Scientific Journal Impact Factor (SJIF) : 5.278
International Journal of Modern Trends in Engineering and Research
IJMTER
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Design and implementation of Data Hiding Technique by using LSB Replacement Algorithm

Ramakrishna Hegde [1], Dr.Jagadeesha S[2], Soumyasri S M[3]
Dept. of Computer Science & Engineering , SDM Institute Of Technology, Ujire
Dept. of Electronics & Communication Engineering, SDM Institute Of Technology, Ujire

Abstract: Steganography is the efficient technique to provide secure data transmission over the network, as the number of users increases effectively. The cryptography is also used to provide security to data over network, but transmission of secured message may be detectable to third party. From security point of view, steganography does not allow to detect the presence of hidden secret other than indeed user, over the communication channel. Here we are implementing the image steganograpgy i.e image as the master file or cover media and secrete message can be text messages. This paper presents to provide the transfer of secret data embedded into master file to obtain new image , which is practically indistinguishable from the original image, so that other than the indeed user, cannot detect the presence of the secrete data sent. Here we use the Least Significant Bit (LSB) algorithm for hiding the secrete data by embedding the secrete data into a master file in sending station and we use reverse process of LSB during the retrieval of the secrete data from the master file by the intended user. Embedding Capacity should be measured as performance characteristics of the steganography.
Keywords: Steganography, Peak Signal to Noise Ratio, Cover media, Master file, Least Significant Bit

I. INTRODUCTION

STEGANOGRAPHY is the art of secure communication where the existence of the communication itself cannot be detected while steganalysis is the art of detecting the secret communication. The requirements for a "good" steganographic scheme are a high embedding capacity, while remaining statistically secure. When there is an active adversary in the transmission channel, the hiding scheme is considered to be an example of "active steganography." Various examples of the active warden scenario (active steganography) are in [1], [2], [3],. It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-media. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data[4].

As people become aware of the internet day-by-day, the number of users in the network increases considerably thereby, facing more challenges in terms of data storage and transmission over the internet, for example information like account number, password etc. Hence, in order to provide a better security mechanism, we propose a data hiding technique called steganography. In cryptography, the secret message that we send may be easily detectable by the attacker. But in steganography, the secret message is not easily detectable. The persons other than the sender and receiver are not able to view the secret message.
Steganography differs from cryptography[3]

- Steganography Hide the messages inside the Cover medium,Many Carrier formats.

- Breaking of steganography is known as Steganalysis.

Cryptography

- Encrypt the message before sending to the destination, no need of carrier/cover medium.
- Breaking of cryptography is known as Cryptanalysis.

Cryptography is used in many applications. Historically, cryptography was used to assure only secrecy. Wax seals, signatures, and other physical mechanisms were typically used to assure integrity of the media and authenticity of the sender. With the advent of electronic funds transfer, the applications of cryptography for integrity began to surpass its use for secrecy. Electronic cash came into being from cryptography, and the electronic credit card and debit card sprung into widespread use. The advent of public key cryptography introduced the possibility of digital signatures, and other related concepts such as electronic credentials. In the information age, cryptography has become one of the major methods for protection in all applications.

Watermarking and fingerprinting related to steganography are basically used for intellectual property protection. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. The embedded information in a watermarked object is a signature refers the ownership of the data in order to ensure copyright protection. In fingerprinting, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the property owner to find out such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other. Figure 1 shows the steganography in the internet.

