Stegocrypto - A Review Of Steganography Techniques Using Cryptography

[1]Vipula Madhukar Wajgade
MTech(CSE) IInd Year
SGT Institute of Technology And Management
Gurgaon, Haryana, India
Email Id: vips.wajgade@gmail.com
Contact No. +918130374991

[2]Dr.Suresh Kumar
HOD,Department Of Computer Science
SGT Institute of Technology And Management
Gurgaon, Haryana, India
Email Id: suresh.ahlawat@gmail.com

Abstract---The information security has become essential part of today's world due to extensive use of internet. The privacy of secret data can be achieved with two classical methods of data security namely Cryptography and Steganography.Cryptography results in scrambling of data into cipher text which is in unreadable or in nonexplainatory 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 alone is not sufficient for information security, so we can make more secure and robust approach by combining the best of steganography and cryptography. This paper describes the various steganographic techniques combined with cryptography.

Keywords-steganography;cryptography;LSB(Least Significant Bit);encryption;decryption

I. INTRODUCTION

Since ancient times secure communication and hiding the secret messages is being an area of interest, steganography is a Greek word which means hiding the secrets. In ancient time this secure communication was achieved into different ways such as using invisible ink, or wax for secret message sharing. Roman people used to tattoo the messages on shaved head, once the hair grew slave was sent to deliver secret messages. Chinese people used to write on silk material and then this material is crunched into wax which is then swallowed [1].On the other hand cryptography is not concerned with message hiding instead it deals with changing the meaning and appearance of message. Cryptography changes the plain text into cipher text by the process of encryption; it uses the mathematical techniques for securing the information. Cryptography uses various encryption algorithms such as public key cryptography, private key or symmetric and asymmetric algorithm. The process of converting secret message into cipher text is called as encryption whereas process of converting cipher text into original message is called decryption. Cryptanalysis is the reverse process of cryptography with the intention of finding original message.

II. CRYPTOGRAPHY

The process of transferring plaintext into unreadable cipher text is called cryptography. While for transferring the data from one place to another in secured manner various cryptographic techniques are used depending upon the type of encryption algorithm. The public key algorithm uses two keys for communication while private key algorithm uses only one key for sending and receiving of the messages. The integrity, authentication, confidentiality and non repudiation of data should be maintained for successful transmission and reception of data. Data should be protected against eavesdropping, modification, fabrication and alteration. Cryptography is generally composed of the sender, plaintext, key, encryption algorithm, ciphertext and receipient.Two basic process of cryptography are encryption and decryption as shown in Fig.1 and Fig.2

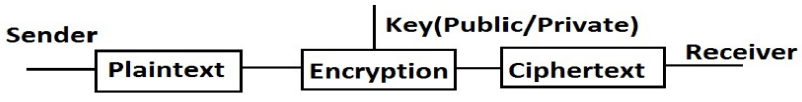

Fig 1: Process of Encryption (At Sender Side)

Cryptography is generally classified on the basis of three parameters.

a)Encryption :-The method used for transforming plaintext to cipher text, the way in which plaintext is converted into cipher text depends on the technique such as i) substitution cipher which is again classified into three main types Caesar cipher in which each character from plaintext is replaced by third letter in succession, substitution cipher involves substituting character by other characters,monoalphabetic cipher uses single character to replace whereas polyalphabetic uses multiple characters to replace. ii) Transposition cipher involves transforming block of characters into others resulting into rearrangement of the plaintext characters.

b) The number of keys used: - Cryptography uses public key or private key for encryption and decryption. The sender and receiver should have same key for communication to take place. Public key cryptography uses two different keys whereas in private key cryptography single key is used for communication.

c)Decryption :-The method used for transforming cipher text to plaintext, A stream cipher processes in continuous fashion one element a time, block cipher processes block of characters at a time [2].

