A Survey on Crypto-Steganography

Shristi Mishra
MTECH scholar, CSE dept.
CSIT Durg
Chhattisgarh, India
shristimishra13@gmail.com

Ms.Prateeksha pandey
Asst. professor,CSE Dept.
CSIT Durg, India
Chhattisgarh, India
prateekshapandey@csit.in

Abstract— Cryptography and Steganography are two popular methods that are more widely used for sending information in secret way. The purpose of cryptography and steganography are same. Both are used to protect important information but in different way. Cryptography scrambles a message so that it cannot be understood and steganography hides the data so that it cannot be seen .Cryptography is not capable of hiding the presence of data alone and it cannot protect data effectively. Any eavesdropper can easily detect the presence of encrypted data and can try several attacks in order to get the original data. This paper focuses on strength of combining cryptography and steganography (crypto-steganography) methods. This paper also describes the basic concept of cryptography and steganography.

Keywords*- cryptography, steganography, AES, DES, LSB.*

*****

I INTRODUCTION

Cryptography is an art and science of storing and transmitting over insecure medium like internet by encoding a data in to non readable format and intended user will be able to convert it in to original form. The word cryptography is derived from crypto (secret) and Graphy (writing).So cryptography means secret writing. It involves two basic functions that are encryption and decryption. Encryption is the process of converting plain text (original message) into cipher text (scrambled message). Decryption is the reverse process of encryption. Cryptography is basically used to hide the original data into a coded data so that unauthorized access can be prevented.

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. The various goals of cryptography are:

- Authentication*:* The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity
- Confidentiality*:* Ensuring that no one can read the message except intended receiver.
- Integrity*:* Assuring the receiver that the received message has not been changed in any way from the original.
- Non-repudiation*:* A mechanism to prove that the sender really sent the message.

Cryptography can be broadly classified in to three categories:

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption.
- Hash Functions: Hash function have no key since plain text is not recoverable from the cipher text.

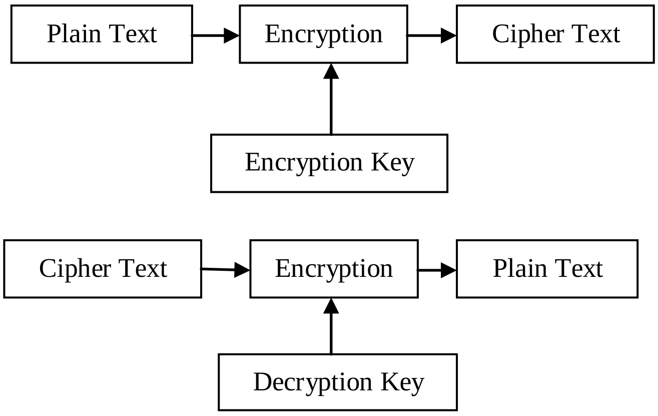

Fig 1: Basic Model of cryptography

Steganography is the art of hiding a message, image, or file within another message, image, or file. The word Steganography comes from Greek word Steganos (covered) and Graphy (writing).Therefore steganography means covered writing. The objective of steganography is to hide a secret message within a cover-media in such a way that in such a way that others cannot detect the presence of the hidden message.

Different types of steganography are:

- Text Steganography: The method of hiding secret information in a text is known as text steganography.
- Image steganography: The image steganography is the process in which we hide the data within an image.
- Audio steganography: The method of hiding secret information in an audio is known as audio steganography.
- Video steganography: The method of hiding secret steganography

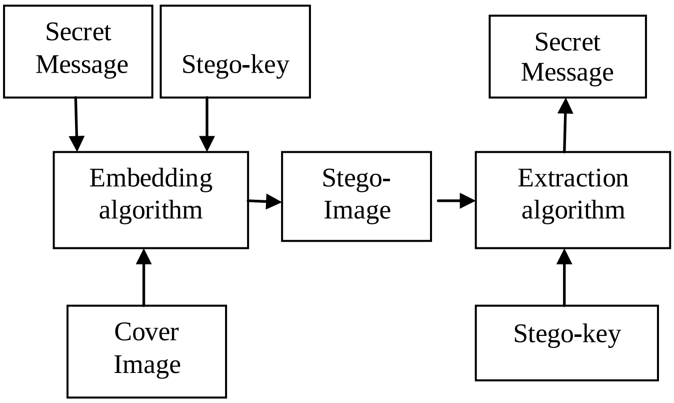

Fig 2 Basic model of Steganography

Cryptography	Steganography
Cryptography means secret writing.	Steganography means covered writing.
It is method of storing and transmitting data in particular form so that only those for whom it is intended can read and process it.	Steganography is the art of hiding message, image , file within another message, image, file.
The goal of a secure cryptographic is to prevent an interceptor from gaining an information about the plain text from the intercepted cipher text.	The goal of steganography is to hide a message.
Known message passing	Unknown message passing
Cryptography alter the structure of message.	Steganography does not alter the structure of secret message.
Most of the algorithm known by all.	Technology still being developed for certain format

Table 1 Comparison

Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Steganography is the art of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it can't be understood; the Steganography hides the message so it can't be seen. Even though both cryptography and steganography methods provide security, but combine cryptography and steganography in to one system for better security and confidentiality.

Some terms which are used in the context of cryptography and steganography.

- Plain text: original message.
- Cipher text: scrambled message.
- Key: It is used for encryption and decryption.
- Encryption: It is the process of transforming plain text in to cipher text.
- Decryption: It is the process of transforming cipher text into plain text.
- Cover-Image: Original image which is used as a carrier for hidden information.
- Stego-Image: After embedding a message in to cover image is known as stego-image.
- Stego-Key: A key is used for Embedding and extraction.
- Cryptanalysis: It is the study of analyzing information systems in order to study the hidden aspects of the systems.
- Steganalysis : It is the study of detecting messages hidden using steganography.

