Study of Cryptography and Steganography System

Md. Khalid Imam Rahmani[1],Mr.Amit Kumar Goyal[2] Manisha Mudgal[3]

[1,2]Associate Professor, Deptt. Of Computer Sc. & Engg.
Echelon Institute of Technology
Faridabad, INDIA.
kirahmani@rediffmail.com, goelkamit@rediffmail.com
[2]M.Tech. Scholar, Deptt. of Computer Sc. & Engg.
Echelon Institute of Technology
Faridabad, INDIA.
mudgal.05.manisha@gmail.com

Abstract—Transmission of data through internet has become very common now a days so, it is important to have secure communication over internet. Cryptography and Steganography are two important methods for providing secure communication. Cryptography converts the message into some gibberish form and Steganography hides the message into some other media file that can be text, image, audio, video etc. In this paper we have explained the concept of cryptography and steganography and have compared them .It also focuses on how combination of cryptography and steganography enhances security
.

Keywords: Cryptoanalysis, Stegano object,cipher text,carrier object .

I. INTRODUCTION

To manipulate or hide the existence of a message, cryptography and steganography are two best techniques. Cryptography scrambles the message so that the message cannot be understood. And steganography hides the existence of the message so that the message is not visible. And combination of both Cryptography and steganography makes the communication more confidential and secure.

Cryptography and Steganography differ in the way they are evaluated. Steganography fails when attacker comes to know the presence of cipher text in Stegano Object. Cryptography fails when attacker cracks the cipher text to get plain text.

The studies that attack the encrypted message and detect the hidden messages are called as Cryptanalysis and Steganalysis. So, we should apply those algorithms that are hard to crack.

II. CRYPTOGRAPHY

Cryptography is the method of secure transmission of data by converting the text into some disgusted form so that only the intended user can remove that disgust and can read the original secret message.
Cryptography has followed man through many stages of evolution. Julius Caesar in his era used normal alphabet substitution method for government communication. Today cryptography has reached a new level and now we also have quantum cryptography. Quantum cryptography combines cryptography and physics to produce a new cryptosystem that cannot be defeated without the sender and receiver.

Some terminologies used in Cryptography are:-

Plaintext: - It is the original text message.

Encryption: - It is the process of encoding the contents of original message so that attacker or any outsider does not understand the real message.
Decryption: - The process of retrieving backs the original message.
Hash Functions: - They generate the digest of the message.
Cipher Text: - The encoded text is called the ciphertext.

In Cryptography there are three distinct mechanisms: -

Symmetric key encipherment (also called as secret key cryptography) in this same key is used both for encryption and decryption.
Asymmetric key encipherment (also called as public key cryptography) in this there are two different keys on is used for encryption and other is used for decryption.
Hash functions are much used for digital signature .For message authentication in many applications hash function has become the standard approach. The result of hash function is hash code.
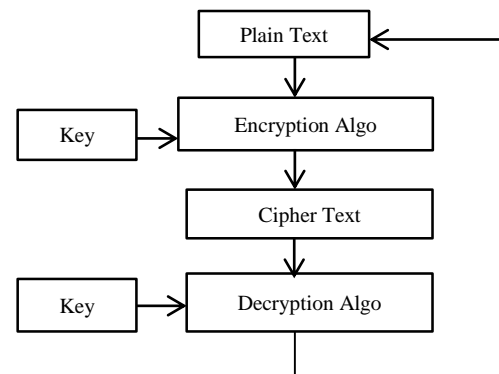

Fig. 1 Basic Encryption and Decryption Process of Cryptograph

III. STEGANOGRAPHY

The word steganography comes from the Greek which mean covered or secret and graphy means writing or drawing. Therefore, steganography is a "covered writing". The main goal of steganography is for secure communication and the data hidden should be undetectable.

The media that is used for covering can be Digital images, audio, videos, text files, and other computer files .These mediums are called Carrier Objects or Cover Objects.

After embedding a secret message into the cover-image, a so-called stegano image is obtained. The basic model of Steganography for embedding and extraction consists of Carrier Object, Secret Message, Embedding algorithm, Extraction algorithm and Stego key.
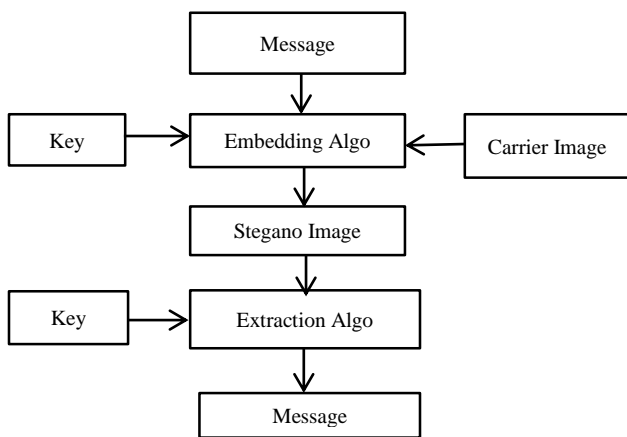

