International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 12, December-2015

A Combined Approach of Steganography and Cryptography Techniques for Information Security: A Survey

Priyanka Haridas
M.Tech Scholar
Computer Science & Engineering
VNS Faculty of Engineering
Bhopal (M.P.) 462044

Gouri Shankar Prajapati
Assistant Professor
Computer Science & Engineering
VNS Faculty of Engineering
Bhopal (M.P.) 462044

***Abstract* - Cryptography is the practice and study of techniques for secure communication in the presence of third parties. Steganography is the art & science of hiding covert information in additional information and it can be defined as the study of unseen communication that classically deals with the ways of hiding the existence of the communicated message. In this paper, we present a survey of recently published Image Steganography techniques. This paper also provides a basic introduction to Cryptography and Steganography.**

Keywords: Cryptography, Steganography, Encryption, Least Significant Bit Insertion.

1. INTRODUCTION

In the present world of communication, one of the essential necessities to avoid data theft is securing the information. Safety measures have become a critical feature for thriving networks and in military alike. Cryptography and Steganography are renowned and broadly used techniques that operate information (messages) in order to cipher or hide their existence. These techniques have numerous applications in computer discipline and other related fields: they are used to protect military communication, E-mails, credit card information, business data, delicate files, etc.

2. BACKGROUND

2.1. CRYPTOGRAPHY:

Cryptography is the science of writing in covert code and is an ancient art. Cryptography is the science of devising methods that allow for information to be sent in a secure form in such a way that the only person able to retrieve this information who is the intended recipient. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes any network, mainly the Internet.[12]

In cryptographic terminology,

- A message being sent is known as Plaintext or Clear text.
- The process that scrambles information into unreadable or non-discernable form is called Encryption. An encrypted message is known as Cipher text.
- The method of restoring the jumbled information to its original form is called Decryption.
- A collection of algorithms and associated procedures for enciphering (or encrypting) and deciphering (or decrypting) information is known as Cryptosystem.
- The art of analyzing a cryptosystem that is to break it or to verify its integrity is the Cryptanalysis.
- The person or system that performs cryptanalysis is known as cryptanalyst.

The security of information encompasses the following aspects:

• Confidentiality or privacy,

• Data integrity,

• Authentication,

• Non-repudiation.

Confidentiality provides privacy for messages. Data Integrity provides assurance that a message remains unaffected from the moment it was created to the moment it was opened. Authentication provides two services: firstly, it identifies the origin of the message and secondly, it verifies the identity of a user logging into a system and continues to confirm their identity in case someone tries to break the system. Non-repudiation can provide a way of proving that the message came from someone even if they try to deny it.[12].

Types of Cryptographic Algorithms:

The modern field of cryptography can be divided into:

Symmetric key: Also known as single or secret key cryptography uses a single key both for encrypting and decrypting the plaintext

Asymmetric key: Too known as public key cryptography uses different keys for encrypting and decrypting the information

Hash values: Uses a mathematical transformation to irreversibly "encrypt" information.

2.2 Steganography:

Steganography is the art that involves communicating covert data in an appropriate multimedia carrier, e.g., image, audio, and video files. The word *Steganography* is resultant from the Greek words *Steganos* meaning "covered" and *graphy* meaning "writing or drawing". It is too known as 'Disappearing Cryptography' [13]. It includes a huge collection of methods of covert communications that conceal the very existence of the message. Among these methods are invisible inks, microdots, digital signatures, hidden channels and spread-spectrum communications.[14].

Steganography, is an ancient technique and has been widely used, including in recent historical times and the present day. Concealed messages within wax tablets, unobserved messages on messenger's body, Romans used invisible inks, which were based on natural substances such as fruit juice and milk. This was accomplished by heating the hidden text, thus revealing its contents etc are the examples of ancient methods of Steganography.

Modern Steganography refers to hiding information in a suitable multimedia carrier, e.g., image, audio, and video files. It works by replacing bits of unused data in normal digital files with bits of unseen information. To embed hidden information into an image requires two files - the envelop image file that will hold the concealed data and the secret message file.

Image Steganography:

In Image steganography, two files are necessary to hide a message inside an image file: the file containing the image into which the message is supposed to be put in, and the file containing the message itself. A message may be plain text, cipher text. When combined, the envelop image and the concealed message makes a stego image. A stego-key or password may be used to hide and decode the message.