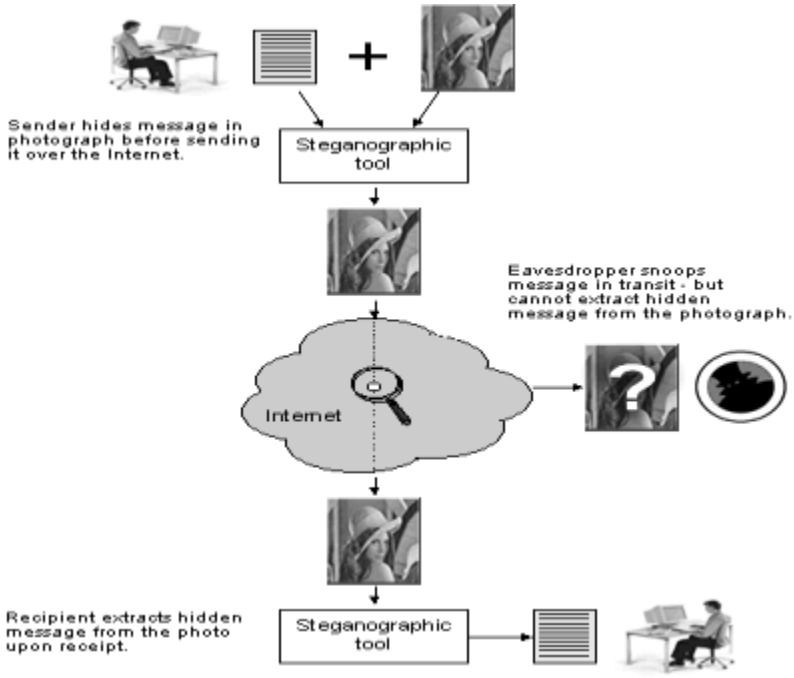

Figure 1: Steganography in the Internet.

II. RELATED WORK

The basic idea behind the steganography is to hide the secrete data into the carrier file and send it to the other party over the network. The carrier files may be text, image, audio or

video. Practically in most of the cases images are taken as the carrier file. Because the digital images are very useful and secure carrier for hiding the secret massage. Image is a collection of color pixels. In standard, 24 bit bitmap we have three color components per pixel: Red, Green and Blue. Each component is 8 bit and have 256 values. In 3 megapixel image we can hide 9 megabits of information using this technique, which is equivalent of 256 pages of book. If we only change the lowest bits of each pixel, then the numeric values can only change by a small percentage. We can only alter the original pixel color value by ±7. Such a minute alterations in the pixel value does not make any difference in the visibility of the image. The original image and embed image both looks similar to the human eye. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it

For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. The research paper [5] gives an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications. The paper [6] explains that, Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us. It is also possible to simply use steganography to store information on a location. Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data. Invisible ink has been in use for centuriesfor fun by children and students and for serious undercover work by spies and terrorists [7].

Hiding information into a medium requires following elements [8]

1. The cover medium(C) that will hold the secrat message.
2. The secret message (M), may be plain text, digital image file or any type of data.
3. The stegonographic techniques
4. A stego-key (K) may be used to hide and unhide the message.

In modern approach, depending on the cover medium, steganography can be divided into five types: 1. Text Steganography 2. Image Steganography 3. Audio Steganography 4. Video Steganography 5. Protocol steganography.

- **Text steganography** Hiding information in text _le is the most common method of steganography. The method was to hide a secret message into a text message.
- **Image steganography** Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key.
- **Audio steganography** Audio steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. The different methods that are commonly used for audio steganography are LSB coding, Parity coding, Phase coding, Spread spectrum, Echo hiding.
- **Video steganography** Video Steganography is a technique to hide any kind of files in any extension into a carrying Video file.

- **Protocol steganography** The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used. [9].

III.METHODOLOGY

3.1 Network:

A Network is a set of devices (often referred to as nodes) connected by media links. A node can be a computer capable of sending and/or receiving data generated by other nodes on the network. The links connecting these nodes are often called communication Channels.

3.2 Least Significant Bit (LSB) Techniques

The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden. A stego-image is obtained by applying LSB algorithm on both the cover and hidden images. The hidden image is extracted from the stego-image by applying the reverse process[10

Figure 3.1 shows LSB insertion algorithm. Figure 3.2 shows LSB extraction mechanism. .

