A Hybrid Approach of Steganography and Cryptography to improve Data Security

Susmita Soni
M.Tech, Dept. of Computer Science and Engineering*
Marudhar Engineering College, Bikaner (Rajathan)
er.susmitasoni@gmail.com

Sunita Chaudhary
Asst. Prof., Dept. of Computer Science and Engineering
Marudhar Engineering College, Bikaner (Rajathan)
er.sunita03@gmail.com

***Abstract*— This paper presents a technique for secret communication using Cryptography and Steganography. In this paper, the secret message of different size is hidden into an image for making the system more secure. The only authorized users can hide and extract the secret message. The secret messages of different size are used to test the system and the system satisfies all requirements of Steganography. The hybrid approach of Steganography and Cryptography makes the communication secured and it is difficult for the attacker to detect the secret message.**

Keywords* - *Cryptography, least significant bit (LSB) method, Steganography.

I. INTRODUCTION

Steganography comes from the Greek steganos (covered or secret) and graphy (writing or drawing). Steganography can be defined as the hiding of information by embedding messages within other, seemingly harmless messages, graphics or sounds [1]. Cryptography is the science of providing security to information by encrypting it. It is the art of secret writing. It scrambles the contents of confidential information.

Steganography is very old methods used around 440 B.C. Steganography is hiding a confidential message within an ordinary file.

Steganography with Cryptography is a useful approach to hide the encrypted message in a carrier file so that no one can suspect the existence of secret message. This approach provides more security to confidential message. Steganography is data hiding within data. Steganography is a technique which can be applied on text, image, audio files and video files. Steganography is a two-step process: First step is to create a stego image which is a combination of secret message and carrier file. Second step is to extract the secret message from the stego image. There are two common methods of embedding a secret message. First, the spatial embedding, in which secret message is inserted into the Least Significant Bit (LSB) of image pixel and second is transform embedding, in which the secret message is embedded by altering the frequency coefficients of the carrier image or stego image [2].

II. IMAGE BASED STEGANOGRAPHY AND CRYPTOGRAPHY

Steganography is not same as Cryptography. Data hiding techniques have been widely used for covert communication for long time. Ensuring data security is a big challenge for computer users over Internet.

Hybrid Steganography and Cryptography approach is a new all in one method which able to perform Steganography with strong encryption technique. This method has been planned either to work with bit streams scattered over multiple images or to work with still images. This approach make possible to use it in real time applications such as mobile video communication [3]. Fig.1 depicts the combination of Cryptography and Steganography At sender side, first the secret message is encrypted which results in cipher message. This cipher message is embedded into cover image which form a stego image as a result. Sender sends this stego image to receiver which contains the confidential message. At receiver side, the intended recipient retrieve the cipher message from the stego image and apply decryption to the cipher message which results in original confidential message.

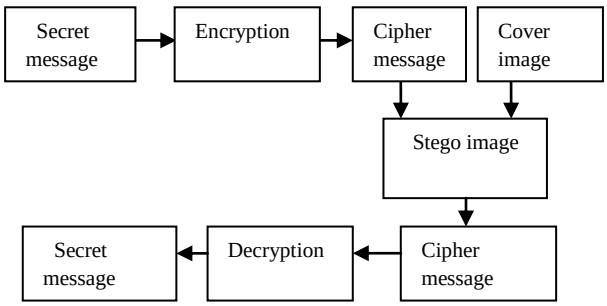

Figure 1. Combination of Steganography and Cryptography

III. IMAGE STEGANOGRAPHY

Embedding secret message in digital image is most widely used method in today's digital world. Image Steganography is about exploiting the limited powers of the human visual system (HVS). It exploits holes in the Human Visual System (HVS). Any plain text, cipher text, an image, or any other file can be embedded in an image. In recent years, Image Steganography has become quite effective due to fast development in graphical computers. Digital image is the mostly used carrier in steganography. A picture is a collection of color pixels. Each pixels have their own characteristics such as 'brightness', 'chroma' etc. These characteristics can be digitally expressed in terms of 0s and 1s.

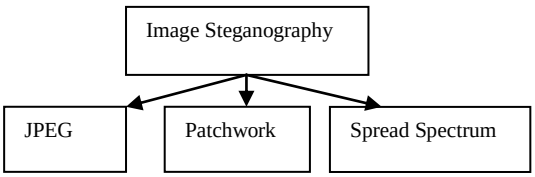

Figure 2. Three categories of Image Steganography

A. Common Approaches of Image Steganography

There are number of ways exist to hide the secret information in digital file. These common approaches are as follow:

1. Least significant bit insertion
2. Masking and filtering
3. Redundant Pattern Encoding
4. Encrypt and Scatter
5. Algorithms and transformations

1) Least Significant Bit insertion: Least Significant Bit insertion is mostly used approach to embed the secret data into an image. In this technique, the secret message is put in the least significant bits of the pixel values. This technique is good for image, audio and video steganography. The resulting stego image is look identical to original file.

Large images are mostly used for image steganography because they have most space to hide the data. An 8-bit image only can use 256 different colors whereas in 24-bit image there are 16777216 possible colors.

