Cryptographic Image Steganography for Data security

Mrs. S. A. Tatugade[1], Hrushikesh[2]
[1, 2] Dept of Computer Engineering
[1] R.M.P. Ambav
[2]B.V.I.T. Palus.

Abstract- *Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information.The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. Work in this paper provide security to the data by using Cryptographic Image Steganography by use of cover as an image. Technique which embeds the message in a subset of the LSB plane of the image. An image is generally not visually affected when its least significant bit plane is changed, basic Steganography for hiding plain text, Steganography plus Cryptography to convert plain text into cipher text and send, LSB and Palette Based Images to add new colors which are visually similar to the existing colors in the palette. Here grayscale image as well as colour image has been used.This work ensures that no valuable information is lost and the data has been transmitted as well as recovered againsafely.*

Keywords- security, Steganography, Cryptography, LSB, Palette.

I. INTRODUCTION

The information communicated comes in numerous forms and is used in many applications. In a large number of these applications, it is desired that the communication to be done in secrete. Such secrete communication ranges from the obvious cases of bank transfers, corporate communications, and credit card purchases, on down to a large percentage of everyday email. Steganography is the ancient art of embedding a secret message into a seemingly harmless message.

The Greek word “steganos” meaning covered writing is basically the concept behind the theory of steganography. Here it is difficult to even detect that a message is being sent. Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately, it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the information is hidden exclusively in images.

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

Cryptography [6] is a technique to scramble a confidential message to make it unreadable for a third party. It is commonly used in the Internet communications today. Cryptography can hide the content of the message, but it can't hide its presence, i.e., the location of the secret message is obvious. This is the reason why an encrypted message can be targeted by the attackers. Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevents the detection of hidden messages. Steganography include an array of secret communication methods that hide the message from being seen or discovered.

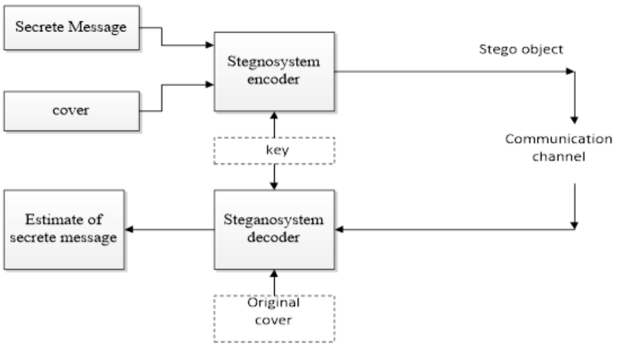

Figure 1.1 Process of Steganography

II. PROBLEM STATEMENT, OBJECTIVE OF THE PAPER

The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity are requiring to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding.

There has been a rapid growth of interest in steganography for two main reasons

(i) The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products.
(ii) Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly protected cover messages.

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information.[1] Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. So proposed system prepares this application, to make the information hiding simpler and user friendly.

Steganography is related to Cryptography by meaning that both are used for security purposes but with different approach or implementation. Steganography along with Cryptography, a very ancient concept but its application varies according to emerging technologies. Here both these technologies have been merged.

III. CRYPTOGRAPHIC IMAGE STEGANOGRAPHY

Many techniques are used to hide data in various formats in steganography. Mechanismused in this paper is the use of the Least Significant Bit [7]. Least Significant Bit is normally used to hide data in a digital image. The other bits may be used but it is highly likely that image would be distorted. Models included in the project are converting plain text into cipher text and then insert into image.
In this project there are only two actor’s sender and receiver. Only sender sends the stego object by login with valid username and password. When the stego object is send then at the receiver side also receiver is need to login with valid username and password. After that receiver can get the message secretly.

Here image [4] is used to hide the text. But when text is too long with respect to the image size then it is difficult to hide the message. We must take image depending upon the message.

A. *Least Significant Bit Insertion*

Many stego tools make use of least significant bit (LSB). For example, 11111111 is an 8-bit binary number. The rightmost bit is called the LSB because changing it has the least effect on the value of the number. The idea is that the LSB of every byte can be replaced with little change to the overall file. The binary data of the secret message is broken up and then inserted into the LSB of each pixel in the image file.