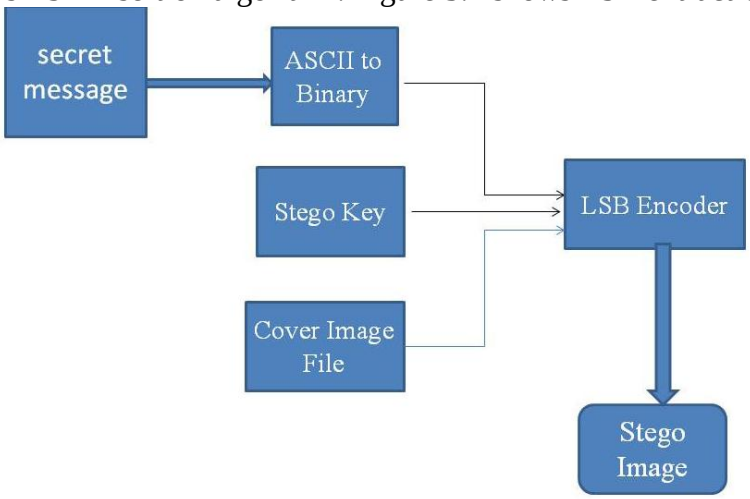

Figure 3.1 LSB Insertion Mechanism

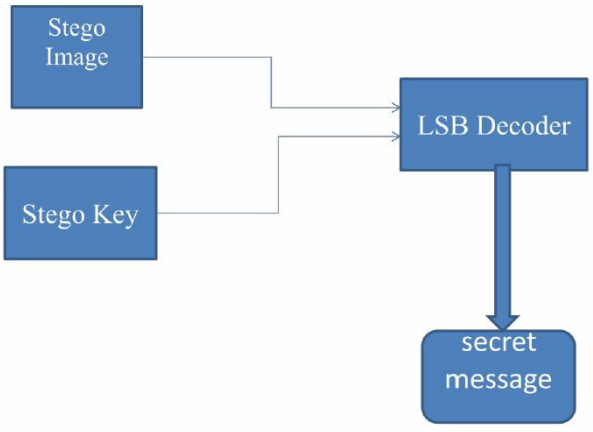

Figure 3.2 LSB Extraction Mechanism.

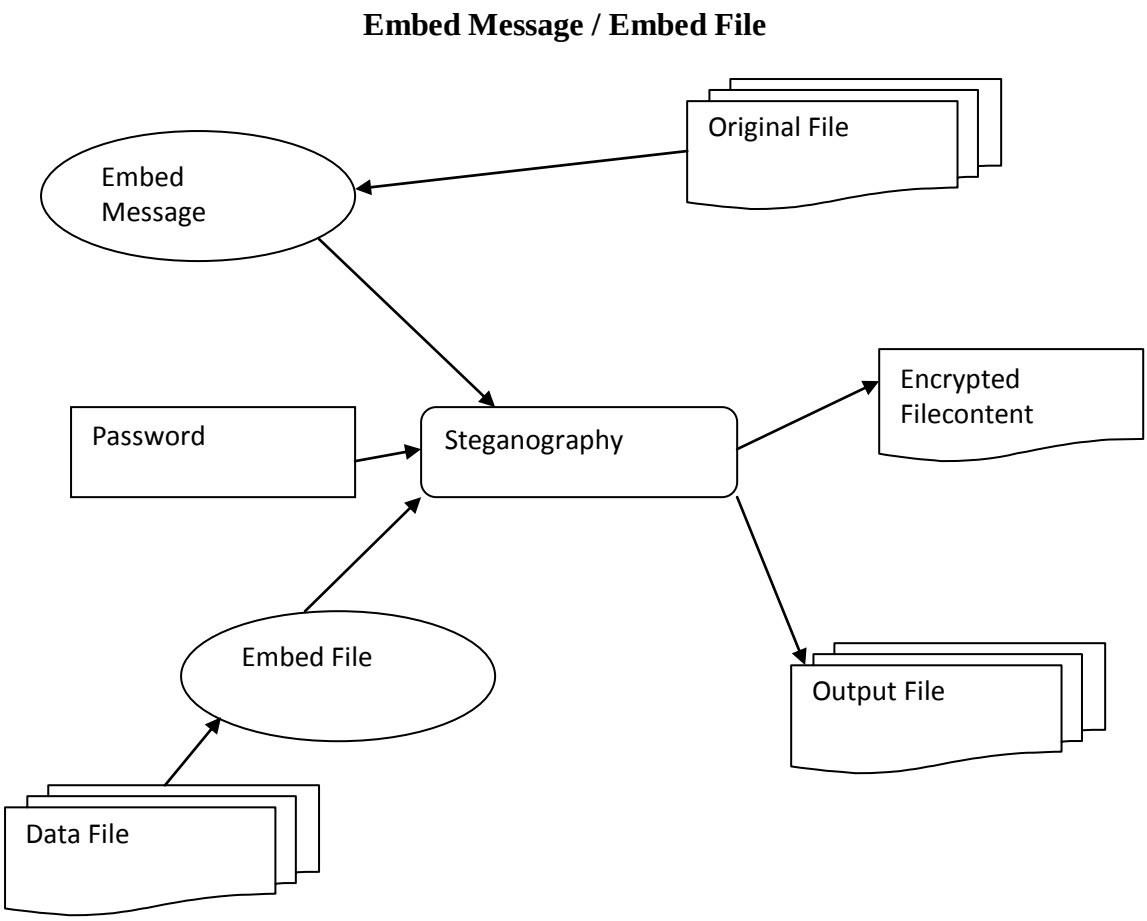

Figure 3.3 DFD of Embed message / Embed file

LSB insertion algorithm

Step1: The first character of the data to be hidden is taken and represented in binary format.

