A SURVEY ON IMAGE STEGANOGRAPHY USING LSB SUBSTITUTION TECHNIQUE

Beenish Siddiqui[1], Sudhir Goswami [3]

[1]*Student, Department of CSE, M.tech, Meerut Institute of Engg. & Technology, Uttar Pradesh, India.*
[2]*Associate Professor, Department of CSE, Meerut Institute of Engg & Technology, Uttar Pradesh, India.*

---***---

Abstract: *Information security is one of the believable areas of research now-a-days. Steganography plays a shiny role in the information security. Its main aim is to covering sensitive information within a host such that the information existence remains confidential. By embedding secret message within other file steganography plays an important role of hiding messages for security purpose. The least significant bit (LSB) is one of the most important and simple method when one want to solve such problems. In this method, a number of bits of LSB is directly replaced by each pixel of the cover image with the embedded message. This paper describes the various techniques using the LSB substitution method to hide the data in images. Image steganography hides the data efficiently and effectively with the help of LSB substitution methods.*

Key Words—image steganography; cover image; stego image; Simple LSB substitution; Optimal LSB technique;

1.INTRODUCTION

The fast development of the Internet deals great struggles to the transmission of secret data over networks. Secret data is candidate to unauthorized access. Therefore, to transmit the data secretly through internet becomes an essential topic. To keep the unauthorized user away, many different approaches have been proposed. To secure communication, Encryption and data hiding are two major methods in steganography.

The method of changing the data (plaintext) into a cipher text via cipher algorithms and form the secret message, is called Encryption process. The secret message can be decrypted from the cipher text by the user that has keys, as shown in Figure 1. For any unauthorized user, this cipher text look like a meaningless and unreadable code until the user does not have a key. The data encryption still has some weaknesses although it is a respectable way to secure data. It makes the messages suspicious enough and streams of meaningless to attract unauthorized attention and give an impulse to recover them. Moreover, when the unauthorized users have trouble recovering the cipher text out of range, they might simply destroy them so that the authorized users cannot get the data in time. That is the reason why data hiding is a hot topic and has been under consideration of researcher recently [1] and [2]

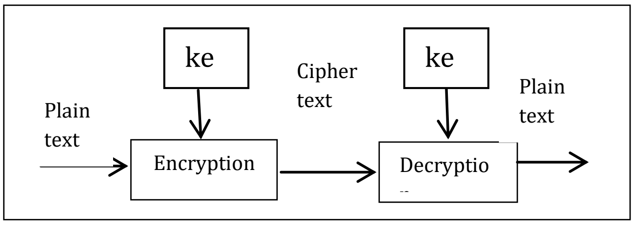

Figure-1: Simplified Model of Conventional Encryption.

Hiding the secret data into multi-media data such as sounds, images or videos is called data hiding technique. Three different aspects contend with each other characterize the techniques as shown in Figure 2: capacity, robustness, and security. The amount of data bits that can be concealed in the cover medium relative to the size of the cover is called capacity . This is measured in bits per pixel (bpp), robustness is the capability of the stego medium to continue intact and resist the modification before an eavesdropper can modify or destroy the hidden data, and security concerned about the ability.

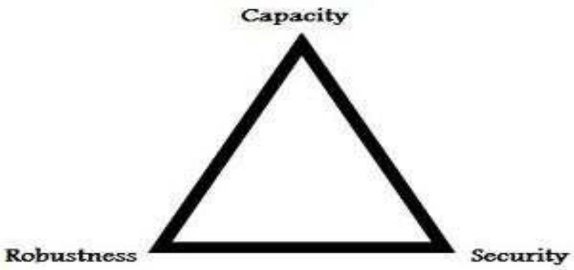

Figure- 2: features of information-hiding system [3]

steganography is the technique used to hide the existence data in different format such as text, images, audio, video etc.The Greek words steganos and graphia are the radix of the word Steganography and it means" hiding writing" [4]. The main aim of steganography is to hide a message from a third party by secret communication. The cryptography differs from this in the manner that it does not hide the message like steganography, unlike it change the message and become the message unreadable to the third party or unauthorized users. Although steganography and cryptography are distinct and separate from each other, still there are some similarities between them, and some researchers define steganography as a type of cryptography since hidden communication is a type of secret writing [2]. Steganography uses audio, text, images, and video media for hiding data. The digital steganography technique has three basic components:

1. The data to be embedded is known as secret data.
2. The image or any medium which is used to hold the secret data is known as secret data.
3. The resulting image or any media which is using is known as stego-file (stego-carrier).

