Steganography Techniques Using Cryptography-A Review Paper

Himanshi Sharma[1], Kamal Kumar Sharma[2], Sharad Chauhan[3]

[1]Student, M. Tech, ESEAR, Ambala
[2]Professor, Dept. of ECE, E-Max group of Institutions, Ambala
[3]Assistant Professor, Dept. of CSE, E-Max group of Institutions, Ambala

Abstract— **The two important aspects of security that deal with transmitting information or data over some medium like internet are cryptography and steganography. Cryptography results in converting plain text into cipher text which is in unreadable or in non-explanatory form, difficult to be guessed by eavesdropper, Steganography on the other hand hides the secret data into carrier medium in such a way that its detection is prevented. Steganography is not a replacement of cryptography but can supplement it to produce good results. It is observed that steganography and cryptography alone is not sufficient for information security, so we can make more secure and robust approach by combining the best of both techniques. This paper describes the various steganography techniques combined with cryptography.**

Keywords— **steganography, cryptography, least significant bit (LSB), encryption, decryption**

I. Introduction

The two important techniques for providing security are cryptography and steganography. Both are well known and widely used methods in information security. One of the reasons why attackers become successful in intrusion is that they have an opportunity to read and comprehend most of the information from the system. Intruders may reveal the information to others, misuse or modify the information, misrepresent them to an individual/ organisation or use them to plan even some more severe attacks. One of the solutions to this problem is through the use of cryptography and steganography.

Steganography is the art of hiding information in digital media through the techniques of embedding hidden messages in such a way that no one except the sender and the intended receiver can detect the existence of messages.

Cryptography is the art of transmitting the data safely over the Internet by applying some cryptographic algorithms so that it will be difficult for an attacker to attack or steal some confidential or private information.

II. CRYPTOGRAPHY

The process of converting plain text into unreadable cipher text is called cryptography. While for transferring the data from one place to another in secure manner various cryptography techniques are used depending upon the type of encryption algorithm used. The public key algorithm uses two different keys for communication while private key algorithm uses only one key for sending and receiving of the messages. The authentication, integrity, confidentiality and non repudiation of data should be maintained for successful transmission and reception of data. Data should be protected against eavesdropping, modification and fabrication etc. Cryptography is generally composed of sender, plain text, key, encryption algorithm, cipher text and recipient. Two basic process of cryptography are encryption and decryption as shown in Fig.1

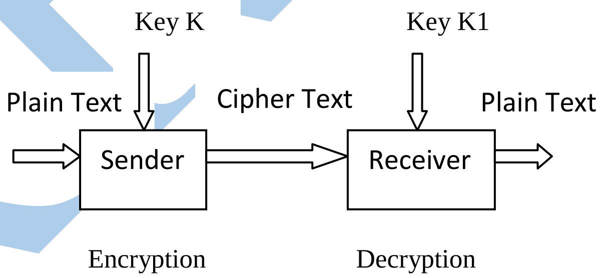

Fig 1: Basic Cryptography Model

Cryptography is normally classified on the basis of three parameters.

a) Encryption: - Encryption transforms original information, called plain text, into cipher text which usually has the appearance of unidentified, unintelligible data. Encrypted form of this transformed information is called the cryptogram.

b) Decryption:-The reverse process of transforming cipher text message back to plain text message is called as decryption.

c) Keys: - Cryptography uses public key or private key for encryption and decryption process. The sender and receiver should have same key for communication. Public key cryptography uses two different keys whereas in private key cryptography single key is used for communication.

III. STEGANOGRAPHY

Steganography is the process of hiding the secret messages or its existence so that it remains unidentified or undetected. The major advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of security. Steganography system generally composed of the carrier medium (image, audio, and video) which is used to hide the original data. It also contains the key for providing more security. The secret message is hided into cover or carrier medium which is then embedded with the help of key into stego file. Sender now can send this stego file to receiver. By performing extraction process who then extracts the original message with the help of key and stego file.

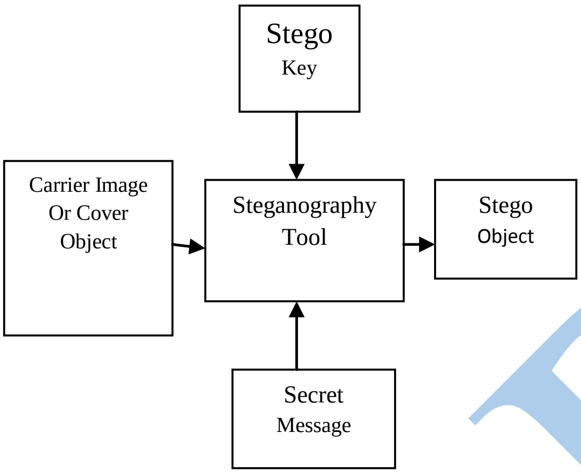

Fig 2: Basic Model of Steganography

A) Basic Types of Steganography:

i) Image Steganography:
For hiding the secret message into carrier image, this is then converted into stego image.

ii) Audio Steganography:
It alters audio files so that they contain hidden messages. The basic techniques are LSB manipulation and phase coding.

iii) Video Steganography:
It is the process of hiding some secret information inside a video.

IV. STEGOCRYPTO TECHNIQUES

To enhance the security level of information and to maintain secrecy and privacy of data steganography alone is not sufficient. It is used where cryptography is inefficient. Thus a new approach of security enhancement has been proposed by many researchers. It works by combining the cryptography and steganography and results in data security. The recent approaches of security generally composed of three main components

i) Encryption
ii) Steganography
iii) Decryption.