Hiding the data: -

Using the Red, Green, Blue (RGB) model a stego tool makes a copy of an image palette, say, an 8-bit image. The copy is rearranged so that colors near each other in the RGB model are near each other in the palette. The LSB of each pixel’s 8-bit binary number is replaced with one bit from the hidden message. A new RGB color in the copied palette is found. A new 8-bit binarynumber of the new RGB color in the original palette is found. The pixel is changed to the 8-bit binary number of the new RGB colour.

Recovering the data

The stego tool finds the 8-bit binary number of each pixel’s RGB color. The LSB of each pixel's 8-bit binary number is one bit of the hidden data file. Each LSB is then written to an output file.

B. *Masking and filtering*

Masking and filtering techniques hide information by marking an image and is usually restricted to 24-bit and gray-scale images. While traditional steganography conceals information, watermarks extend information since it becomes an attribute of the cover image. Masking techniques hide information in such a way that the hidden message is more integral to the cover image than simply hiding data in the "noise" level. Masking adds redundancy to the hidden information. This makes the masking technique more suitable than LSB with lossy JPEG images.

C. *Hiding Message into Image*

- *Steganography without using keys:*

The steps in steganography include the writing the text messages, encryption of the text message [2] is one of the options available. Later, text is hidden in the selected media and transmitted to recipient. Various techniques used in the art of steganography is the arrangements of various bits of the characters of the text in an image or other media. Keeping in mind the above, two files are needed; the image file and the text file that contains the data.

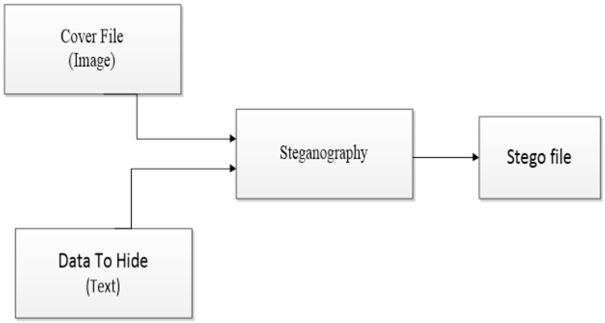

Figure 3.1 Steganography without using keys

- *Steganography using keys:*

The basic model of steganography consists of Carrier, Message and Password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message.

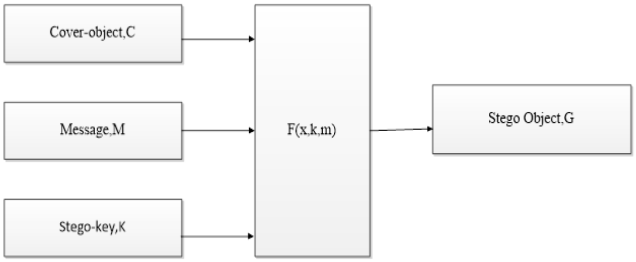

Figure 3.2 Steganography using keys

Message is the data that the sender wishes to remain it confidential. It can be plain text, cipher text, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as stego-key, which ensures that only recipient who know the corresponding decoding key will be able to extract the message from a cover-object. The cover-object [3] with the secretly embedded message is then called the stego-object.