There are many techniques of steganography, image steganography is widely used technique compared to others because of its simplicity and an easiest way to conceal the data in images. The main purpose of this popularity is, the amount of data is more than enough existing in the images and can be altered easily to hide secret messages in them, and because it has a restricted power of the human visual system (HVS) [5]. In image steganography the cover image is known as the original image. The stego image is called the resultant which comes after embedding the secret bits into cover image that has no sense, and then the sender can transfers the stego image to the other side through a public channel. Whenever the cover image and the stego image are more similarities, it will be harder for an unauthorized person to obtain the stego image which the secret message embedded inside it. This way, the secret message can be transmitted from the sender to the receiver safely and soundly.

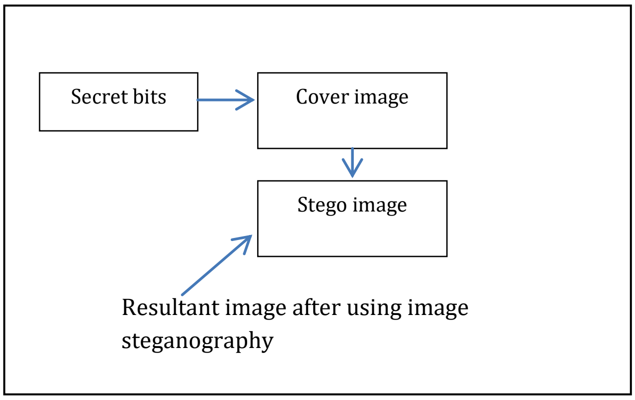

Figure-3: Image steganography

The powerful of the LSB method are simplicity of calculation and a large amount of data can be concealed in the original image with high visually.

2. RELATED WORK

Wang et al. [6] proposed an embedded technique in the moderately significant bit of the host image. A genetic algorithm is established to find optimal substitution matrix for embedding the secret messages. They also enhanced the stego-image quality by using local pixel adjustment process (LPAP).

Wang et al. [7] presented also a new method to hide data inside the cover-image. The basic concept of the method is carried out by the simple version of LSB substitution data hiding. They also solved the problem when k is large.

C.-K. Chan ans L.M. Cheng [8] proposed a data hiding method by the simple version of LSB substitution method. Low extra computational complexity based on an optimal pixel adjustment process is applied to the stego-image obtained by the simple LSB substitution scheme to improve the quality of the stego-image.

Wu and Hwang [9] presented some well-accepted schemes and classified them into two major types: high hiding capacities schemes and high stego-image degradation imperceptibility schemes. One of his methods called optimal LSBs method is a good choice for a large amount of data is to be hidden. On the other hand, two other methods called PVD and MBNS schemes which are superior to LSB-based schemes in terms of stego-image quality.

Marghny et al. [10] proposed a dynamic LSB substitution techniques by dividing the cover image into edge and smooth areas. This method can embed large amount of data as well as imperceptibility of stego image based on the pixel-value differencing for secret communication. Experimental results show that the proposed method can obtain a stego image with satisfactory quality. Moreover, it can resist steganalysis systems which are carried out by statistical analysis.

Marghny et al. [2] proposed a method for optimal key selection based on permutation method using genetic algorithms. The method is tested with varying data size as well as key space with different standard images. The experimental results show the improving of system security and decreasing of in computation time when the number of keys is increased.

Liao et al. [1] presented a novel method of steganographic to improve the multi-pixel differencing of LSB substitution to offer better stego-image quality and large amount of embedded message. Where, A four pixel blocks are considered with three difference values.

Marghny et al. [11] proposed a technique to embed secret message into the original image by a dynamic LSB substitution scheme. This scheme is carried out by utilizing the similarity in the smooth area not the edge area as in the simple techniques, and using the LSB substitution methods as a fundamental stage. This method increase the data capacity with preserving the quality of stego image.