It works by first encrypting the secret data that needs to send after that applying the steganography technique such as image, video etc. then decrypting the stego files to get the original data. Following are some of the steganography approaches combined with cryptography.

A) AES Algorithm

This is the basic architecture of Stegocrypto technique. In this the secret message is first encrypted using AES algorithm, the key which is provided by user is hashed using SHA-1.This hashed key is again given to encryption module which generates cipher text using AES algorithm. Then the text generated by AES is given to steganography module, where this cipher text is embedded with one of the cover medium i.e. Image, audio or video as shown in figure below. This embedding is generally performed by Least Significant Bit Substitution Method which will hide the cipher text into cover medium , generated file is called as stego file. At receiver side this stego file is extracted, then by applying the decryption AES algorithm and decrypted hash key the plain text which is the original secret message is retrieved.

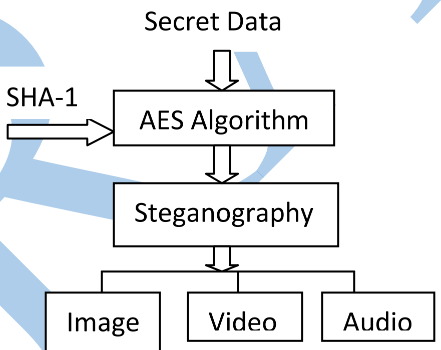

Fig 3: Steganography with use of AES Algorithm

B) Alteration Component

Several methods are implemented to encrypt the data before hiding it into cover medium. The alteration component method is same as the AES but message hiding technique is different. In the alteration method the secret message is first encrypted with AES algorithm then by applying the technique of alteration component the original message is hiding into cover medium and after applying the stego key stego file is generated. The alteration technique composed of three byte array such as pixel array, key array and character array. The key is converted into binary form and then filled into first array of first pixel. Then after key the secret message is filled into first component of next pixel as shown in figure 4. This technique work as follows first the extraction process is carried out with following steps

Step [i]: Extracting all the pixels from the image and storing it in the pixel array.

Step [ii]: Extracting all the characters from text file and store it in the character array.

Step [iii]: Extracting all the characters from the stego key and store them in key array.

Step[iv]: Then select the first pixel and choose the character from key array place it in the first component of the pixel, if more characters then place the remaining, terminate this array by placing terminate symbol.

Step[v]: Now select from the character array. These values are to be placed in the next pixel by using the same procedure.

Extraction process is basically reverse of this embedding process in which all the arrays are first extracted then key array extracted is verified. Then on comparing check if extracted key is matched with the receiver key then the next pixel values are extracted which is the original message or secret data.

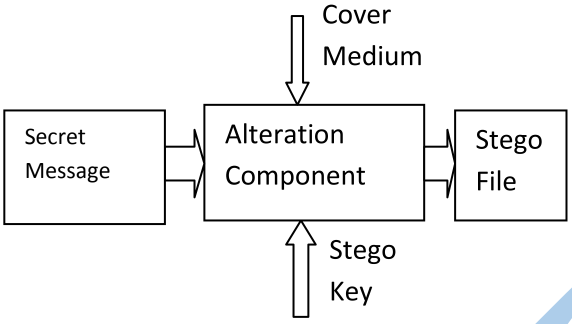

Fig 4: Technique of Alteration Component

C) Random Key Generation

This technique uses the random key generator device for providing the unique key when user log in. It generally consists of steganography tool which provides the user authentication with username and passwords, and key. Key generator device can generate unique keys after a fixed interval of time. This method is very useful for public place message sharing.

D) Distortion Process

This method proposes one more security module in between the cryptography and steganography. This module is responsible for generating two keys and provides extra security by modifying the cipher text and generating the two keys. (i) Before the steganography hiding process this process separates digits and the alphabets from the cipher text and stores the position of this into Key 1. (ii) Key 2 is obtained by separating the first seven alphabets and digits and adding remaining alphabets at the end of digits. (iii) Then the hiding is done by taking the seven alphabets applying the 64 bit key then finding the DCT of the gray scale image while hiding the seven alphabets with inverse DCT.

As a result the stego file is generated and retrieving is done by following opposite procedure as taking DCT coefficient and then retrieving the seven alphabets and rearranging the distorted alphabets using key. Then by applying the key1 and key2 cipher text is retrieved and reverse AES is applied to get the original message.

E) Key Based Security Algorithm

This algorithm is same as the AES technique with some difference. In this before encryption, the secret message is first compressed then after applying the algorithm and encryption key it is given to steganography module where actual embedding is done by hiding it in the cover media and applying stego key as shown in the Fig.5. The extraction process is exactly opposite of this where extraction is done with stego key after which with the help of key decryption of message is done, which on decompression gives the original message.

V. CONCLUSION

In this paper, we presented various steganography techniques which in combination with cryptography, results in increasing the security level of data or information. Steganography usually not designed to replace the cryptography but it helps in creating more secure communication after combining with cryptography by using best of both techniques. Thus it is proved that using cryptography techniques which use compression, hash function, automatic key generation, distortion process etc., the data becomes more secure and robust as compared to steganography technique alone. Thus the encryption of secret message and then hiding results in more secured approach.

REFERENCES

[1] Md. Khalid Imam Rahmani, Kamiya Arora , Naina Pal," A Crypto-Steganography: A Survey", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 5, No. 7,2014

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

[3] Dipti Kapoor Sarmah, Neha Bajpai, "Proposed System for Data Hiding using Cryptography and Steganography", Technical report, pp.483-490.

[4] Vipula M. Wajgade, Dr. Suresh Kumar," Stegocrypto- A Review of Steganography Techniques using Cryptography" International Journal of Computer Science & Engineering technology (IJCSET)