"A Review Of Hiding Technique To Developing A Secure System: Dual Steganography"

Babita[1], Gurjeet Kaur[2]

[1]M.Tech Scholar, Department of Computer Science &Engineering, S.B.B.S.U, Jalandhar, Punjab, India
[2]Assistant Professor, Department of Computer Science & Engineering, S.B.B.S.U, Jalandhar, Punjab, India

---***---

Abstract - ***With the rapid advance in digital network, information technology and digital communication has become very important to secure information transmission between the sender and receiver. Security is the important features in communication and other text information because of the intruders who wait for attack on data and chances to access the private information. There are two important type of techniques which provide securities are cryptography and steganography. Both are well-known and most important techniques which are used methods in information security for confidentiality of data exchange. One technique is cryptography, where the sender uses an encryption key to encrypt the message, this encrypted message is transmitted through the insecure public media, and decryption algorithm is used to decrypt the data/message with using key. The reconstruction of the original message/data is possible only if the receiver has the decryption key to use for decryption for recover the hidden message. The second method is steganography, where the hidden message is inserted in another object while using the algorithms. There are different kinds of cryptographic and steganography technique so we used different combinations of cryptography and steganography. Dual steganography is the security in which steganography and cryptography both are used together i.e. combine use of both techniques. In this paper we are comparing the different combinations of both cryptography and steganography which is based on their security. We are focused on digital image based steganography i.e. the cover medium is digital image.***

Key Words: Cryptography, Steganography, Digital Network, Confidentiality

1. INTRODUCTION

In the present era, Security of information is one of the most important factors of information technology and communication. The internet is an important part for communication and information sharing. Every person wants their communicating data to be secret and safe. Any organization who deals with confidential data whose first priority is sending the safe and secure messages to other. Almost all information hiding techniques are used for military, internet banking, intelligence agencies and for privacy etc. so it is most important topic in the current time. [2]. For hiding and detecting the data or information as more and more techniques are developed For protecting confidential data from intruders or hackers it is necessary to develop a strong new technique [2]. The two important techniques for providing security are cryptography and steganography. Both are well-known and widely used techniques which used for information security for confidentiality of data exchange.

1.1 Steganography

Steganography is the technique of embedding hidden messages /data in such a way that no one can detect the existence of the messages, except the sender and intended receiver(s). The main aim of steganography is to hide the secret message or information in such a way that no one is able to detect it. If they found any suspicion data, then goal is defeated [1]. The various types of data in steganography can be audio, video, text and images etc. The basic model of Steganography consists of three components:

The Carrier image: The carrier image is also called the cover object that will carry the message/data which is used to be hidden.
The Message: A message can be anything like data, file or image etc.
The Key: A key is used to decode/decipher the hidden message.

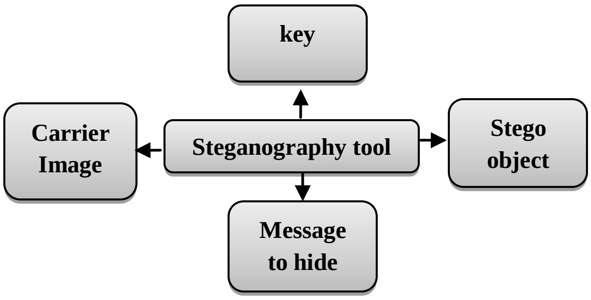

Fig -1: Basic Model Of Steganography

1.1.1 Types For Steganography

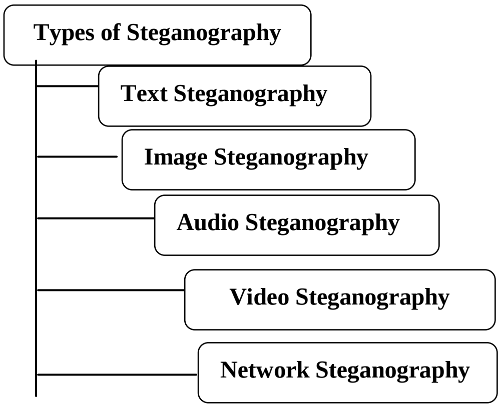

Fig-2: Techniques Of Steganography

a) Text Techniques:
•Line Shift Coding Protocol • Word Shift Coding Protocol • Feature Coding Protocol • White Space Manipulation • Text Content

b) Image Techniques:
• Simple Watermarking • LSB (Least Significant Bit Hiding)
• Direct Cosine Transformation • Wavelet Transformation

c) Audio Steganography: Four main steps for audio Steganography are: 1. Alteration 2. Modification
3. Verification 4. Reconstruction

d) Video Steganography: This technique is used for mixing of sound and image and sends it together over the transmission medium.