There are three methods to hide messages in images, they are:

1. Least Significant Bit Insertion.

2. Filtering and Masking.

3. Algorithms and Transformations.

3. LITERATURE REVIEW

For studying the concepts of image steganography, we have surveyed many research papers. In this section we have described the relevant papers of different authors.

In paper [1] Ramesh Kumar, et.al uses bit plane method to hide data. A bit plane consists of bits corresponding to same significant level in all the elements. This method replaces the lowest 3 or 4 bits of the cover image to hide the data, hence, embedding data into the bit planes of the cover image. The message is encrypted before embedding in the cover file. A secret key is used for encryption, which is XOR with 2's complement of the message, hence results in encrypted text. An image is selected, which is converted into gray-scale. Numbers of bit-planes are selected and then the encrypted text is embedded into the selected planes of the cover file. Bitmap images are used to hide the data.

In paper [2], Ankita and Vishal introduces a new approach to substitute the LSB of RGB true color image. The proposed method, uses a secret key to hide information into cover image. The cover image is divided into three matrices (Red, Green and Blue) . The secret key is converted into 1D array of bit stream. Matrices are XORed with the secret key to find the position to hide the data. This 0process provides a new dimension for image steganography.

In paper[3] Garima proposed a scheme , combining asymmetric key cryptography with steganography. Secret data is encrypted using RSA encryption algorithm, the cipher is then converted into binary sequence bit and embedded into each cover pixels by modifying the least significant bits of cover pixels. In paper [6] Shailendra Gupta et.al also used RSA algorithm. They proposed a scheme using two popular techniques Rivest, Shamir, Adleman (RSA) algorithm and Diffie Hellman algorithm to encrypt the secret information. To provide higher security the secret information is encrypted first and encrypted ASCII value is converted in binary form. The image file used is tif. This paper also compares the results of embedding data in last 1, 2, 3, and 4 bit of the cover image. While a method is introduced in paper [4] by Deepali, to hide the data in the image. The message is encrypted using RSA algorithm and embedded in the 1st least significant bit (LSB technique) and last four significant bits (Modulus four bit technique) of the pixel of image. MD5 hash algorithm is also used to provide the integrity.

In paper [5], Mr.Vikas Tyagi et.al, discussed a technique based on the LSB (Least Significant Bit) and a new encryption algorithm. Before hiding the data in an image the application firsts encrypts it. Symmetric key encryption is used to encrypt the data and then the encrypted data is embedded using least significant bit technique (matching pixel).

In paper[7], Ahmad T.Al-Taani and Abdullah M. Al-Issa, proposed a method for hiding information within the spatial domain of the gray-scale image. In this , the cover image is divided into blocks of equal sizes and depending on the number of ones in left four bits of the pixel, the message is embedded in the edge of the block.

In paper[8], B. Raja Rao et.al, proposed a system in which cryptography and steganography are used as integrated part along with newly developed enhanced security model. In cryptography, MD-5 Algorithm is used to encrypt a message and a part of message is hidden in DCT of an image, remaining part of the message is used to generate three (3) secret keys to make the system secure. While in the paper [9], Dipti Kapoor Sarmah and Neha Bajpai

introduces a system with the combination of cryptography and steganography using four(4) keys. AES Algorithm is used to encrypt a message and a part of the message is hidden in DCT of an image; remaining part of the message is used to generate two secret keys.

In paper[10], Ankita presents a model by combining cryptography and steganography techniques. In cryptography, Simplified Data Encryption Standard (S-DES) algorithm is used to encrypt the secret message and then alteration component method is used to hide encrypted message in the cover image.

In paper [11], Rajkumar Yadav used combination of cryptography and steganography to enhance embedding capacity of a steganographic channel by preprocessing the secret data and applying encryption technique over it and compress the data before sending it to receiver using gray level modification (GLM) technique. Matrix en coding technique is used for encryption of the data. The proposed work technique is limited to textual data only. Here the concept of Scrambled Letters, Dictionary Module is also used.