Marghny et al. [4] propose an efficient steganographic method to embed message over gray scale images. This scheme is based on the nature of the human eye, which is more perceptive to the change in the smooth area than the edge area using pixel value difference, as well using the LSB substitution method as a fundamental stage. This method increased the capacity of embedding message, achieving the visual quality and more security.

In this paper, a method is proposed to increase the amount of capacity of embedding message and the quality of the stego-image based on LSB substitution scheme which embeds data by replacing k LSBs of a pixel in the cover image with k secret bits directly. A fixed number of LSB's is used. The cover image is divided into two parts and changing process is applied to the value of some bits that have the secret bits in the stego-image that are obtained by the simple form of LSB substitution technique. The experimental results on various standard images that evaluate the efficiency of the proposed method show that our method can embed a large amount of data than other methods and the quality of the stego image is enhanced as well.

The objective of this paper is showing the disadvantages of the previous LSB and enhancement scheme for steganography based on LSB substitution considering high capacity and high robustness, as well as system security. Presenting methods that improve data hiding method based on simple LSB substitution method.

3. DIGITAL IMAGE

A numeric representation of two dimensional images is called a digital image. Colour value or gray level is represented by each pixel (at a single point in image) of image and these values are for coloured and black & white images respectively. Picture elements i.e. pixels are collected and form a digital image.

Each pixel of colour image holds three numbers of corresponding to the red, green, blue levels of the image at a particular location. These three colours are also called RGB and are primary colours for mixing light. Here we can see in fig 1, when light falls on the LED screen it differentiate the primary colour RGB.

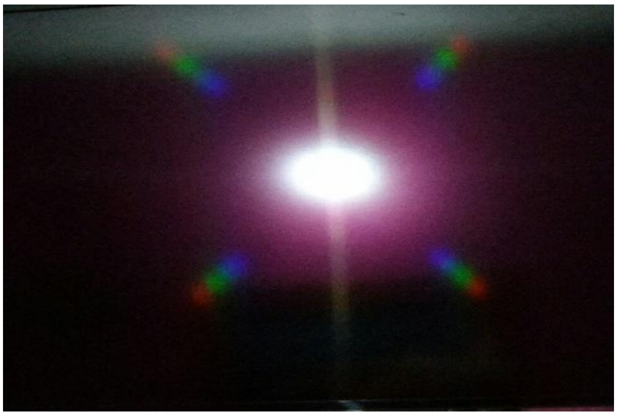

Figure-3: Differentiating light into RGB.

These colours so called primary are different from the subtractive primary colours used for mixing paints. Any colour can be created by mixing the correct amount of red green and blue light [12]. Assuming 256 levels for each primary colour, each colour pixel of image can be stored in 24 bits (3 bytes) of memory. This is corresponding to approximately 16.7 million different possible colours.

Bit depth is another technical term associated with each digital image. It refers to how many „bits" are used to store colour information in an image file. A bit is the smallest unit of information that a computer can store and it can have two values: 1 or 0. The higher the bit depth, the more accurately colours will be represented „bits" are used to store colour information in an image file [12].

4. AN OVERVIEW OF STEGANOGRAPHY

Steganography is used an important sub discipline of information concealing and cryptography is used for protecting the content of messages. Steganography efforts only covering their existence. This modern adaptation of steganography is usually interpreted as hiding information in other information [13].

The basic functioning of steganography is shown in Fig.4. Here sender hides the secret information in an image, known as cover image, with the help of a key. Image embedded with secret information, known as stego image, is transmitted over communication channel. At the other end, receiver extracts the hidden secret information with the help of the same key from the stego image. The medium used here to hide the secret information is digital JPEG image while it could be an audio, video and other file format.

