RESEARCH ARTICLE OPEN ACCESS

A Study- To Combined Cryptography and Steganography Methods

Kavita Rawat, Mr. Shambhu Sah
Research Scholar, Department of Computer Science
Graphic Era Hill University
Uttarakhand – India

ABSTRACT

The Formalization of passing data from sender side to receiver side by a fixed way is been changed due to Information Highway or Internet and Communication Technology. Advancement is so much fast so the concern lies on security and integrity of data. Digital communication has become an essential part of advancement nowadays. Maximum services are internet based and it is very important that communication be made secret. Cryptography and Steganography are the two popular method available to provide security. One hides the existence of the message and the other distorts the message itself.

Keywords:- Cryptography, Steganography.

I. INTRODUCTION

Cryptography and Steganography are well known and widely used techniques that operate information in order to destroys the message itself or hide their existence respectively [2]. Cryptography jumble a message so it cannot be understood, the steganography hides the message so it cannot be seen. Even though they both techniques provide security as well as integrity, I am trying to combine both of them for better confidentiality and security.

History: Cryptography can be found as far back as 1900 B.C. in ancient Egyptian scribe using non-standard hieroglyphics in an inscription. From 50-6-B. C. Julius Caesar used a simple substitution with the normal alphabet in government communications [2]. Nowadays cryptography has touched a new level, quantum cryptography. Quantum cryptography is the combination of physics and cryptography to produce a new cryptosystem.

Steganography comes from the Greek stegano (covered or secret) and –graphy (writing or drawing). The first steganographic technique was developed in ancient Greece around 440 B.C. The Greek ruler Histaeus employed an early version of steganography which involved: Shaving the head of a slave, tattooing the message on the slaves scalp, waiting for the growth of hair to disclose the secret message, and sending he slave on his way to deliver the message, and sending the slave on his way to deliver the message. The recipient would have the slave's head to uncover the message. The recipient would reply in the same form of steganography.

Cryptography: Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, authentication, integrity of data. Cryptography is to make data unreadable by the intruder. Cryptography algorithm are divided into symmetric(secret key) and asymmetric(public key) network security protocols [2].

Cryptographic Technique: there are some important cryptographic techniques which I am trying to explain them into short terms.

a. DES technique: Data encryption standard is used to encrypt electronic data. It is symmetric key encryption technique which is used by IBM at first time. DES is used very small key with 56- bit. DES can be cracked using brute force attack[2].

b. AES algorithm for cryptography: Advanced encryption standard is same as DES in some ways like encrypt electronic data, using symmetric key etc.

but main difference is AES is used a symmetric block cipher that can process data blocks of 128- bits, using key size 128,192 and 256 bits[2].

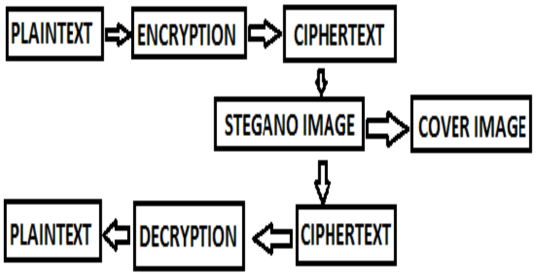
Steganography: Stegnography is the art of practice of concealing a file, message ,image, video with in another file, message, image, video [3]. The steganography technique takes a cover image secreat data and a key, embeds the secret data into the cover image and produce a steganography image. This steganography image is transferred to the receiver end and the secret message is extract by the recipient if he knows the key [2].

Steganography techniques: Stegnography is the art of hiding the cipher text with the image carrier. It does not replace cryptography but it can be used to improve the security of cryptography[2].

LSB- Steganography: in the least significant bit steganography[8] combine the text message in least significant bits of digital image. In which data is combine by replacing the LSB of cover carrier with the data to be send i.e. first read the cover image and text message which is to be hidden in the cover image [1].

Cryptography and Stegnography Combine Together: We are trying to provide the level of security to combining both methods using cryptography can distorts the message itself but it can not hide the message, steganography can hide the message. So here we have several combinations.

1. 1st Level Combination: The information or data from the sender is taken as the plaintext. Then plaintext converted into cipher text using any encryption method. The transformed cipher text can be used as the input for the steganography. The key of cryptography is kept secret then the cipher text is embedded into the cover medium using steganography techniques. The cover image is transmitted to the receiver.

