementation of steganography.

In the reversible data hiding, Integer transform technique is used to hide the cipher text into an image.

IV. RESULT & ANALYSIS

A. Results

In the proposed work, RDH and Random Padding methods for image steganography are used with the AES and Blowfish cryptography. For the presented readings, the key length is taken as 128-bits for AES encryption and Blowfish encryption. An experiment is done for the four image files of different size.

a. Original Image

b. Stego Image

Fig 1: Result of AES Cryptography and RDH Techniuqe

B. Performance Analysis

In this paper, implementation of AES and Blowfish cryptography with RDH & Random Padding method of image steganography is carried out.

PSNR

PSNR is calculated for two files viz original audio and stego-audio (distorted) as follows-

1. Read two files in variables (Lets say A & B)
2. Get the diff. of variables as follow

if A ==B -> display message that "Two file is identical" and PSNR = inf otherwise get diff of two vector as diff = A-B;

3. Use PSNR formula 10*log10 (max (original_sig/ variable which store original sig)/ (sqrt (mean (mean (diff^2)))));

10* log10 ensures that o/p is in dB

Table 1 and Table 2 show the result of analysis, by working with PSNR, for the proposed technique with AES and Blowfish encryption respectively. It is noticed that the quality of Stego-image is depends on the block size and the key size used in respective encryption algorithms.

Table 1: PSNR Analysis with AES

Image	Random Padding Algorithm	RDH Algorithm
Tulip (Color 1024X768)	49.39	72.99
Monalisa (Color 230X216)	49.39	61.87
Lena Soderberg (Gray 512X512)	49.38	52.21
William Shakespeare (Gray 512X512)	49.38	51.50

Table 1: PSNR Analysis with Blowfish

Image	Random Padding Algorithm	RDH Algorithm
Tulip (Color 1024X768)	54.36	75.86
Monalisa (Color 230X216)	54.35	63.74
Lena Soderberg (Gray 512X512)	54.34	58.38
William Shakespeare (Gray 512X512)	54.33	59.50

V. CONCLUSION

Today, Steganography is not implemented in wider ways but it can be used as the best security tool. The main problem of today’s world is to secure their confidential information; the techniques used at present are either cryptography or steganography, are not efficient to secure this information. Proposed analysis highlights the use of cryptography with steganography by providing multilevel security to the confidential data. Analysis of Random

Padding and RDH algorithms with dual security model is observed. The proposed algorithm gives better results for color images in dual-level security.

VI. NOTE

This paper is a revised and expanded version of a paper entitled 'An improved method for reversible data hiding steganography combined with cryptography', 2018 2nd IEEE International Conference on Inventive Systems and Control(ICISC),*Coimbatore,2018.*

REFERENCES

[1] P. Joseph and S. Vishnukumar, "A study on steganographic techniques,"*2015 Global IEEE Conference on Communication Technologies (GCCT)*, Thuckalay, 2015, pp.206-210. doi: 10.1109/GCCT.2015.7342653

[2] Teck Jian, Chua & Chuah, Chai Wen & Hidayah Binti Ab. Rahman, Nurul & A Hamid, isredza rahmi. (2017). Audio Steganography with Embedded Text. IOP Conference Series: Materials Science and Engineering. 226. 012084. 10.1088/1757-899X/226/1/012084.

[3] Vishnu S Babu, Prof. Helen K J, "A Study on combined Cryptography and Steganography",International Journal of Research Studies in Computer Science and Engineering, Vol 2, Issue 5, May 2015, ISSN 2349-4859

[4] Sara Khosravi, Mashallah Abbasi Dezfoli, Mohammad Hossein Yektaie, "A new steganography method based HIOP (Higher Intensity Of Pixel)algorithm and Strassen's matrix multiplication", Journal of Global Research in Computer Science, Vol. 2, No. 1, 2011

[5] Priya Thomas, "Literature Survey on Modern Image Steganographic Techniques", International Journal of Engineering Research and Technology, Vol 2, Issue 5, May 2014, ISSN 2278-0181

[6] Ajit Singh, Swati Malik, "Securing Data by Cryptography with Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Isuue 5, May 2013, ISSN 2277-128x

[7] Ankit Gambhir, Sibaram Khara, "Integrating RSA cryptography & audio steganography", Computing Communication and Automation (ICCCA) 2016 IEEE International Conference on, pp. 481-484, 2016.