Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhancement of Security in Steganography

[1]Jay Shah, [2]Jigar Vavadia, [3]Vishal Banwari, [4]Dr. Vishal R Dahiya
[1, 2, 3] Student-CE, IITE, India
[4] Head, IICT, Indus University, India

***Abstract*—Digital communication has become a critical part of infrastructure nowadays. A lot of applications, messages are passed from sender to receiver end. Security of information passing over a channel has become an important issue in this internet era. Confidentiality and Authenticity of the information is required. Cryptography and Steganography are two popular methods to achieve the security of information. Cryptography is obscuring the content of message and Steganography refers to hiding whole message into an image. This paper focuses on the various combining cryptography and Steganography methods that can be used to hide information.**

***Keywords*—Cryptography, Steganography, Authentication, Compression, LSB.**

I. INTRODUCTION

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography.

Cryptography is the science of writing in secret code. It derived from Greek word Krypto's (hidden). Cryptography is about concealing the content of the message. At the Same time encrypted data package is itself evidence of the existence of valuable information. Steganography goes a step further and makes the cipher text invisible to unauthorized users.Steganography derives from the Greek word steganos, meaning covered or secret. Steganography was used even in ancient times and these ancient methods are called Physical Steganography [1].

Some examples for these methods are messages hidden in messages body, messages written in secret inks, messages written on envelopes in areas covered by stamps, etc. Steganography is a technology in which modern data compression, cryptography technologies can bring together to satisfy the need for privacy on the Internet. Modern Steganography methods are called Digital Steganography [2].

These modern methods include hiding messages within noisy images, embedding a message within random data, embedding pictures with the message within video files, etc. Furthermore, Network Steganography is used in telecommunication networks. This includes techniques like Steganophony and WLAN Steganography methods for transmitting Steganograms in Wireless Local Area Networks.

II. CRYPTOGRAPHY AND STEGANOGRAPHY

Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world. Due to this, Steganography removes the unwanted attention coming to the hidden message.

- **COMBINATION OF CRYPTOGRAPHY AND STEGANOGRAPHY**

Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content. By combining Steganography and Cryptography one can achieve better security [3].

- **COMPRESSION**

Technique that can be used to convert large size data into small size data without any kind of data loss.

- **AUTHENTICATION**

Technique ensures that origin of the data is correctly identified.

We will be discussing combination of four individual methods that can be used to enhance the security of the data.

III. IMPLEMENTATION STEPS

There are five steps which we have discussed in this research paper. Steps are depicted in Figure 1.

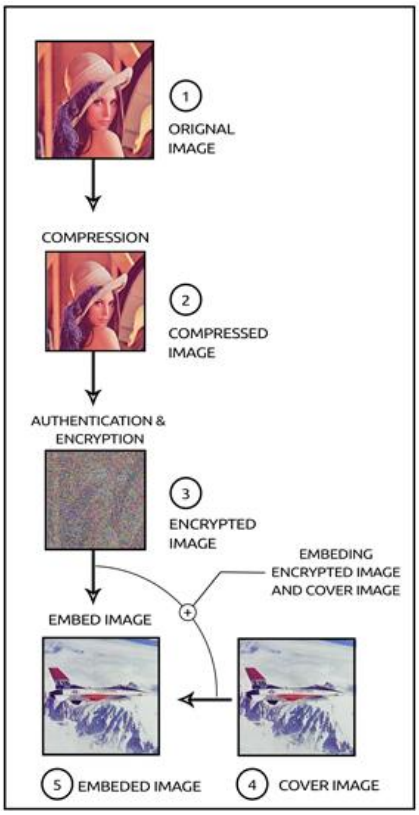

Figure 1: Steps of the proposed methodology

Implementation steps

1. First Original image which is to be embedded is selected as shown in (1) step in fig 1.1.
2. Various compression techniques is used to compress selected image in step (2) as in fig 1.1 Compression Techniques such as:

a. Lempel-Ziv-Welch
b. MD5 Encoding
c. Huffman Encoding
d. Run-Length Encoding

All this type of Compression technique is applied on image as they all are Lossless in Nature.

3. For Secrecy Authentication and Encryption is carried out on Encrypted image so that original image data is secure for transmission.

Authentication Technique such as Public Private Key-cryptography (RC5, Deffe-helmen), Hash MAC, Zero Knowledge Proof, Digital Signatures and Protocol such as Secure Socket Layer, IPSEC, Kerberos. [4]
Standard Byte Encryption Techniques Are used to secure data such as:

a. AES Algorithm
b. DES Algorithm
c. Blowfish Algorithm
d. RSA, IDEA

4. After Encryption is completed it is Embedded in cover image

Cover Image: It is an Image larger in size than original Data Image in which data/Image should be hidden as shown in Fig 1.1
Various technique are there for embedding one image into another but the best technique we use is LSB (Least Significant Bit) Techniques.

BASIC STEPS OF LSB TECHNIQUE FOR IMAGE ENCODING [5]:

1. The cover and original images are read and converted into the unit 8 type that is set of 8 bits.
2. The numbers in secret image called matrix are conveyed to 8-bit binary. Then the matrix is reshaped to a new matrix called matrix a.
3. The matrix of the cover image is also reshaped and called matrix b.
4. Increasing or decreasing the value by changing the LSB does not change the appearance of the image so the resultant embedded image looks almost same as the cover image.
5. The embedded -image, which is very similar to the original cover image, is achieved by reshaping matrix b that is reshaping our cover image.

