A REVIEW ON STEGANOGRAPHY TECHNIQUES USING CRYPTOGRAPHY

[1]Shristi Mishra, [2]Prateeksha Pandey

[1] Scholar, [2]Asst. Professor, Department of Computer Science Engineering,

C.S.I.T, Durg, Chhattisgarh (India)

ABSTRACT

Cryptography and steganography are widely used methods to provide data security. The motivation behind cryptography and steganography are same. Both are utilized to secure essential data however in distinctive way. Cryptography only hides the content of message not the existence of message and Steganography hides the existence of message .This paper introduces various methods where cryptography and steganography are combined to encrypt the data as well as to hide the data in image. It provides two levels of security to the information being transmitted. This paper also concentrates on strength of combining cryptography and steganography methods.

Keywords: Cryptography, Steganography, Advanced Encryption Standard (AES), Least Significant Bit (LSB).

I. INTRODUCTION

Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Cryptography is derived its name from Greek words cryptos and Graphy. Cryptography is the practice and study of hiding information. It is the art of converting a plain intelligible in to unintelligible data and again retransforming the data in to its original form. It involve two process- Encryption and Decryption. Encryption is the process of converting plain text into cipher text. Decryption is the reverse process of Encryption. Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. It provides confidentiality, Integrity. Cryptography can be categorized in to two types:

- Symmetric cryptography
- Asymmetric cryptography.

In Symmetric Cryptography, a single key is used for Encryption and Decryption. In Asymmetric Cryptography, one key is used for encryption and other key is used for decryption. Some terms which are used in context of Cryptography:

- Plain Text: Original Message
- Cipher Text: Encrypted message
- Encryption: It is the procedure of changing plain Text into Cipher Text.
- Decryption: It is the procedure of changing cipher text into plain text.
- Cryptanalysis: the study of analyzing information systems in order to study the hidden aspects of the systems.

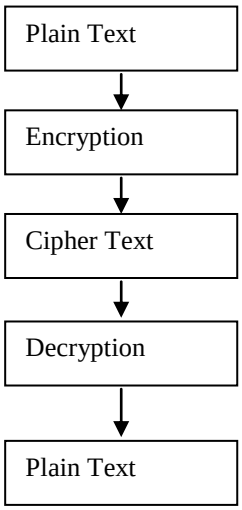

Fig 1 Basic Steps of Cryptography

Steganography is art of writing a hidden message so that only the intended user will be able to know the existence of the original message. It comes from Greek words Steganos and Graphy .Steganos means covered and Graphy means writing. So steganography means covered writing. The objective of steganography is to hide a secret message within a cover-media (Image, audio and video) in such a way that in such a way that others cannot detect the presence of the hidden message. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot detect the presence of the hidden message.

There are 4 ways to implement steganography:

- Using Text
- Using Images
- Using Audio
- Using Video

Some terms are used on context of Steganography

- Cover Image: Image which is used as a carrier for hidden Information.
- Embedding: It is process of hiding information in text, image, audio and video.
- Extraction: It is the reverse process of embedding.
- Stego-File: After embedding a message in to image, audio and video.
- Steganalysis: Study of detecting hidden message.

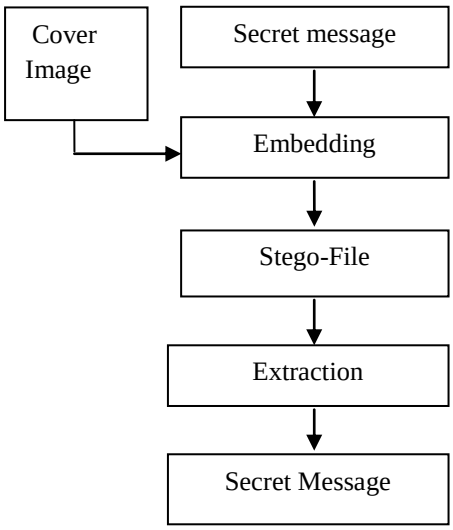

Fig 2. Basic Steps of Steganography

II LITERATURE REVIEW

In [1], A. Joseph Raphael introduces basic terminologies of cryptography and steganography and ensures that the combination of both will provide better security.

In [2], Dr. R. Sridevi, Vijaya Lakshmi Paruchuri, K. S Sadasiva Rao proposed the method of embedding the secret message into an image using LSB technique and then it is encrypted by AES algorithm for better security.