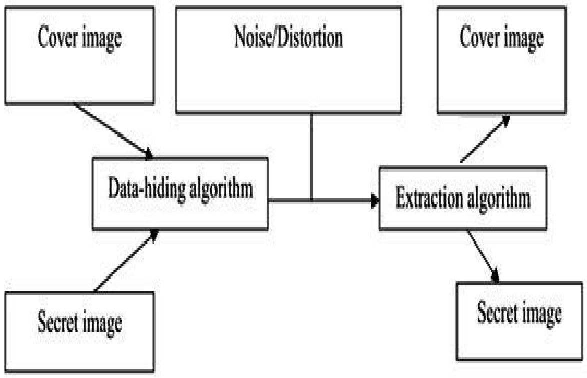

Figure-4: Image Steganography System

There are three basic techniques which are generally used for steganography [14].

4.1 Injection

Hiding the data in sections of a file that is ignored by the processing application. Therefore avoid modification of those bits in file that are relevant to end-user and leaving the cover file perfectly usable.

4.2 Substitution

In this method, least significant bits of information that determine the meaningful content of the original file can be replaced by the secret data or secret bits in a way that causes the least amount of distortion.

4.3 Generation

In this it generates a cover file for the sole purpose of concealing the message unlike injection and substitution, this does not require an existing cover file.

We have used the substitution method with the help of LSB. LSB approach does fewer changes in bit pattern; therefore it alters the cover image to minimum [16]. The size of secret information embedded in it lesser than other methods, which is one of the limitations of this approach. Simple LSB approach is extremely vulnerable to attack. LSB techniques implemented on 24 bit formats are difficult to detect contrary to 8 bit format. All algorithms employed for any type of format have pros and cons. They also depend upon the environments used for the information to be embedded.

5. DATA HIDING BY SIMPLE LSB SUBSTITUTION

The most common and easiest steganography technique is LSB method. In this method, a number of bits of the least significant bits(LSB) is directly replaced by each pixel of the cover image with the embedded message. However, this method suffers from some problems as many steganograpic schemes. Noticeable the problem is produced by simple LSB substitution is distortion .

This means that the quality of stego image may be not suitable and perhaps attracts illegal attention.
LSB substitution method can be understood by the example shown here, suppose we have the following pixels in the image: $P1$ = [10011011], P_2 = [01101010], P_3= [11001100], and the secret bits are M = [011], and the resulted pixels after embedding the secret bits are P_1 = [10011010], P_2 = [01101011], P_3= [11001101]. So the LSB method has the following conditions [4]:

- Due to its simplicity the LSB becomes vulnerable to security attacks.
- Increasing the amount of secret data in each pixel implies to more visual degradation in the quality of the image.
- The image histogram becomes noticeable Due to its uniform distribution of the secret message.

6. THE OPTIMAL LSBS TECHNIQUE

Many authers has been has enhanced the simple LSBs methods. One of the enhanced method called the optimal LSBs method. In this method image quality of the stego image is improved by applying an optimal pixel adjustment process.

To obtain the neighboring one to the original pixel value with the secret data, three nominees are selected from the pixels and matched [17]. Best nominee is the optimal pixel and is used to hide the secret data. The following steps describe the embedding algorithm:
Suppose P_i is the corresponding pixel values of the ith Pixel in the cover image C and $k\ bit(s)$ of embedded message.
Use the LSBs method to embed $k\ bit(s)$ into P_i.Then the stego-image P'_i can then be obtained.
By adjusting the $(k$+1)th bit of P'_i another two pixel values P'_+ and P'_- will be generated as follows:

$$(P'_+, P'_-)=\begin{cases} P'_+ = P'_i + 2^k \\ P'_- = P'_i - 2^k \end{cases} \qquad (1)$$

The last bits of P'_+ and P'_- are the same, so the hidden data in P'_+ and P'_- are identical pixel value P''_i can be found by the following formaula:

$$P''_i = \begin{cases} P'_i \ \ if\left|P_i - P'_i\right| \le \left|P_i - P'_-\right| \le \left|P_i - P'_+\right| \\ P'_i \ \ if\left|P_i - P'_+\right| \le \left|P_i - P'_i\right| \le \left|P_i - P'_-\right| \\ P'_i \ \ if\left|P_i - P'_-\right| \le \left|P_i - P'_-\right| \le \left|P_i - P'_+\right| \end{cases} \qquad (2)$$

