International Journal of Research in Advent Technology, Vol.2, No.4, April 2014

E-ISSN: 2321-9637

Data Security Using Cryptography and SLSB Algorithm

Suraj J. Warade[1], Pritish A. Tijare [2], Swapnil N. Sawalkar[3]
M.E (Pursuing)[1], Associate Professor[2], Assistant Professor[3]
Computer Engineering[1], Computer Science and Engineering[2,3]
Sipna C .O. E. T, Amravati, India[1,2,3]
surajwarade@hotmail.com[1]

Abstract- In the today's world transfer of data over the network increases tremendously. So, the security of data is very important for secure communication. The Steganography is a technique in which the data is hidden in the multimedia content like image, audio, video. The Cryptography alone is not sufficient for securing the data. So, in this paper we use the concept of data security using cryptography along with Steganographic SLSB algorithm.

Index Terms - ***Steganography; LSB; SLSB; Data Security; Cryptography.***

1. INTRODUCTION

With the vast use of internet for communication the most important factor is security of information from sender to receiver. Cryptography the technique which converts the data into unreadable form i.e. it scrambled the original message, the process is known as encryption [1]. There are number of well known algorithms are available for encrypting and decrypting the message. Like

- Data Encryption Standard (DES)
- Blowfish Algorithm
- Advanced Encryption Standard (AES)
- Deffie Hellman.
- RSA. Etc

But it cannot assure the complete protection because the scrambled message may available at the eve's dropper and by trying several attacks it may get the original message [2]. The Cryptography keeps the message secret but sometime it is not sufficient to keep only data secret. So, at that time the concept of Steganography is useful.

Steganography is a technique which hides data inside other data. The difference between Cryptography and steganography is cryptography keep the message secret and steganography keeps the existence of the message secret [3]. The aim of both Cryptography and Steganography is keep the data safe from unwanted parties. So, for providing the Complete Security to the data we are using the concept of two layer of security i.e. Cryptography along with Steganography. Here in this paper we are using the Steganographic SLSB (Selected Least Significant Bit) algorithm for hiding the secret message inside the image.

2. PROPOSED WORK

Neither Cryptography nor Steganography alone can provide the data security efficiently. So, better way for securing a data by combining both the technique. Advantages of both techniques combined will provide the better security. First the secret message(Plain Text) which has to be send to the other party is encrypted by using suitable cryptographic algorithm, then take encrypted text and carrier image in which data should be hide. The SLSB algorithm is applied on the encrypted text and carrier image. After applying SLSB algorithm we get the stego image which carrying the encrypted message.