In [3], Mehdi Hussain, Mureed Hussain proposed various technologies which is used in image steganography.

In [4],Lokesh Kumar introduced the concept of encrypting the secret Message using AES and Alteration component technique is used to hide encrypted secret message into cover image

In [5], H.Al-Barhmtoshy,E.Osman and M.Ezzaand proposed a method of combining cryptography and steganography but here the secret message is first compressed then the message is hashed and encrypted using encryption key. Then Encrypted message is embedded in to cover media using stego key.

In [6], Dipti Kapoor Sarmah,Neha Bajpai have introduced a method.This method proposes one more security module between and steganography. This module is responsible for generating 2 keys

In [7], Manoj Ramaiya, Naveen Hemarajani and anil Kishore Saxena proposed the method of encrypting the secret message using AES algorithm and then it is embedded in to image using LSB technique.

III METHODOLOGY

Cryptography and steganography is not capable of hiding the presence of data alone. To enhance the security level of information and to maintain secrecy and privacy of data steganography alone is not sufficient..

Cryptography is used where steganography is inefficient Steganography is used where cryptography is efficient. Thus a new approach of security enhancement has been proposed by many researchers and it works by combining the cryptography and steganography and results in to more secure transmission of data. The recent approaches generally composed of four main components:

i) Encryption
ii) Embedding
iii) Extraction
iv) Decryption

This is the basic steps of combining cryptography and steganography, where secret message is first encrypted by using encryption algorithm, then it gives cipher text. Cipher text is embedded with other cover medium i.e text, image, audio and video.

1. AES and LSB

Secret message is encrypted by using AES algorithm, then it gives cipher Text. The text generated by AES is given to steganography module, where the cipher text is embedded in to cover File (Image , audio or video) .If it is embedded with image by using LSB, then it gives stego-Image. This stego-image is extracted at receiver side, then by applying AES algorithm on cipher text, receiver will get the plain text which is secret message.

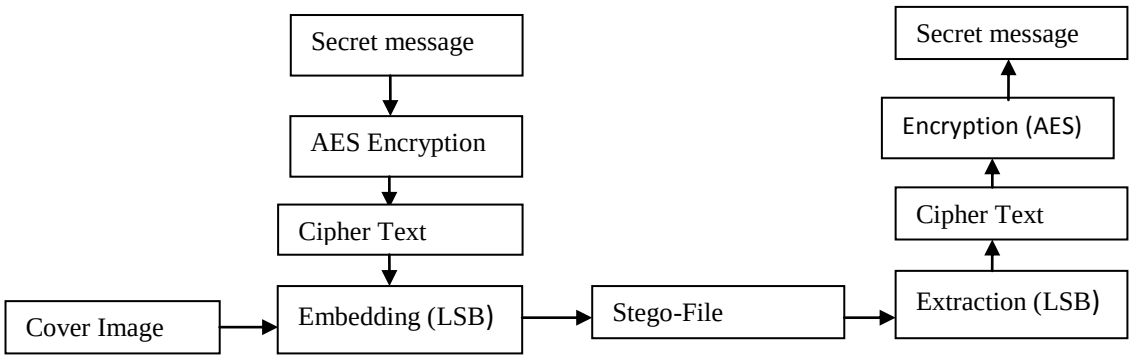

Fig 3: Cryptography using AES and Steganography using LSB

2. Alteration component

The secret information is encrypted by using AES encryption algorithm. Then encrypted message is embedded into cover image by using Alteration component technique and then after applying Stego-Key, Stego-Image is generated.Data is hidden by using Alteration component technique in which pixels have been replaced by key and secret message. Firstly 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. After then, secret message is converted into binary form and its binary form is filled in first component of next pixels.This stego-image is extracted at receiver side, then by applying AES algorithm on cipher text, receiver will get the plain text which is secret message.