4. PROBLEM DEFINITION

In general, bitmap images (.bmp) are used widely as a carrier, to hide the data inside it. Bitmap images are used widely because of its large size; hence large amount of data can be hidden. But, due to its large size, it cannot be used on the internet.

The growing possibilities of modern communications require the use of secure means of protecting information throughout transmission against illegal access and use. Hacking is growing day by day and intruders can easily access important information . Hence we need better solutions which have good security level.

4.1 Problem Solution

The proposed technique is supposed to offer enhanced security while transferring the data or messages from one end to the other end. The objective of the project is to hide the message or a secret data into an PNG image which acts as a carrier file having covert information and to transmit to the destination securely. Hence, can be used on Internet.

The aim of the research is to hide the image over an image via least significant steganographic algorithm with modification contrast with cryptography using other image files rather than bitmap.

This work is to use other image files to hide the secret data in it.

5. CONCLUSION

The main intention of the work is to develop a steganographic application that provides good security. The proposed approach provides higher security and can protect the secret data from stego attacks. The image resolution doesn't change much and is minor when we insert the message into the image. We are using the Least Significant Bit algorithm in this work for developing the application which is faster and reliable and compression ratio is moderate compared to other algorithm.

There are number of methods in cryptography and steganography and are different from each other. Each method have some pros and cons in comparison with other methods. The Least Significant Bit Insertion Method of Image Steganography provides an easy way to embed the information in the images. It is a very easy method to embed, so, it is used widely. But, it is very easy to decode also. The proposed method will surely prevent it from steganalysis.

6. EXPECTED OUTCOMES:

Cryptography and Steganography are very ancient methods and till now are in use there are many various methods introduced in each. Also, there were many attacks done to extract the information by the hackers. Hence, to secure the information, this approach is seem to be very useful and also prevents the possibilities of steganalysis.

REFERENCES

[1] B.Ramesh Kumar, K.Suresh, S.K.Basheer, M. Raja Krishna Kumar, “Enhanced Approach to Steganography Using Bitplanes” , International Journal of Computer Science and Information Technologies, Vol. 3 (6), 2012,5472-5475, ISSN:0975-9646.

[2] Ankita Gangwar , Vishal shrivastava, “Improved RGB -LSB Steganography Using Secret Key “, International Journal of Computer Trends and Technology- volume4Issue2- 2013.

[3] Garima Tomar , “Effect of Noise on image steganography based on LSB insertion and RSA encryption”, IOSR Journal of Engineering Mar. 2012, Vol. 2(3) pp: 473-477

[4] Deepali , “Steganography With Data Integrity” , I nternational Journal Of Computational Engineering Research , Vol. 2, Issue. 7, Issn 2250-3005, November 2012 .

[5] Mr . Vikas Tyagi, Mr. Atul kumar , Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar, “Image Steganography Using Least Significant Bit With Cryptography” , Journal of Global Research in Computer ScienceVolume 3, No. 3, March 2012.

[6] Shailender Gupta, Ankur Goyal, Bharat Bhushan, “Information Hiding Using Least Significant Bit Steganography and Cryptography” , I.J.Modern Education and Computer Science, 2012.

[7] Ahmad T. Al-Taani and Abdullah M. AL-Issa, “A Novel Steganographic Method for Gray-Level Images” , World Academy of Science, Engineering and Technology 27 2009.

[8] B.Raja Rao, P.Anil Kumar, K Rama Mohana Rao, M.Nagu, “A Novel Information Security Scheme using Cryptic Steganography” , Indian Journal of Computer Science and Engineering Vol. 1 No. 4 327-332, ISSN : 0976-5166.

[9] Dipti Kapoor Sarmah , Neha Bajpai,” Proposed System for data hiding using Cryptography and Steganography”.

[10] Ankita Agarwal, “Security Enhancement Scheme for Image Steganography using S-DES Technique” , International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012.

[11] Rajkumar Yadav, “Information Security Using Blend of Steganography and Cryptography”, Int. J. Comp. Tech. Appl., Vol 2 (6), NOV-DEC 2011.

[12] Information,Theory, Coding and Cryptography Second Edition: Ranjan Bose.

[13] http://io.acad.athabascau.ca/~grizzlie/Comp607/menu.htm

[14] http://www.jjtc.com/stegdoc/sec201.html