1.1.2. Steganography Techniques

a) Spatial Domain methods: These methods directly changed some bits in the image pixel values of hiding data. There are various spatial domain methods such as (i) Least significant bits (LSB) (ii) Pixel values differencing (PVD) (iii) Edges based data embedding method (EBE) (iv)Pixel intensity based LSB

b) Transform Domain techniques: In this technique, the secret data is embedded in the transform or frequency domains of the cover object. In this many different algorithms and transformations are used for hiding information in an image. This technique is more robust and complex. There are some transform domain techniques such as (i) Discrete Fourier transformation technique (DFT), (ii) Discrete cosine transformation technique (DCT), (iii) Discrete wavelet transformation technique (DWT).

c) Masking and Filtering: The technique in which secret data/message is hidden in the more significant areas by marking an image. This method is more robust than LSB method. The main limitation of this technique is that this method can be applied only to gray scale images and 24 bits images.

2. Cryptography

Cryptography is the art of achieve the security by encode the messages to make them non-readable. Cryptography is an art of transmitting the data safely over the Internet by applying some cryptographic algorithms so that it will be difficult for intruders to attack some confidential or private information. Two basic terms used in cryptography are encryption and decryption; encryption process is the process of converting plain text into cipher text and decryption process is the reverse process of encryption. Plain text is the text which have the original message or data which is not encrypted and cipher text is the text which is ready to be shared after encryption of message. A key is needed for both encryption and decryption of the message [1].

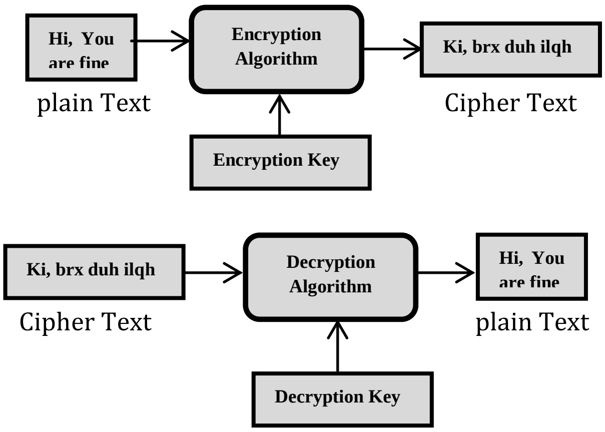

Fig- 3: Encryption and Decryption

There are basically, three types of cryptography schemes typically used to accomplish these goals: Symmetric key cryptography, Public key cryptography.

a) Symmetric-Key Cryptography
This algorithm is also known as Secret Key cryptography, where the sender and the receiver use the same keys to encrypt and decrypt the message. The algorithms known as the symmetric-key algorithm which is used for symmetric-key cryptography. The symmetric algorithms are classified into two types: stream cipher and block cipher. The stream cipher algorithms which are designed to accept a crypto key and a stream of plaintext which are use to produce a stream of cipher text. The block cipher algorithms operate on blocks of data where, the plaintext is broke into blocks and operates on every block independently.
List of Symmetric Algorithms:
Data Encryption Standard (DES)
Advanced Encryption Standard (AES)
Triple Data Encryption Standard
Blowfish Encryption Algorithm
International Data Encryption Algorithm

b) Public-Key Cryptography

In the Public Key Cryptography, each user generates two keys: One is a Public key used by anyone for encrypting messages to be sent to the user and a Private key which the user needs for decrypt the messages. List of Public- key Algorithms:
Diffie-Hellman
RSA
DSA etc.

3. DIFFERENCE BETWEEN CRYPTOGRAPHY AND STEGANOGRAPHY:

- Cryptography is used to encrypt information and steganography is used to hide the existence of data.
- Cryptography encrypt the information by using a secret key so that a third person cannot access the information without the secret key. Steganography hides the information by using a cover medium so that a third person cannot identify the hidden data in the cover medium.[3]
- Sometimes sending encrypted information may take attention, while invisible information will not.
- Accordingly, cryptography is not the permanent solution for secure communication; it is only part of the solution. Both techniques can be used together to form better security.

4. DUAL STEGANOGRAPHY

As we know steganography and cryptography, both are data hiding techniques used for secure communications over insecure channel. But for obtaining much higher security, the combination of two is used. Inside the steganography process, cryptography is used, so it's called as Dual Steganography.

The basic model of dual steganography is the secret data is firstly converted into encrypted form and then using this encrypted information as secret data, is hidden inside the cover image with the help of embedding algorithm and finally the stego image is formed which is same as cover image in human perceptible way.

Sometimes a stego key is also used to make the communication more secured. This key can directly be given by the sender and used during the embedding algorithm. The stego key must be known at both transmitter and receiver side. Thus using cryptography along with steganography, secret information can be easily communicated with high security. This is more secured way of using cryptography and steganography.