Fig.3 Basic Model of Steganography for Embedding and Extracting Message

IV. STEGANOGRAPHY VS CRYPTOGRAPHY

TABLE I COMPARISION BETWEEN STEGANOGRAPHY AND CRYPTOGRAPHY

Steganography	Cryptography
In this unknown message is passed.	In this known message is passed.
It does not alter the structure of the message.	It alters the structure of the message.
Key is optional.	Key is necessary.
Used to hide the message.	Used to encode the message.
Carrier can be any media file like Text, audio, image , video.	In this mostly text are used.
Attack on Stego Object is called Stegoanalysis.	Attack on Cipher Text is called Cryptoanalysis.
Output are Stegano File	Output are Cipher text

V. COMBINATION OF BOTH CRYPTOGRAPHY AND STEGANOGRAPHY

Cryptography encrypts the message and that helps in hiding the content of the message. So, after encryption the content of the message are not visible. This provides the security but attacker can crack the code and interpreted the message.
So, to add a new layer of security cryptography along with steganography is a best option. If an attacker found that stegano image has a message then also he will get an encrypted message not the original one. The combination of both makes the communication more secure and robust.

Algorithm of the combination technique:-

- Sender will provide the plain text and a key
- Then an algorithm is used for encryption of the message.
- Then this encrypted message or cipher text is embedded in an image with the help of some algorithm to produce a Stegano Image and key is option in this process.
- Then the Stegano image is transmitted for communication.
- Then the receiver will perform the reverse processes. Receiver will first extract the Cipher message form image using extraction algorithm.
- Then receiver will apply decryption algorithm and will provide key to decrypt the cipher text.
- The output will be the original plain text message.

VI. CONCLUSIONS

In this paper we have studied about Cryptography and Steganography and about their combination. Both Steganography and Cryptography provides security but combination of both provides multiple layer of security. First, we encrypt the message then that message is embedded into the image. This process enhances the security, capacity and robustness for secure combination.

REFERENCES

[1] A. Joseph Raphae.lDr. V. Sundaram, Head & Director, "Cryptography and Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630.

[2] Dr.R.Sridevi, Vijaya Lakshmi Paruchuri, K.S Sadasiva Rao, "Image Steganography combined with Cryptography", International Journal of Computers & Technology, Vol.9, July15, 2013.

[3] S.Ashwin, J.Ramesh, K.Gunavathi, "Novel and Secure Encoding and Hiding Techniques Using Image Steganography: A Survey", IEEE Xplore International Conference on Emerging Trends in Electrical Engineering and Energy Management, p.p 171-177, Dec 2012.

[4] D.Jacobs, Snehal Kamalapur, Neeta Sonawane, "Implementation of LSB Steganography and its Evaluation for Various Bits", IEEE Xplore International Conference on Digital Information Management, p.p. 173-178, Dec 2006.

[5] A.Joseph Raphael, Dr. V.Sundaram, "Cryptography and Steganography- A Survey, International Journal of Computer and .Technology Applications", Vol.2 (3), 2010.

[6] Rohit Kumar Gangwar1, Mukesh Kumar2, A.K.Jaiswal3 And Rohini Saxena,"Performance Analysis Of Image Compression Using Fuzzy Logic Algorithm",An International Journal (SIPIJ) Vol.5, No.2, April 2014.

[7] Dhawal Seth, L.Ramanathan, Abhishek Pandey, "Security Enhancement: Combining Cryptography and Steganography", International Journal of Computers Applications, 2010.

[8] M.Sitaram Prasad, S.Nagan janeyulu, Ch. Gopi Krishna, C. Nagaraju, "A Novel Information HidingTechnique for Security by Using Image Steganography", Journal of Theoretical and Applied Information Technology, 2005-2009.

[9] Wai Wai Zin, "Implementation and Analysis of Three Steganographic Approaches", IEEE Xplore International Conference on Computer Research and Development, p.p. 456-460, March 2011.

[10] Khalil Challita, Hikmat Farhat, "Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and Their Applications (IJNCAA), 2011.

[11] R.Nivedhitha, Dr.T.Meyyappan. "Image Security Using Steganography And Cryptographic Techniques", International Journal of Engineering Trends and Technology, Vol.7, 2012.

[12] N.V Rao, J.TL Philjon, "Metamorphic Crypto- A Paradox Between Cryptography and Steganography Using Dynamic Encryption", IEEE Xplore International Conference on Recent Trends in Information Technology, p.p. 217-222, June 2011.