The embedding algorithm comes to its end by replacing the optimal candidates P''_i by the original pixel values P''_i. To explain that the distortion in the simple form of LSBs technique can be decreased by the optimal LSBs method, we present the following example:
Suppose P_i = 9, k = 3, and the three bits of embedded message are 110. Then, by using the simple 3-LSBs method, the stego-image P'_i = 14 is obtained. After adjusting the 4-th bit of P'_i , another two pixel values P'_+= 22 and P'_-= 6 can be obtained. The pixel values of last three bits P'_i=14, P'_+= 22, P'_-= 6 are the same. However, the optimal candidate is $P'_- = 6$ because it is the most closest one to the original pixel value P_i = 9. This example observes that the quality of the stego-image can be significantly improved by using the optimal LSBs
method. observes that the quality of the stego-image can be significantly improved by using the optimal LSBs method.

7. CONCLUSION

The most challenging and important task is data hiding in the field of information security. In this paper we discuss about the digital image, an overview of steganography and varios techniques of steganography. We can propose a new approach based on Discret Wavelet Transform using NSGA (Non Dominated Sorting Algorithm) for better quality of stego image.

REFERENCES

[1] X. Liao, Q.Wen and J. Zhang,"A steganographic method fordigital images with four-pixel differencing and modified LSBsubstitution", Journal of Visual Communication and ImageRepresentation, vol 22, no 1, pp. 18, 2011.

[2]M. H. Marghny, F. Al-Afari and M. A. Bamatraf, "Data Hiding by LSB Substitution Using Genetic Optimal Key- Permutation", International Arab Journal of e-Technology, Vol.2, No.1, 2011.

[3] E. Lin and E. Delp,"A Review of Data Hiding in DigitalImages", in Conference on Image Processing, Image Quality,and Image Capture Systems, PICS, pp. 274-278, 1999.

[4] M. H. Marghny, N. M. AL-Aidroos and M. A. Bamatraf, "Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference", International Journal in Foundations of Computer Science & Technology, vol. 2, no. 6, pp. 1-13, 2012.

[5]M. Al-Husainy, "A New Image Steganography Based onDecimal-Digits Representation, Computer and InformationScience", vol. 4, no. 6, pp. 38-47, 2011.

[6] R.-Z. Wang, C.-F. Lin and J.-C. Lin, "Hiding data in images by optimal moderately significant-bit replacement", IEE Electron. Lett , vol.36, no. 25, pp. 2069070, 2000.

[7] R.-Z. Wang, C.-F. Lin and J.-C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recognition, vol. 34, no. 3, pp. 671683, 2001.

[8] R.-Z. Wang, C.-F. Lin and J.-C. Lin, "Hiding data in imagesby optimal moderately significant-bit replacement", IEE Electron. Lett , vol.36, no. 25, pp. 2069070, 2000.

[9] R.-Z. Wang, C.-F. Lin and J.-C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recognition, vol. 34, no. 3, pp. 671683, 2001.

[10] N. M. AL- Aidroos, M. H. Marghny, and M. A. Bamatraf,"Data Hiding Technique Based on Dynamic LSB", Naif Arab University for Security Sciences.

[11]M. H. Marghny, N. M. AL-Aidroos, and M. A. Bamatraf "A Combined Image Steganography Technique Based on Edge Concept & Dynamic LSB." International Journal of Engineering Research and Technology, Vol.1, No. 8, ESRSA Publications, 2012.

[12] Sudhir Goswami, Jyoti goswami, Rajesh Mehra, " An Efficient Algorithm Of Steganography Using JPEG Colored Image" IEEE International Conference on Recent Advances and Innovations in Engineering(ICRAIE), May09-11-14,Jaipur India

[13] FIPS. 46-3, „"Data Encryption Standard," Federal Information Processing Standard (FIPS), Publication 46-3, National Bureau of Standards, US. Department of Commerce, Washington D.C. October 25, 1999.

[14] Delahaye, J. P. ; "Embeddeed Information, Information Hiding", *Scientific American*, pp.142-46, 1996.

[15] T. Morkel, J. H. P. Eloff, M. S. Olivier, "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of CS, Universitof Pretoria, SA

[16] Denning, Dorothy E. Information Warfare and Security. Boston, MA: ACM Press, 1999, pp. 310-313.