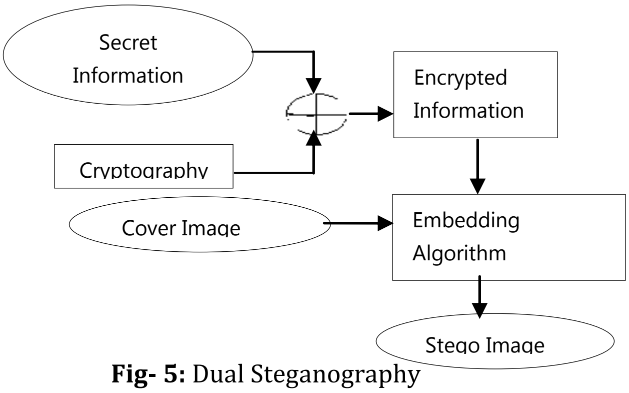

Fig- 5: Dual Steganography

5. COMBINE TECHNIQUES USE IN DUAL STEGANOGRAPHY

a) Combine use of LSB Method with Secret Key:

In this combine technique the LSB Steganography method use the secret key for hide the data into input pixel of cover image without producing distortions. In which a bit of hidden data is placed in either LSB of green or blue matrix of a specified pixel which is decided by secret key. [22]

b) Combine use of linked list method and fiestel network:

In this method the secret text should be encrypted using Fiestel network and then embedded inside the the cover image to obtain stego image. The embedded process is done using Linked List method , in this method ,after embedding the byte of information inside one 3*3 pixel, the address of location of next byte of information should be embedded next to it.[11]

c) Combine use of DWT and Blowfish:

The techniques included in the combination would be image compression, cryptography and steganography. DWT compression has been used, because it is a very strong compression algorithm. The steganography image would be compressed to reduce size. Blowfish encryption algorithm would be used for the encryption purposes. It offers maximum throughput (faster) and also energy efficient.[4]

d) Combine use of AES and DCT:

In cryptography, this system is used AES algorithm with its symmetric key and the cipher text is converted into two extra keys for high security. The system is designed with three creation steps to hide the text –
Crypto Creation Step – AES Implementation Step
Security Creation Step – Newly Developed Technique
Stego Creation Step – DCT Techniques Implementation Step

e) Combine use of DSA and audio steganography:

In which firstly Encryption is done using Digital Signatures. In which user create self-signed PDF document by creating own certificate. Embedding data is done using Audio steganography.

6. CHARACTERISTICS FEATURE OF DUAL STEGANOGRAPHY:

a) Payload Capacity: It means how much information/data can be embedded in the cover object. Payload capacity of secret information is based on the number of pixels of the cover image.
b) Robustness: It means that the secret message can't be demaged after embedding and extraction procedure of an stego image.
c) Imperceptibility: After hiding the secret message in the cover image, one should not be suspicion of the existence of the secret message with the cover medium.
d) Accurate & Reliable: The extraction of the secret message from the cover object should be reliable and accurate.
e) Peak signal to noise ratio (PSNR): The ratio that is used to measures the quality between the original and a compressed image. IF PSNR ratio is high then will be better quality of an image.
f) Mean square error (MSE): It represents the total error in the received data when it is compared to the data before and after processing. The small value of MSE will be represented more efficient image steganography technique.

7. LITERATURE REVIEW

Author Name	**Title Name**	**Proposed work**	**Advantages**	**Disadvantages**
S.M. Masud Karim et. al	A New Approch for LSB based image steganography using secret key[22]	To combine cryptography with modified LSB steganographic technique.	High PSNR, good security	High time complexity , no robust
P. Selvigrija and E.Ramya	Dual Steganography for Hiding Text in Video by Linked List Method[11]	the linked list method and Feistel Network	High quality and security	High Time Complexity
Pooja Rani, Apoorva Arora	Image Security System using Encryption and Steganography[4]	DWT compression, Blowfish encryption algorithm	Good Image Quality	Average PSNR value
Kamal and Lovnish Bansal	Enhancement Key Of Cryptography And Steganography Using RSA And Neural Network	Combination of DCT and LSB with RSA	Better Integrity	Higher complexity
Pye Pye Aung et. Al.	A Novel Secure Combination Technique of Steganography and Cryptography	To combine the AES Cryptographic technique and the DCT steganography	Higher time complexity	limited embedding capacity
Natasha Taneja, Dr. Prinima Gupta	Implementation of Dual Security through DSA and Audio Steganography	Combine use of DSA with Audio Steganography	Provide Double Security	Limited embedded
Piyush Marwaha et al.	Visual Cryptographic Steganography in Images[21]	To combine LSB steganography with visual cryptography	Less Time Complexity, more secure	Lower PNSR value
Shailender Gupta, et al.	Information hiding using Least Significant bit steganography and cryptography	To combine cryptography techniques RSA and Diffie Hellman with Lsb steganography technique	High security	Higher time complexity, limited embedding capacity and not robust

Table -1: Literature Survay

8. CONCLUSIONS

Due to increasing demand for privacy and security, a need for various data hiding techniques which lead to the development of several techniques for embedding and extraction.
As we know, cryptography and steganography have been known for many years. We can encrypt data, but it will be exposed while transferring. On the other hand, we can hide data into a common object, but if someone extracts it, he/ she can get the information easily. Therefore if we combine both of them, so in case one gets the embedded stuff, she/he will face an encrypted data.