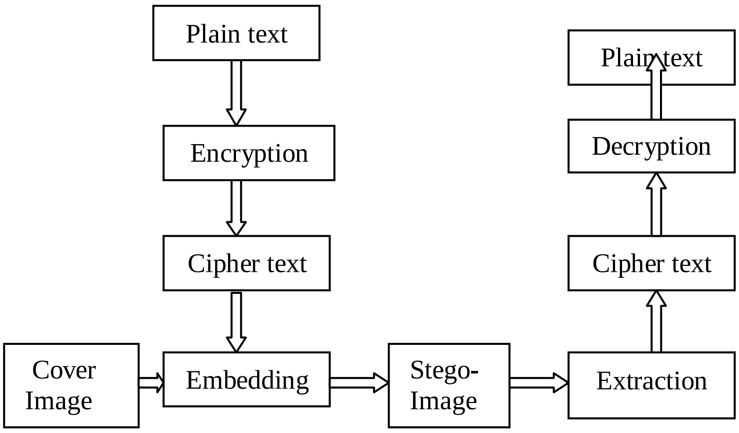

Fig 3 Combination of Cryptography and Steganography

II LITERATURE REVIEW

In paper [1], basic cryptographic concepts and techniques are defined.

In paper [2], various technologies used in image steganography are proposed.

In paper [3], author introduced the concept of embedding the secret message into an image using LSB technique and then applied AES to provide better security.

In paper [4], author introduced the method for embedding the secret image into cover image using LSB technique and then encrypts using DES algorithm and used the key image.

In paper [5], user selects plain text and encrypts using BLOWFISH Algorithm. This encrypted message is embedded into image using LSB technique.

In paper [6], A. Joseph Raphael introduces basic terminologies of cryptography and steganography.

In paper [7], data is encrypted by using AES and encrypted data is hidden into image using LSB technique.

III METHODOLOGY

Cryptography Methods:

There are several ways of classifying cryptographic algorithm. They will be categorized based on the number of keys that are employed for encryption and decryption.

- Symmetric cryptography: a single key is used for both encryption and decryption
  Symmetric cryptography are

Data Encryption Standard (DES):The DES is common standard for data encryption and a form of secret key cryptography, which uses only one key for both encryption and decryption. DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks.

Advanced Encryption standard (AES):AES is based on design principle known as substitution-permutation network which is a combination of both substitution and permutation. It is a symmetric block cipher that can process data blocks of 128 bits, using cipher keys length of 128, 192, and 256 bits. AES is more secure than other algorithm. The input, the output and the cipher key for Rijndael are each bit sequences containing 128, 192 or 256 bits with the constraint that the input and output sequences have the same length. In general the length of the input and output sequences can be any of the three allowed values but for the Advanced Encryption Standard (AES) the only length allowed is 128.[7]

1. Blowfish Algorithm:

It is designed in 1993 by Bruce Scheier. It is based on Feistel network. Blowfish has a variable-length key and 64-bit block cipher. The algorithm has two parts: a key-expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of key-dependent permutation, and a data-dependent substitution. All operations are XORs and additions on 32-bit words [5].

- Asymmetric Cryptography: sender encrypts with one key and receiver decrypts with another key. Asymmetric cryptography are:

1. Digital Signature Algorithm: It was developed by the United States government for digital signatures. Digital Signature Algorithm can be used only for signing data and it cannot be used for encryption. The DSA signing process is performed through a series of calculations based on a selected prime number. Although intended to have a maximum key size of 1,024 bits, longer key sizes are now supported.
2. **Rivest Shamir Adleman (RSA): Ron Rivest, Adi Shamir, and Len Adleman released the Rivest-Shamir-Adleman (RSA) public key algorithm in 1978. This algorithm can be used for encrypting and signing data. The encryption and signing processes are performed through a series of modular multiplications.**

Steganography Techniques:

Image steganography techniques can be divided into following domains.

- Spatial domain techniques: There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values. Changes in the value of the LSB are imperceptible for human eyes [2].

- Transform domain Techniques: This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it[2]. Transform domain techniques are broadly classified into :
  1. Discrete Fourier Transform (DFT),
  2. Discrete Cosine Transform(DCT),
  3. Discrete Wavelet Transform(DWT).

V CONCLUSION

This paper gives a brief review on cryptography and steganography techniques. Cryptography and steganography are the two popular methods available to provide security. One hides the existence of the message and the other distorts the message itself .Even though both cryptography and steganography methods provide security, but combination of these two methods will enhance the security.

REFERENCES

[1] Venkata Sai Manoj, "Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 1 – No.12.

[2] Mehdi Hussain, Mureed Hussain, "A Survey of Image Steganography Technique", International Journal of Advanced Science and Technology, Vol. 54, 2013, pp. 113-124.

[3] Dr. R. Sridevi, Vijaya Lakshmi Paruchuri, K.S. Sadasiva Rao, "Image Steganography combined with Cryptography",
International Journal of Computers & Technology ISSN: 22773061, Vol.9, July 2013, pp. 976-984.

[4] R.Nivedhitha, Dr.T.Meyyappan, "Image Security using Steganography and Cryptographic Techniques", International Journal of Engineering Trends and Technology, ISSN: 2231-5381, Vol.7, 2012, pp. 366-371.

[5] Ajit Singh, Swati Malik, "Securing Data by using Cryptography with Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 3(5), May 2013, pp. 404-409 .

[6] A. Joseph Raphael, Dr. V. Sundaram, "Cryptography and Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630

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

[8] Cryptography and Network Security Principles and Practices, 4th edition by William Stallings.