For example in 24 bit image, we want to insert letter S whose binary value is 01010011 which uses the RGB color model. Each pixel uses eight bits for the intensity of red, green and blue. Here we need 3 pixels for hiding letter S [4,5,6].

	RED	GREEN	BLUE
Pixel 0	00100111	11101001	11001000
Pixel1	00100111	11001000	11101001
Pixel 2	11001000	00100111	11101001

After inserting S into the above sequence the embedded image will be look like this

	RED	GREEN	BLUE
Pixel 0	0010011**0**	1110100**1**	1100100**0**
Pixel 1	0010011**1**	1100100**0**	1110100**0**
Pixel 2	1100100**1**	0010011**1**	11101001

2) *Masking and Filtering:* Masking and filtering techniques are mostly used on 24 bit and gray scale images. They hide secret message similar to digital watermarking. Masking images includes change in the luminance of the masked area. The smaller the luminance change, the less of a chance to be detected. This technique masks secret message over the carrier image by changing the luminance of particular areas. During masking, it embeds the secret message in significant bits of the carrier image. It is not influenced by lossy techniques because if the attacker alters the image it does not affect the secret message. Masking is more robust technique than LSB insertion with respect to image compression, cropping, and some image processing techniques [4,5,6].

3) Redundant Pattern Encoding: For redundant pattern encoding, patchwork and other similar tools are used, which is a kind of spread spectrum technique. In this technique the secret message is scattered throughout the carrier image. By using this technique the image becomes more resistant to image cropping and rotation.

4) Encrypt and Scatter: The Encrypt and Scatter technique is most widely used technique in image steganography. It tries to emulate white noise. White Noise Storm is a combination of spread spectrum and frequency hopping practices. The principle of White Noise Storm is it scatters the secret message to hide over a carrier image.

5) Algorithms and Transformations: This technique is often used in the lossy compression domain with JPEG digital images. JPEG images use the discrete cosine transform (DCT) to perform compression task. In this technique, the cosine values cannot be calculated accurately due to this the DCT yields a lossy compression. In transformation based steganography algorithms, first the secret message is compressed using DCT and then embedded within the JPEG image. The secret information is strongly embedded into the image and due to this it is hard to decode the message unless the image is first decompressed and the hidden message is retrieve [7].

IV. PROPOSED WORK

During transferring the data, the attacker can know that there is some confidential information by using cryptography. So it is easy for the attacker to make modification to secret message. In order to overcome this problem a model is proposing below. In this model, image steganography is used for hiding the secret message into a carrier file so that the attacker cannot feel the presence of the secret message in it and in this way the transmission will be secured.

A. Proposed Algorithm

In Proposed algorithm, first of all we take a pixel from the image and break it into color components. From each color component we get the Least Significant Bit i.e. LSB. Now we read the message byte and take the first bit of it. Each LSB of the pixel is substituted with each bit of the message byte respectively. In this way we embed the secret message into an image.

The embedding process is as follow:

Inputs: Secret message and Image

Output: Stego image

Step 1: First of all read the secret message.

Step 2: Read every bit of the message byte and take first bit of it.

Step 3: Read the pixel from the image and take a pixel of the image.

Step 4: Break the pixel into color component.

Step 5: Take the first color component of that pixel.

Step 6: Get the LSB of the color component.

Step 7: Substitute one LSB bit of color component (from step 6) with one bit of secret message (from step 2).

Step 8: Repeat the above steps for the next seven bits of the secret message.

B. Flowchart

While using the system we can embed the secret message into an image and get the stego image. Similarly we can also get the original message through extraction process.

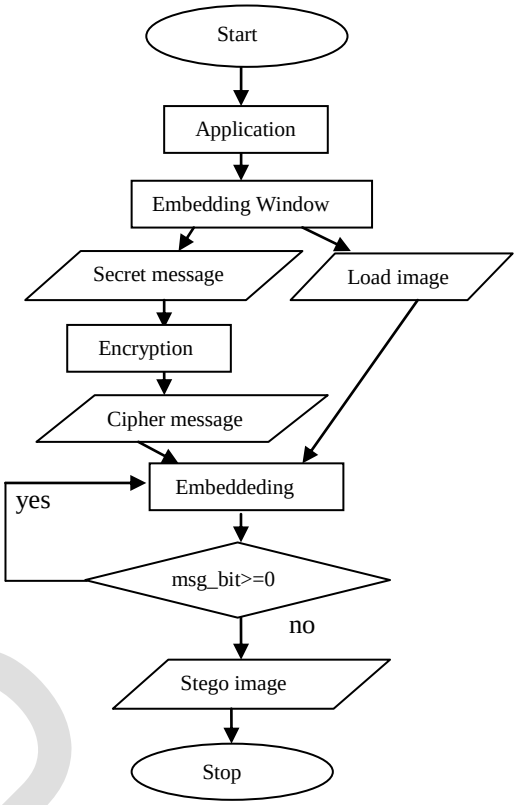

Figure 3. Flowchart of the system

V. RESULTS

The result and the snapshot of the proposed algorithm are given below. The technique is implemented using MATLAB programming language as Front End. The experimental result is observed. Fig.4 is snapshot of embedding window. Fig.5 and Fig.6 are snapshots of original road image and stego road image respectively. Fig.7 and Fig.8 shows histograms of both original and encrypted road image.