REFERENCES

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

[2] Jigar Makwana, S.G Chudasama, “Dual Steganography: A New Hiding Technique for Digital Communication” in IJAREEIE International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 5, Issue 4, April 2016.

[3]Vishnu S babu and Prof. Helen KJ, “A study on combine cryptography and steganography” in IJRSCSE International Journal of Research Studies in Computer Science and Engineering, Volume 2, Issue 5, May 2015, PP 45-49

[4] Pooja Rani , Apoorva Arora, “Image Security System using Encryption and Steganography” in IJIRSET International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 6, June 2015.

[5]Nitin Kaul and Nikesh Bajaj, “Audio in Image Steganography based on Wavelet Transform” in International Joural of Computer Applications (0975-8887), October 2013.

[6] Jitha Raj.T, E.T Sivadasan, “Secure Transmission of Data by Splitting Image in” in IEEE, Dec. 16-19, 2015.

[7] Divya Makwana ,Shrikant Lade, “Dual Steganography Implementation Using LSB Technique” in IJAREST International Journal of Advance Research in Engineering, Science & Technology, August- 2015.

[8] Dipanwita Debnath, Suman Deb, Nirmalya Kar, “An Advanced Image Encryption Standard Providing Dual Security: encryption using Hill Cipher & RGB image steganography” in IEEE International Conference on Computational Intelligence & Networks, 2015.

[9] Vijay Kumar and Dinesh Kumar, “Digital Image Steganography Based on Combination of DCT and DWT” in Springer-Verlag Berlin Heidelberg, pp. 596–601, 2010.

[10] Kamal and Lavnesh Bansal, “Enhancement Key Of Cryptography And Steganography Using RSA And Neural Network” in IJARCET International Journal of Advanced Research in Computer Engineering & Technology Volume 3 Issue 5, May 2014

[11] P. Selvigrija and E. Ramya,”Dual Steganography for Hiding Text in Video by Linked List Method” in IEEE International Conference on Engineering and Technology (ICETECH), 20th March 2015, Coimbatore, TN, India.

[12] Nikita Sharma, Meha Khera, “A Novel Approach to Image Steganography Using Hash-LSB and DWT Technique” in IJARCSSE International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 6, June 2015

[13] Vijay Kumar and Dinesh Kumar, “Digital Image Steganography Based on Combination of DCT and DWT” in Springer-Verlag Berlin Heidelberg 2010, pp. 596–601.

[14] Divya.Aynapur, S.Thenmozhi, “A SECURE STEGANOGRAPHY APPROACH OF MULTIPLE SECRET IMAGES USING ANN” in @IJRTER-2016

[15] Mihir H Rajyaguru, “CRYSTOGRAPHY-Combination of Cryptography and Steganography With Rapidly Changing Keys” in International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 10, October 2012)

[16] A.E.Mustafa, A.M.F.ElGamal, M.E.ElAlmi, Ahmed.BD, “A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit” in Research Journal Specific Education Faculty of Specific Education Mansoura University Issue No. 21, April. 2011

[17] Bibhudendra Acharya et al. “Image Encryption Using Advanced Hill Cipher Algorithm” in International Journal of Recent Trends in Engineering, Vol.1, No.1, May 2009, pp.663-667.

[18] Harshitha K M and Dr. P. A. Vijaya , “secure data hiding algorithm using encrypted secret message” in International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012.

[19] Hemang A. Prajapati, Dr. Nehal G. Chitaliya, “Secured and Robust Dual Image Steganography: A Survey” in International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 1, January 2015

[20]Aarti Mehndiratta, “Data Hiding System Using Cryptography & Steganography: A Comprehensive Modern Investigation” in International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 01 | Apr-2015

[21] Piyush Marwaha, Paresh Marwaha ,"Visual Cryptographic Steganography in Images" in proceedings of Second International conference on Computing, Communication and Networking Technologies, pp 1-6, 20104.

[22] S.M. Masud Karim et. Al, "A New Approch for LSB based image steganography using secret key"in proceeding of 14th international conference on computer and information technology(ICCIT 2011) 22-24 December,2011.

BIOGRAPHIES

"Babita, Mtech Scholar from S.B.B.S.U, Jalandhar, Punjab , India"