Step2: Next the first pixel value of the video is taken and represented in binary format.

Step3: The converted data is extracted bit by bit from the least bit. (i. e the order of left to right)

Step4: For each bit we are appending or prefixing zeros to make it a 1 byte.

Step5: After appending the zeros, if the value of that byte is 0, then we represent it as 2 (i.e. change the value to 2), if its 1 then we don't do any changes.

Step6: Next we take the pixel value if the pixel value is 255 or 256 then we subtract the value of the data with the pixels. If not then we add.

LSB Extraction algorithm (Reverse LSB)

Step1: The first value of the keyfile and the first pixel value of the steganographed video file are taken.

Step2: Next we subtract the two values that are extracted and store it in a temp array.

Step3: Step 1 and step 2 is repeated till the end of the file.

Step4: The temp file is opened and then every continuous 8 bytes are taken and they are clubbed to make them as 1 byte using the left shift operator.

Step5: The extracted byte is converted into character format and stored in a data file

Figure 3.2.1 and 3.2.2 explains the LSB insertion and LSB extraction mechanisms.

Retrieve Message/Retrieve File

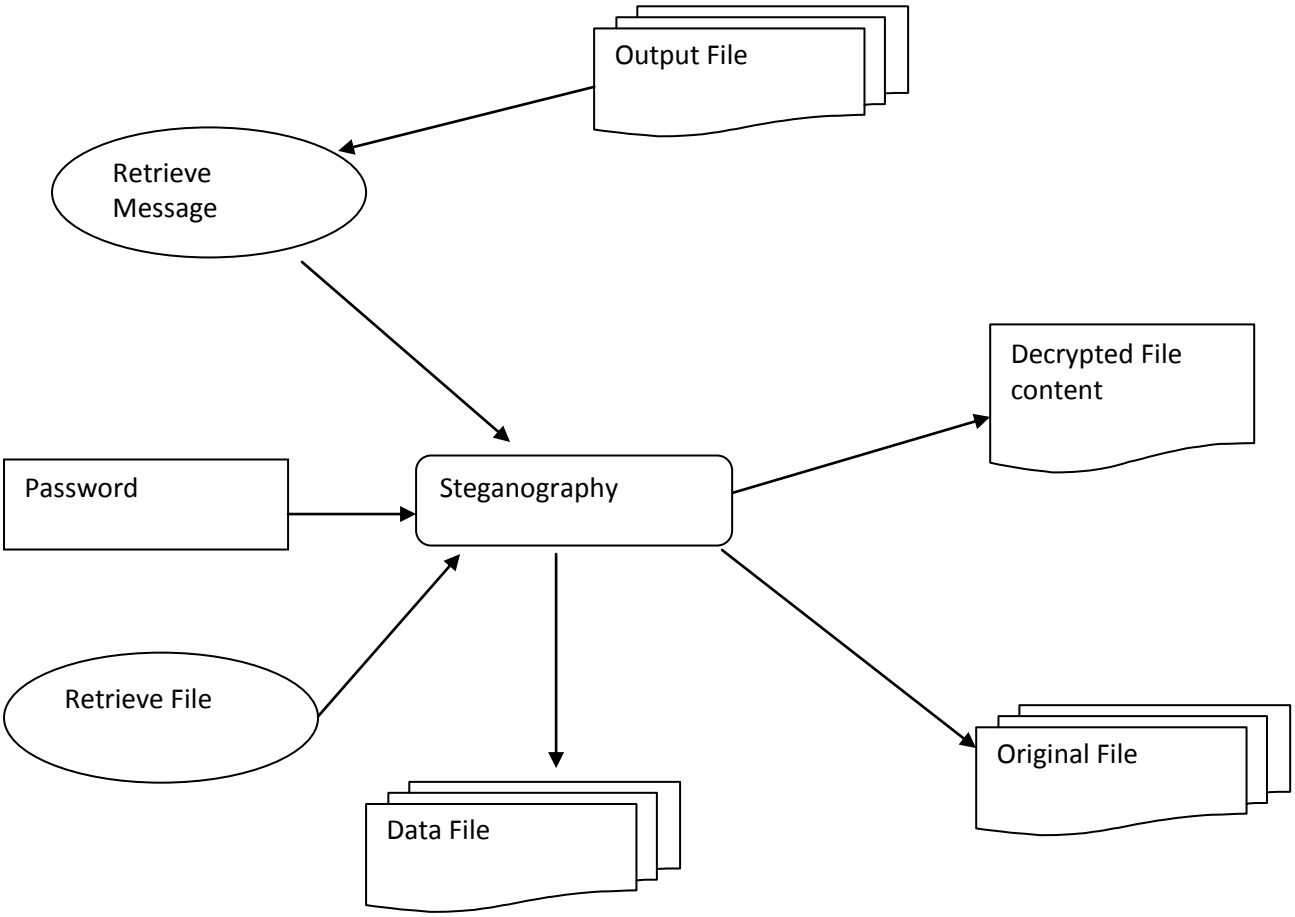

Figure 3.4 DFD of Retrieve Message / Retrieve File

Send/Overlap

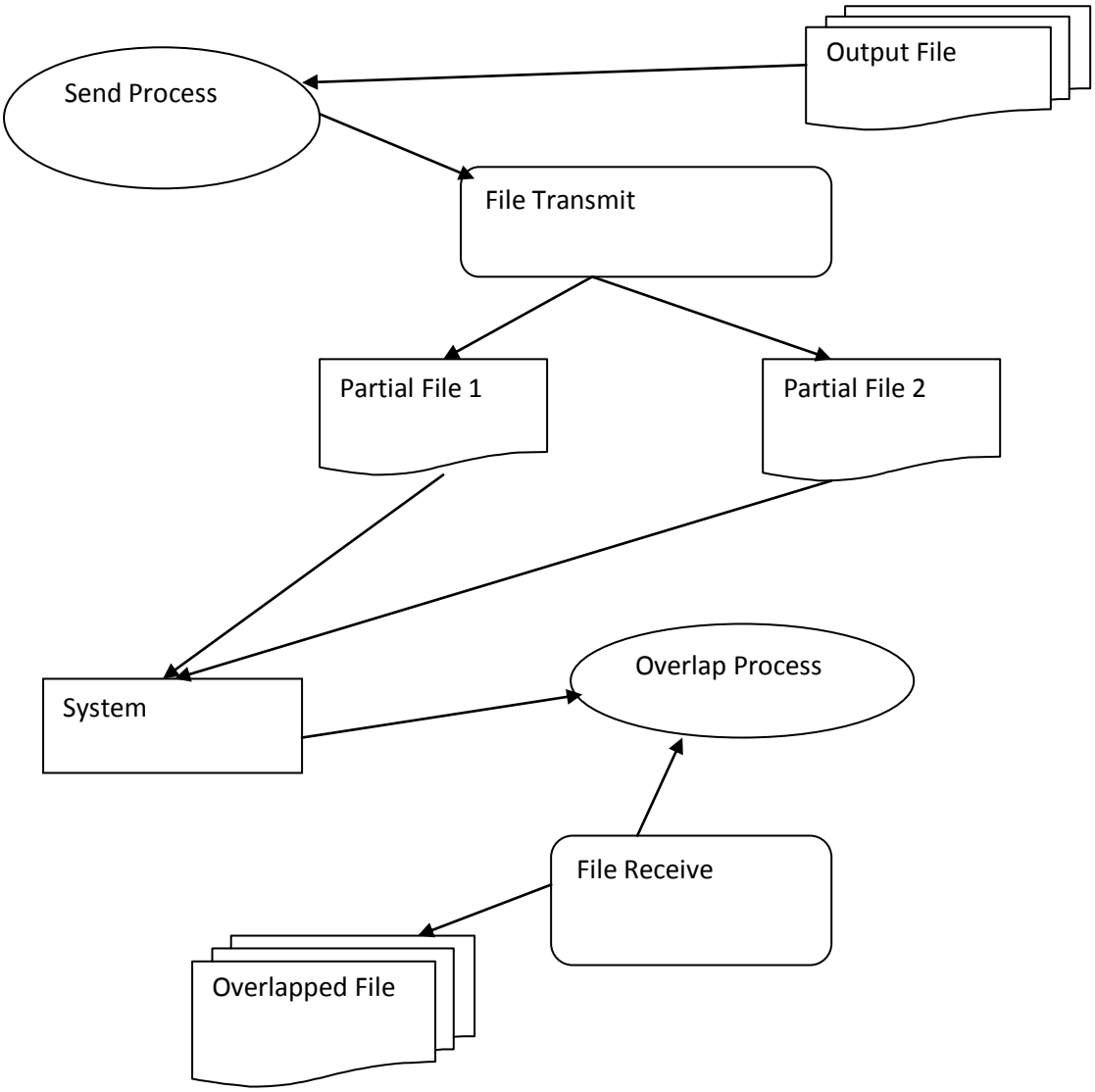

Figure 3.5 DFD of Send / Overlap

Figure 3.3, 3,4 and 3.5 shows the Data Flow Diagrams of Embed Message, Retrieve Message and Send respectively.