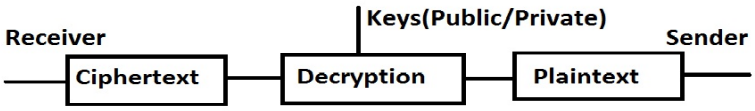

Fig 2: Process of Decryption (At Receiver Side)

III. STEGANOGRAPHY

Steganography is the process of hiding the secret messages or its existence so that it remains unidentified or undetected**.**The strong steganography should follow certain properties such as capacity-it should be capable of hiding information. Robust-it should be robust against the attacks and modifications.inperceptability-it should remain undetected from eavesdroppers. Steganography system composed of the carrier medium (image, audio, video) in which the original data is hided, 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 stegofile.Sender now can send this file to receiver, who extracts the original message with the help of key and stego file by performing extraction process. The basic steganographic system is as shown in Fig.3

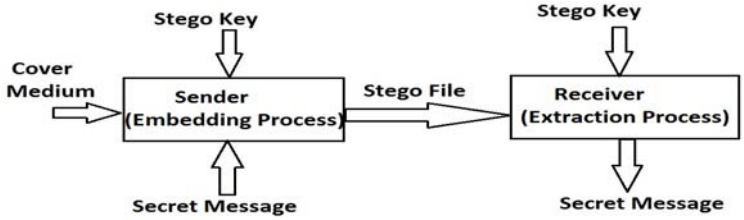

Fig 3: Basic Steganographic System

Three basic types of steganography system are as follows

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

ii) Audio Steganography:-The secret message is embedded into unused audio bits as every file contains some unused bits or unused area of bits where secret message can be hided.

iii) Video Steganography:-Video steganography divides the video into audio and image frames where embedding is performed in the audio file.

IV. STEGOCRYPTO TECHNIQUES- NEED TO COMBINE

To enhance the security level of information and to maintain secrecy and privacy of data steganography alone is not sufficient.Steganography is used where cryptography is inefficient. Thus a new approach of security enhancement has been proposed by many researchers. This approach works by combining the cryptography and steganography and results in data security. The recent approaches 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, audio, video then decrypting the stego file to get the original data. Following are some of the steganographic approaches combined with cryptography.

A. AES Algorithm

This is the basic architecture of Stegocrypto technique, where the secret message is first encrypted using AES algorithm, the key which is provided by user is hashed with SHA-1.This hashed key is again given to encryption module which generates cipher text using AES algorithm, the text generated by AES is now given to steganography module, where the cipher text is embedded with one of the cover medium i.e.Image, audio or video as shown in Fig.4. This embedding is generally performed by Lease Significant Bit Substitution Method which will hide the cipher text into cover medium, generated file is called as stego file. This stego file is extracted at receiver side, then by applying the decryption AES algorithm and decrypted hash key the plain text which is the original secret message is retrieved [3]

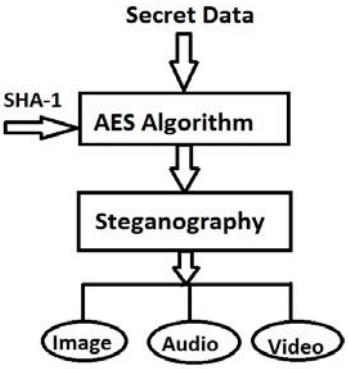

Fig.4 Steganography Using AES algorithm

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 hided into cover medium and after applying the stego key stego file is generated. The alteration technique composed of three byte array as key array, pixel array and character array. The key is converted into binary form and then filled into first array of first pixel, after key the secret message is filled into first component of next pixel as shown in Fig.5.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]:Selecting the first pixel and choosing the character from key array place it in the first component of pixel, if more characters then place the remaining, terminate this array by placing terminate symbol. Step[v]: Now select from the character array and place these values in the next pixel following the same procedure. Extraction process is the opposite of this embedding process where all the arrays are first extracted