6. While extracting the data, the LSB of the stego image is collected and they are reconstructed into the decimal numbers. The decimal numbers are reshaped to the secret image [6].

IV. DETAILS OF THE PROCESS

We start with the input image that is the original image. Conversion of pixel in the bits takes place to apply compression process. The key will be added with the compressed bits the authentication and encryption method will be applied to get encrypted data. The encrypted data and cover image is to be merged using LSB technique. The resultant image will be the embedded image.

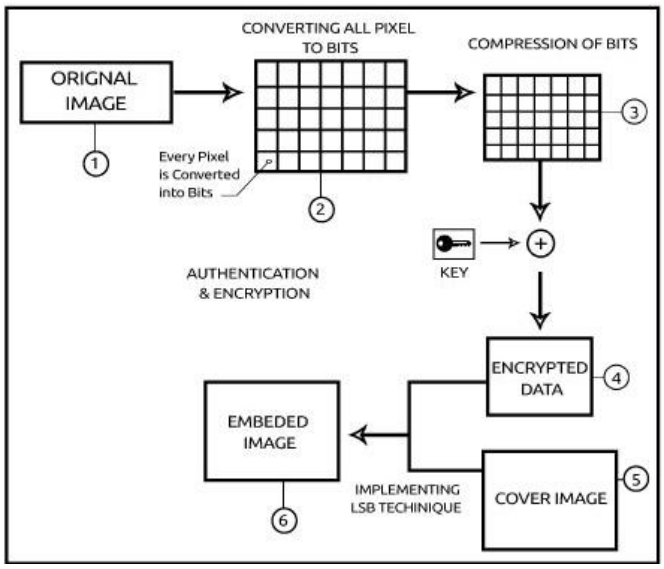

Figure 2.1:Process Diagram

DETAIL EXPLANATION:

SENDER SIDE:-

1. First any image is selected which user want to securely sent to another user as shown in (1) step in fig 2.1.
2. Every pixel of selected image is converted into bit format as shown in (2) step in fig 2.1 as bit format is properly processed with compression and encryption techniques rather than rgb value of pixels.
3. Total compression of all bits is carried out after conversation of pixels into bits as shown in (3) step of fig 2.1. compression techniques are used as discussed in Implementation Steps
4. For authentication various techniques are used as discussed in Implementation Steps
5. For Encryption key is generated by user which must be given to receiver end for decryption process as shown in fig 2.2 above (4) step.
6. Encryption of overall compressed image is carried out and processed for further steps as shown in (4) step in fig 2.1.
7. Valid cover image is selected that is bigger in size than original image and it will act as cover up image. Inside which our secret (original) image is embedded.
8. Secret or original image is embedded in cover image using LSB technique as discussed in Implementation steps.
9. Final Image is generated as shown in (6) step in fig 2.1.
10. Final image contain our compressed and encrypted image which look similar to cover image.
11. This final image is transmitted via any medium to user at receiver end.

RECEIVER SIDE:-

1. After Receiving Final Image user will apply LSB technique in reverse order to extract original image from Final image.
2. After that user will decrypt the image with help of key given by user from sender side and authentication is also carried out at receiver end.
3. On decrypted image decompression technique is applied which is same technique used at compression time now final image is obtained but it is in bit form.
4. So bits to pixel conversion is done a particular set of bits indicated particular pixel, at last over all image is obtain in pixel format
5. At Last User gets Original image.

IV. CONCLUSIONS

In the proposed work overall efficiency in security is increased as different technique are used such as compression technique by which overall image is compress which leads to decrease in complexity of pixel to bit conversion program and transmission of compressed data is faster compare to original data. Other technique such as Encryption technique which leads to enhanced security of image before using steganography. As in steganography, image or data is embedded

in different image without preprocessing the image which gives less security as extraction of original image is easy by intruder than encrypted image. Authentication is proposed in this paper which leads to conformation on both side that image/data is not modified or replaced while transmitting. We conclude are paper as the proposed work i.e. when we include compression, authentication and encryption within steganography it will for sure enhance the security and processing of the image compare to using only steganography for data hiding or image hiding which can be justified my steps explained in implementation steps.

REFERENCES

[1] Jacob Mathai, History of Computer Cryptography and Secrecy Systems.[Online]. Available: http://www.dsm.fordham.edu/~mathai/crypto.html.

[2] C.P.Sumathi, T.Santanam and G.Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding" *International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, pp. 1, 2 December 2013*.

[3] How to hide one image in another [Online] Available: http://www.instructables.com/id/How-to-hide-one-image-in-another-An-introduction-/?ALLSTEPS.

[4] Richard Duncan "An Overview of Different Authentication Methods and Protocols" *SANS Institute InfoSec Reading Roompp. 4-6 October 2003.*

[5] KshetrimayumJenita Devi, "A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique" project thesis, National Institute of Technology-Rourkela Odisha, May2013.

[6] Pratap Chandra Mandal, "Modern Steganographic technique: A survey" *International Journal of Computer Science & Engineering Technology (IJCSET) Vol.3, No.9, pp 446. September 2012*.