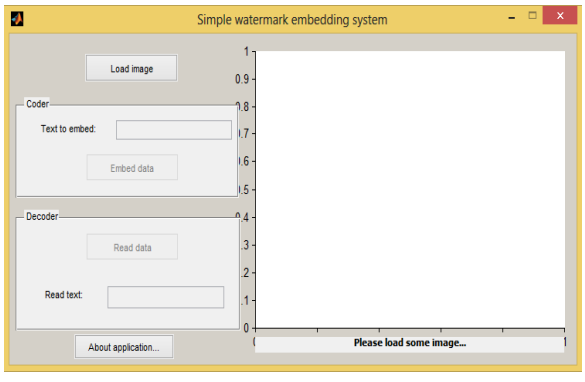

Figure 4. Snapshot of embedding window

Fig.4 is embedding window. When we run the main program this window is displayed. Here we load an image for the further processing.

Figure 5. Snapshot of original road image

Fig.5 is window after loading an image for embedding secret data into it. After loading original image we then enter our secret message in the text box. After writing secret message in the text field we embed the secret data by clicking 'embed data' button. After that a stego image is displayed as a result which is shown in next figure.

Figure 6. Snapshot of stego road image after embedding secret message

Fig.6 is window after embedding the secret message. This figure shows the stego image after the insertion of secret message.

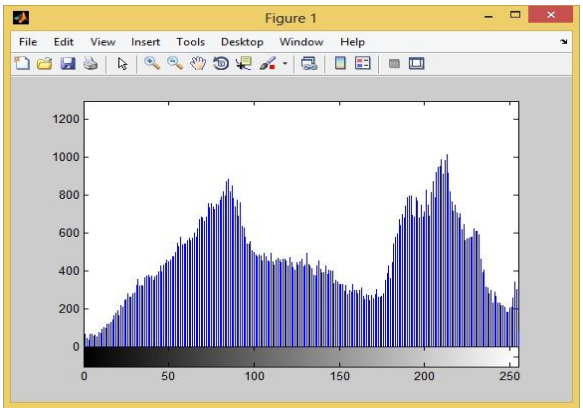

Figure 7. Histogram of original road image

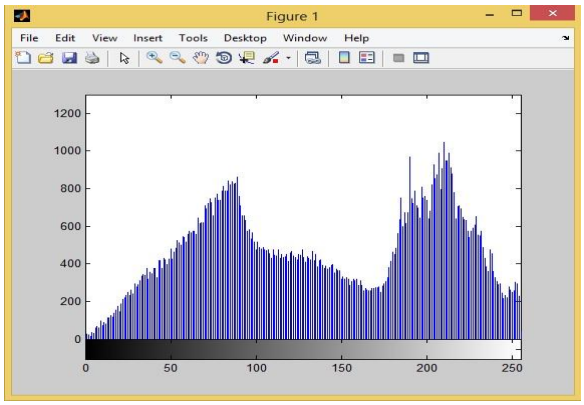

Figure 8. Histogram of stego road image

Fig.7 and Fig.8 show histograms of original and stego road image.

CONCLUSION

In this paper, Steganography was implemented using image as a carrier file. Image file contain different formats. The mostly used format in Steganography is Jpeg image file. Embedding the encrypted message into an image is too much secure.

As future work, we plan to study steganalytic techniques for hybrid steganography and cryptography approach and extend this approach to mobile video communication. We also plan to extend our system so that it can hide other digital files into image, for example hiding audio into image etc.

REFERENCES

[1] A.Joseph Raphael,Dr.V Sundaram "Cryptography and Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630.

[2] "Hiding the Text Messages of Variable Size using Encryption and Decryption Algorithm in Image Steganography" International Journal of Computer Applications (0975-8887) Volume 61-No.6, January 2013.

[3] Sumit Kushwaha, Amit kushwaha "Advanced Network Security using Cryptography and Steganography" Journal of Global Research in Electronics and Communication, Volume 1, No.1, November-December 2012.

[4] Adel Almohammad "Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility" A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing , Brunel University, August, 2010.

[5] Neil F Johnson, Sushil Jajodia, "Exploring Stenography: Seeing the Unseen", IEEEComputer, Feb 1998, pp 26-34.

[6] Rajkumar Yadav "Analysis of Incremental Growth in Image Steganography Techniques for Various Parameters" Int. J. Comp. Tech. Appl., Vol 2 (6),1867-1870, NOV-DEC 2011

[7] Khan, Mohammed Minhajuddin "Steganography"

[8] S. Nithya Devi, P.Laura Juliet "SURVEY ON IMAGE STEGANOGRAPHY ALGORITHM "International Journal of Communications and Engineering Volume 04– No.4, Issue: 02 March2012.