- *Converting image into bits*

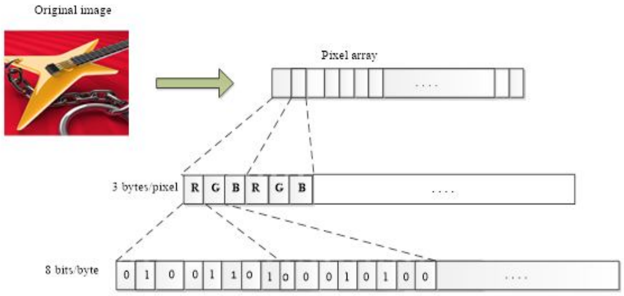

Figure 3.3 Converting image into bits

- *Converting data into bits*

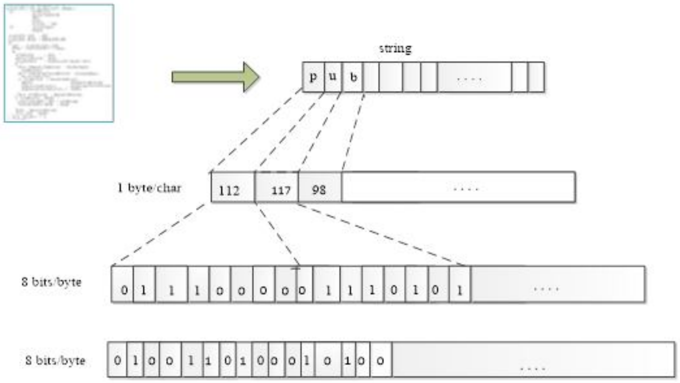

Figure 3.4 Converting data into bits

- *Inserting text bits into image*

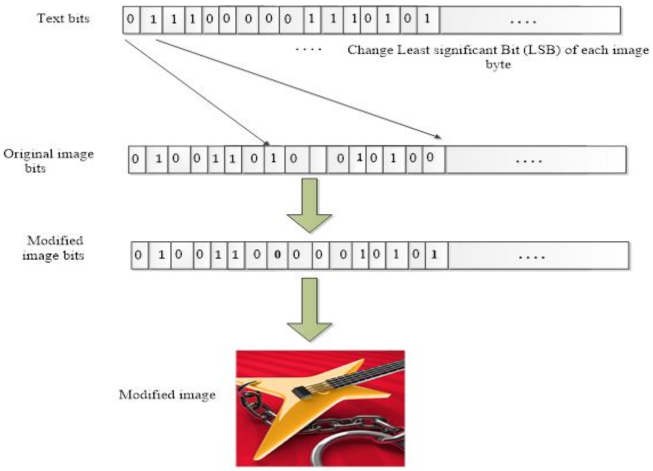

Figure3.5 Inserting text bits into image

D. Retrieving Message from Image

At receiver end, reverse process is implemented to recover the original text message. Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message. In general, the information hiding process extracts redundant bits from cover-object.

The process consists of two steps.

(i) Identification of redundant bits in a cover-object. Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the cover-object.
(ii) The embedding process then selects the subset of the redundant bits to be replaced with data from a secret message. The stego-object is created by replacing the selected redundant bits with message bits.