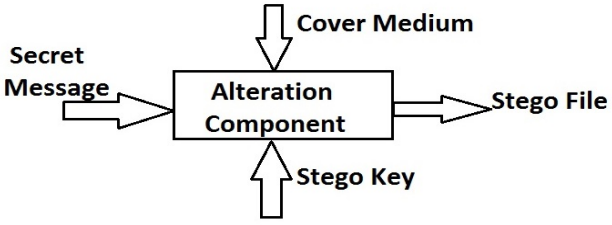

Fig.5. Alteration Component Technique

then key array extracted is verified if extracted key is matched with the receiver key the next pixel values are extracted which is the original message or secret data[4].

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 steganographic 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 [5].

D. Distortion Process

This method proposes one more security module in between the steganography and cryptography. This module is responsible for generating two keys. This intermediate module provides extra security by modifying the cipher text and generating the two keys. Before the steganographic hiding process this process separates digits and the alphabets from the cipher text and stores the position of this into Key 1.Key 2 is obtained by separating the first seven alphabets and digits and adding remaining alphabets at the end of digits. 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, the stego file is generated. Retrieving is done by following opposite procedure as taking DCT coefficient, 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 [6].

E. Key Based Security Algorithm

This algorithm is same as the AES technique with some difference. Before encrypting 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.6. The extraction process is exactly opposite of this where extraction is done with stego key after which decryption of message with key is done, which on decompression gives the original message[7].

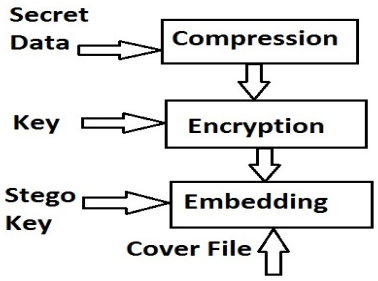

Fig.6. Key Based Steganography

F. Static Parsing

The static parsing method generally consists of two steps [i] Embedding the secret message and cover file and converting it into bits. [ii]In this step the common substring of image and secret message is found. If match is found the values of indexes are stored as the output [8].

V. CONCLUSION

In this paper, we presented various steganographic technique combined with cryptography, which results in increasing the security level of information or data. Steganography is not designed to replace the cryptography but it supplements the cryptography. Thus it is proved that using compression, hash function, static parsing, automatic key generation, distortion process etc. techniques, the data becomes more secure and robust as compared to steganography alone. Thus the encryption of secret message and then hiding results in more secured approach.

REFERENCES

[1] N.Johnson and S.Jajodia.Exploring Steganography:Seeing the Unseen.Computer,vol.31,no.2,pp.2634,1998.
[2] William Stallings,"Cryptography and Network Security:Principles and Practices:,Pearson education,Third Edition,ISBN 81-7808-902-5.
[3] Shery Elizabeth Thomas,Sumod Tom Philip,Sumaya Nazar,Ashams Mathew & Niya Joseph."Advanced Cryptographic Steganography Using Multimedia Files".International Conference on Electrical Engineering and Computer Science(ICEECS-2012),May 2012.
[4] Lokesh Kumar,"Novel security scheme for image steganography using cryptography technique",Procc.International journal of advanced research in computer science and software engineering.Vol.2,Issue 4,April 2012,pp.143-146.
[5] Mihir H Rajyaguru,"CRYSTOGRAPHY-combination of cryptography and steganography with rapidly changing keys".Vol.2,Issue 10,Oct. 2012,pp.329-332.
[6] Dipti Kapoor Sarmah,Neha Bajpai."Proposed System for Data Hiding using Cryptography and Steganography".
[7] H.Al-Barhmtoshy,E.Osman and M.Ezzaand."A Novel Security Model Combining Cryptography and Steganography".Technical report,pp.483-490.
[8] Khalil Challita and Hikmat Farhat."Combining Steganography and Cryptography:New Directions".International Journal on New Computer Architecture and Their Applications(IJNCAA),2011.