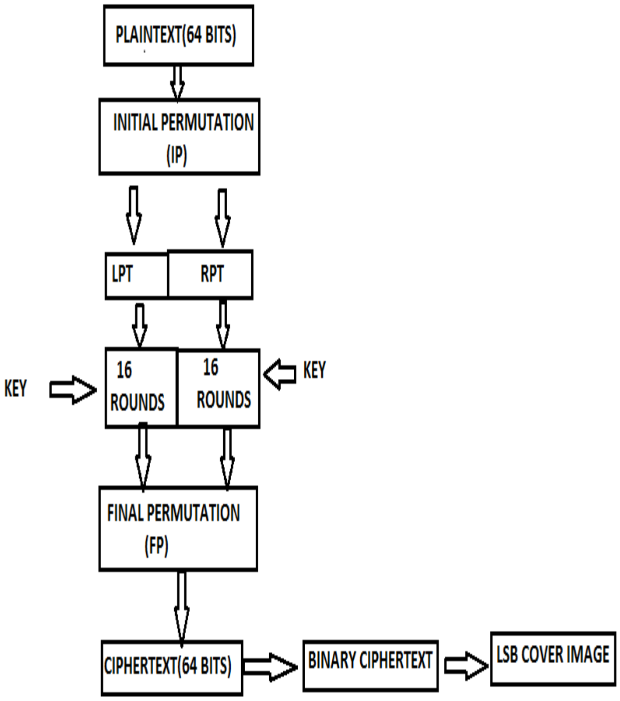


This is direct approach [1] in which both the methods are combined by encrypting message using cryptography and then hiding the message using steganography.

II. DES WITH LSB STEGANOGRAPHY

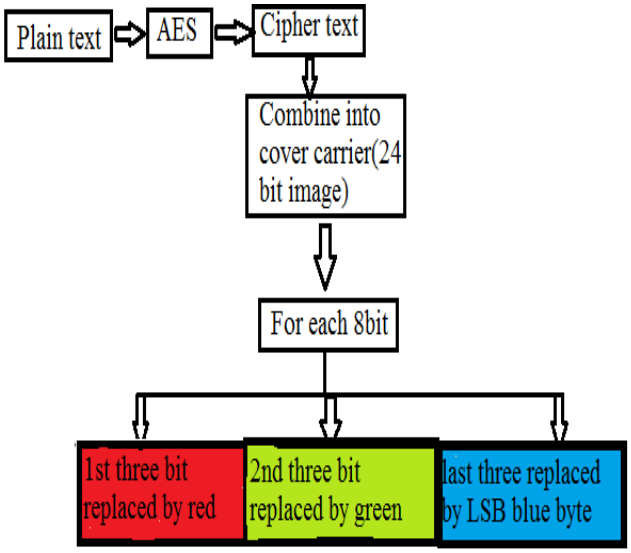
DES algorithm is used to encrypt the message to be transferred then the encrypted information i.e. cipher text is hide within a cover background. Here an image can be used as the cover background. The embedding process performed using LSB (Least significant bit) steganography.

First, the secret message is converted using DES cryptography thus we get cipher text. The cipher text is converted into binary. The LSB of cover image is replaced with the binary ciphertext then the image is transmitted to the receiver.



III. AES WITH LSB STEGANOGRAPHY

AES is used to encrypt the data to be transferred then cipher text is combine into a cover carrier. And 24 bit image can be used as cover carrier. The combining process performed using LSB steganography technique [2]. First the plain text is converted using AES cryptography thus we have cipher text. The cipher text is converted into binary. For each 8 bit data, the first three bits of the data are replaced by the three least significant bits of the red byte, the second three data bits are replaced by the three least significant bits of the green byte, the last two data bits are replaced by the two least significant bits of the blue byte[2]. Then the image is transmitted to the receiver.


Plain text
AES
Cipher text
Combine into cover carrier(24 bit image)
For each 8bit
1st three bit replaced by red
2nd three bit replaced by green
last three replaced by LSB blue byte

IV. CONCLUSION

Creyptography and Steganography are well known methods for providing security. To improve security we can use combined cryptography and steganography instead of using cryptography or steganography alone [2]. After an inconclusive comparison, it is difficult to certainly say that Steganography can be used as an alternate to Cryptography. In this paper we are trying to combined some cryptography methods and steganography methods.

REFERENCES

[1] Hardik kumar,V.desai(B.Sc. MCA), "Stegnography, Cryptography, Watermarking: A Comparative Study", Journal of Global Research in C.S.-Volume 3,no.12, dec2012 ISSN-2229-371X.

[2] A Joseph Rephael.Dr. V.Sundaram,"Cryptography And Stegnography- A Survey", Int J.Comp.Tech.Appl. Vol 2(3)626-630, ISSN:2229-6093.

[3] Vishnu S. Babu, Prof. Helen K. J.,"A Study on Combined Cryptography and Steganography" I.J.R.S.C.S.E, vol.2 5may2015, ISSN 2349-4840.

[4] R. Nivedhitha, Dr. Meyyappan, “Image Security Using Steganography And Cryptographyic Technique”, I.J.E.T.T., vol.3, issue3-2012

[5] Pranali R. Ekatpure, Rutuja N Benkar, “A Comparative Study of Steganography & Cryptography”, I.J.S.R. ,ISSN(online):2319-7064.

[6] McGraw Hill Education(india) pvt. Ltd., Atul Kahate,”Cryptography And Network Security”.