IV.EXPERIMENTAL RESULTS

4.1 Performance Analysis

There are several parameters are used to measure the performances and some of them are explained below.

Perceptibility: It does embedding information distort cover medium to a visually unacceptable level.

Embedding Capacity : How much secrete data can be hidden.

Robustness to attacks: It is attack on the stego medium in an effort to destroy, remove, or change the embedded data.

Table 4.1 Characteristics in the above two techniques.

Technique	Imperceptibility	Embedding Capacity	Robustness
LSB algorithm	High*	50-60%	Low

***** Indicates depends on the used cover image.

Figure 4.1 Grey Scale Image (Cover media)

Figure 4.2 RGB Image. (Cover media)

We consider grey scale and RGB image as cover media (before the embedding of the secrete message) as shown in figure 4.1 and 4.2 respectively. Text file / image taken as secrete message for both the techniques. Figure 4.3 and Figure 4.4 are the grey scale image with text file and RGB image with text file respectively. By referring the Figures from 4.1 to 4.4, we notice that human eyes cannot distinguish images before embedding the secrete message and after embedding the secrete message.

Figure 4.3 Grey Scale image with text file

Figure 4.4 RGB image with text file

It is possible to embed more secrete information into the RGB image compare to the grey scale images. PSNR of RGB image with text file as secrete message is more than the grey scale image with text file and distortion rate is also less in RGB images.

V. CONCLUSION

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. In areas where cryptography and strong encryption are being outlawed, citizens are looking at steganography to circumvent such policies and pass messages covertly. Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate. In this project we have used steganography and cryptography both.

In this paper, we have used Least Significant Bit (LSB) algorithm and for steganography. The secrete text message is embedded successfully with the master file (carrier file) and transmitted to intended user. Image file can be used as master file. And also we successfully embedded the data file with the master file and transmitted to intended party. The secrete text message or secrete data file is retrieved back by the intended user from the master file. The negligible changes in the master file after embedding the secrete text message or secrete data file cannot identify by the human beings. Our results shows that Embedding Capacity is varies from 50% to 60% .

REFERENCE

[1] M. Backes and C. Cachin, "Public-key steganography with active attacks," in *Proc. Theory of Cryptography Conf.*, 2005, vol. 3378, pp.210–226, Springer.
[2] S. Craver, "On public-key steganography in the presence of an active warden," in *Proc. Second Int. Information Hiding Workshop*, pp.355–368, Springer.
[3] G. Fisk, M. Fisk, C. Papadopoulos, and J. Neil, "Eliminating steganography in Internet traffic with active wardens," in *Lecture Notes in Computer Science*, 2003, pp. 18–35.
[4] Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE computer society,2003
[5] T. Morkel 1, J.H.P. Eloff 2, M.S. Olivier 'AN OVERVIEW OF IMAGE STEGANOGRAPHY', Information and Computer Security Architecture (ICSA) Research Group. Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa.
[6] Arvind Kumar Km. 'Steganography- the data hiding technique', *International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.*
[7] "A Tutorial Review on Steganography" by Samir K Bandyopadhyay, Debnath Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das, Heritage Institute of Technology.
[8] Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE computer society,2003.
[9] Pratap Chandra Mandal Asst. Prof., Department of Computer Application B.P.Poddar Institute of Management Technology . "Modern Steganographic technique: A Survey" , International Journal of Computer Science Engineering Technology (IJCSET).
[10] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). "Digital image steganography: survey and analysis of current methods." Signal Processing Journal.
[11]"A Tutorial Review on Steganography" by Samir K Bandyopadhyay, Debnath Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das, Heritage Institute of Technology.
[12] International journal of computer engineering technology (ijcet) "steganography based on random pixel selection for efficient data hiding'.Shamim Ahmed Laskar and Kattamanchi Hemachandran (Research Scholar, Department of Computer Science, Assam University).
[13] Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1. A steganography algorithm for hiding image in Image by improved lsb substitution by minimize Detection by vijay kumar sharma, 2vishal shrivastava M.Tech. scholar, Arya college of Engineering IT, Jaipur , Rajasthan (India).