- *Extracting the text from modified image*

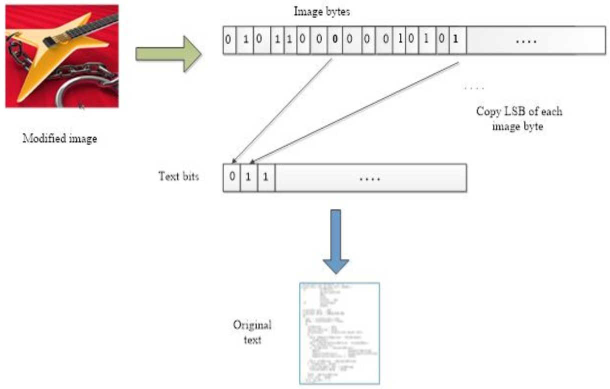

Figure 3.6 Extracting the text from modified image

- *Class Diagram*

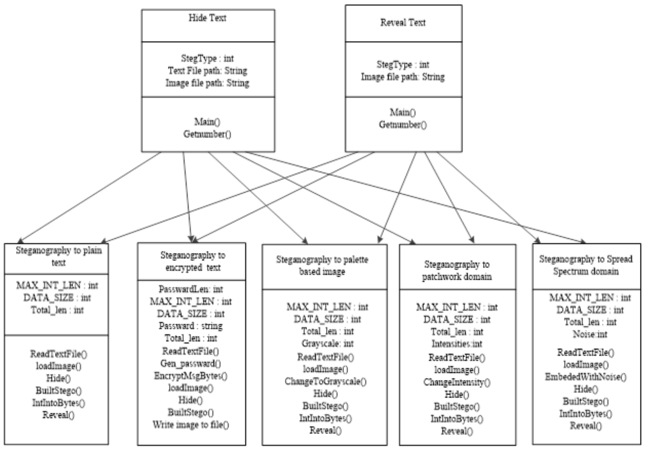

Figure 3.7 Class Diagram

- *Dataflow Diagram*

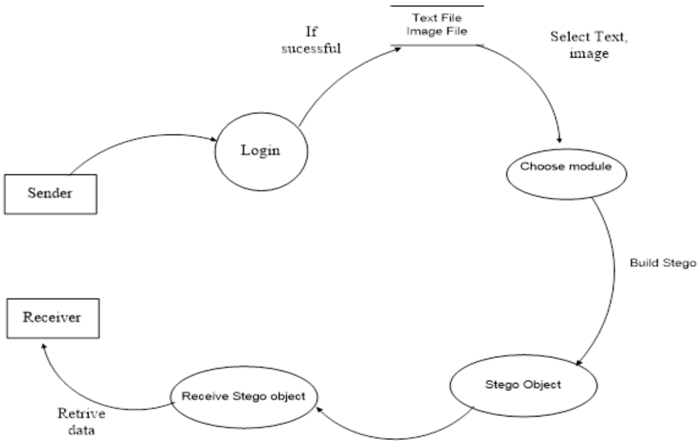

Figure 3.8 Dataflow Diagram

- *Image before and after*

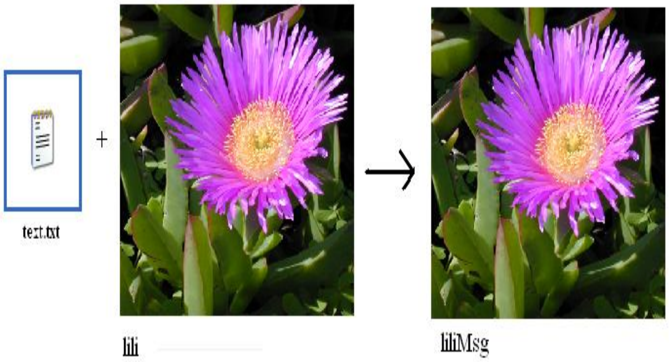

Figure: 3.9: Image before and After

IV. CONCLUSION

In this paper we have presented an enhancement of the image steganographic system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover-image. In our proposed approach, the message bits are embedded sequentially into the cover image pixels. The further research will include the enhancement of the algorithm that will utilize the entire image for embedding the message. Military communications system makes increasing use of traffic security technique which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections.

V. FUTURE SCOPE AND EXTENSION

The future scope for this system as thought of at this point in time are as follows –

- This steganography can be done for other images also like .TIF, JPEG etc. we can use more size of image to send more data in one single image.
- The development of a system that will utilize the Steganographic methods on incoming and email messages and attachments.
- Audio as well as video steganography.

VI. ACKNOWLEDGEMENTS

The authors would like to thank all the authors mentioned in the references as well as other authors for their earlier work on this topic. Their earlier work helps a lot for this review paper to complete.

REFERENCES

[1] Lynch St., Jackson, USA. Luis von Ahn and Nicholas, "An Overview of Image Steganography" Carnegie Mellon University, Pittsburgh, USA.

[2] Abhishek Koluguri, Sheikh Gouse, Dr. P. Bhaskara Reddy, "Text Steganography Methods and its Tools", International Journal of Advanced Scientific and Technical Research, Issue 4 volume 2, March-April 2014.

[3] Takashi Mihara , "A New Framework of Steganography Using the Content of Cover Data", Journal of Information Hiding and Multimedia Signal Processing, Volume 5, Number 2, April 2014.

[4] Swati Nimje, Amruta Belkhede, Gaurav Chaudhari, Akanksha Pawar and KunaliKharbikar, "Hiding Existence of Communication Using Image Steganography", International Journal of Computer Science and Engineering, Volume-2, Issue-3, March 2014.

[5] R. Rejani, D. Murugan and Deepu V. Krishnan, "DIGITAL DATA PROTECTION USING STEGANOGRAPHY", ICTACT JOURNAL ON COMMUNICATION TECHNOLOGY, MARCH 2016, VOLUME: 07, ISSUE: 01.

[6] Book- Cryptography and network security, forth edition by William Stallings.

[7] Book- An overview of image seganography by T. Morkel, J. H.P. Eloff, M. S. Olivier.

[8] XuejingNiu, Meng Ma, Rui Tang and Zhaoxia Yin, "Image Steganography via Fully Exploiting Modification Direction", International Journal of Security and Its Applications, Vol. 9, No. 5 (2015), pp. 243-254.