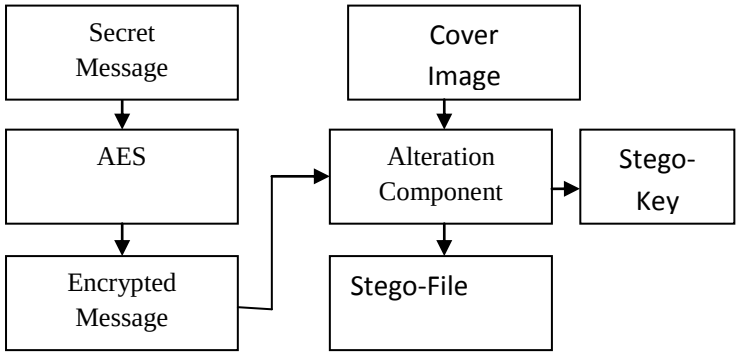

Fig 4: Steganography Using Alteration Component

3. Distortion Process

This is an intermediate module which provides extra security Firstly the process separates digits and alphabet from cipher text. And stores the original position of the alphabet and the digits in the form of a secret key (Key 1).second key(key2) is obtained by separating the first alphabet and add the remaining alphabets at the end of the separated digits. Then hiding is done by taking seven alphabets from the security Module and scramble the alphabets using a 64 bit key (Key 2) then after finding the DCT of gray scale Image while hiding the seven alphabets with inverse DCT, the stego file is generated. Retrieving is done by opposite procedure 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 then AES algorithm is applied to get the original message.

4. Key Based security algorithm

Secret message is first compressed and then after applying encryption algorithm and key given to steganography module where data is embedded in to cover media and apply stego-key. The extraction is just the reverse process of embedding process. Here extraction is done with stego-key and then after decryption of message with key is done, and then decompression gives the original message.

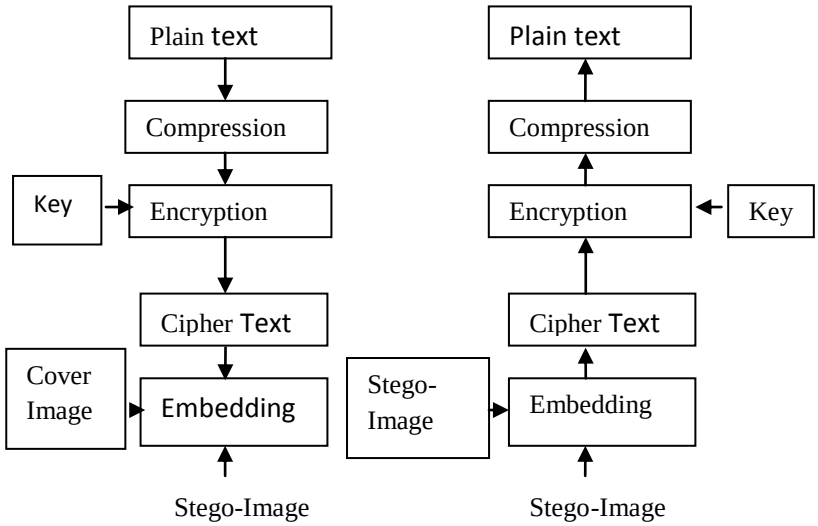

Fig. 5:Key Based Security

IV CONCLUSION

In this paper, we presented various steganography technique combined with cryptography technique, which results in to increasing the security level of information. Thus it is proved that the combination of cryptography and steganography(using AES and LSB, Alteration Component, Distortion Process and Key based security algorithm) gives better security, the data becomes more secure as compared to individually applying cryptography and steganography methods.

REFERENCES

[1] A Joseph Raphael and Dr. V Sundaram ,"*Cryptography and Steganography – A Survey*",International journal of computer technology and applications,2010.

[2] Dr.R.Sridevi, Vijaya Lakshmi Paruchuri, K.S.SadaSiva Rao, *Image Steganography combined with cryptography*,International Journal of Computers & Technology, 2013

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

[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] H.Al-Barhmtoshy,E.Osman and M.Ezzaand."*A Novel Security Model Combining Cryptography and Steganography*".Technical report,pp.483-490.

[6] Dipti Kapoor Sarmah, Neha Bajpai, "*Proposed System for data hiding using Cryptography and Steganography",* International journal of computer technology and applications,2010.

[7] Manoj Ramaiya, Naveen Hemarajani and anil Kishore Saxena, "*Secured steganography approach using AES*", International journal of computer science engineering and information Technology

Research(IJCSEITR),AUG 2013.

Biographical Notes

Ms. Shristi Mishra is presently pursuing M. Tech. final year in Computer Science and Engineering Department from C.S.I.T , Durg ,Chhattisgarh, India.

MsPrateeksha Pandey is working as a Assistant Professor in Computer Science and Engineering Department, C.S.I.T ,Durg , Chhattisgarh.