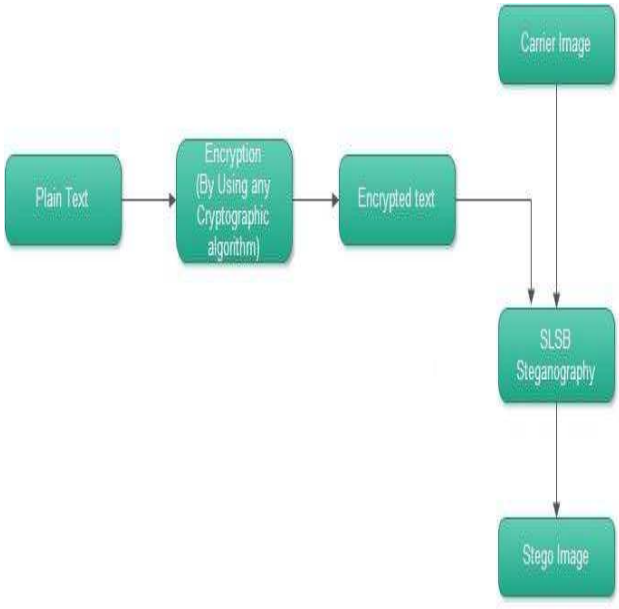

Figure 1: At Sender site

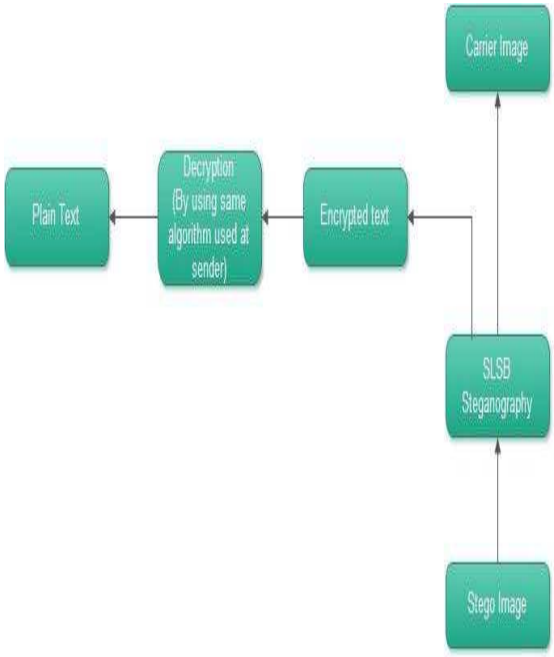

Figure 2: At Receiver Site

At the receiver site exact opposite procedure done for decryption of the message. The stego image is taken as an input and by applying SLSB algorithm separates the encrypted text and carrier image. After separation, the same cryptographic algorithm should apply on encrypted text for the decryption i.e. to get the secret message (plain text).

3. SLSB ALGORITHM

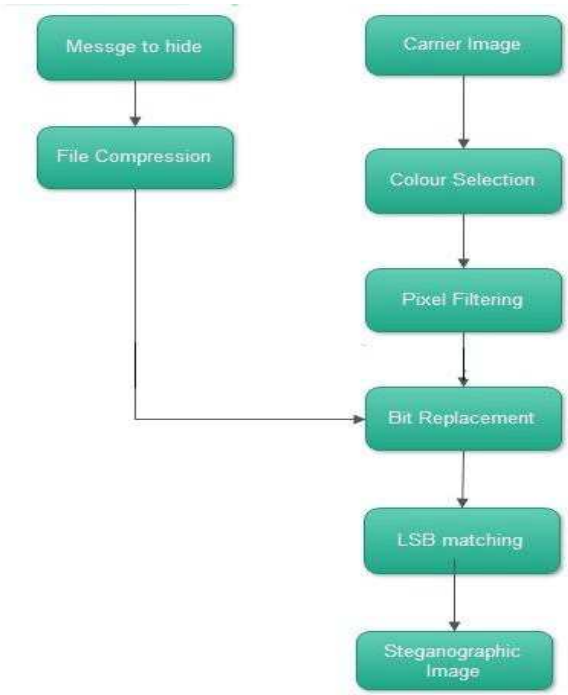

Figure 3: Structure of SLSB algorithm [4][5].

The SLSB is the spatial domain filtering Steganography algorithm. Spatial domain algorithms are simpler and faster [4][5]. Most of the spatial domain algorithms use the LSB method or some of its derivatives. SLSB (Selected Least Significant Bit) is improves the performance of the recently most popular algorithm for data hiding LSB (Least Significant Bit).

The LSB algorithm hide single bit of information in least significant bit of each color pixel. But this method is not effective when the Statistical Analysis like Sample Pair [6], Reed Soloman Analysis [7] is applied. When we are updating three colors of a pixel then the large distortion is occurs in the resulting image.

The SLSB hides the data in only one of three (Red, Green, Blue) colors at each pixel of the carrier image. For choosing the color to hide a data, SLSB algorithm performs the sample pair analysis and selects the color with higher ratio because it shows higher diversity. The choice of sample pair analysis in LSLB algorithm is because of the work of ker[8][9] in the field of hidden data detection. If we uses the sample pair analysis technique the color chosen with greater distortion and when we hide data in that area is less detectable.

The following examples shows how the distortion is minimize using LSLB algorithm.

Ex.1) If the pixel of the carrier image are(Red-Green-blue) 9E8C7A. In Binary 10011110-10001100-01111010 and we have to hide a message 111.

By LSB Algorithm:

It hides the each 1 bit into the least significant bit of each color pixel i.e. 10011111**1**-10001100**1**-01111001**1**

	Hexadecimal	Decimal	Red	Green	Blue
Original Pixel	9E8C7A	10390650	158	140	122
Updated Pixel	9F8D7B	10456443	159	141	123

Table 1: Result obtained by LSB

The table shows the distortion between original and updated color are of 65793 color on color scale.

By SLSB Algorithm:

It hides the all data into a single color selected by the sample pair analysis i.e. 10011**111**-10001100-01111010. Here data hide into the Red color.

	Hexadecimal	Decimal	Red	Green	Blue
Original Pixel	9E8C7A	10390650	158	140	122
Updated Pixel	9F8C7A	10456186	161	140	122

Table 2: Result obtained by SLSB

The table shows the distortion between original and updated color are of 65536 color on color scale. This is less than LSB method.

Ex.2) If the pixel of the carrier image is (Red-Green-blue) A0B8C2. In Binary 10100000-10111000-11000010 and we have to hide a message 111.

By LSB Algorithm:

It hides the each 1 bit into the least significant bit of each color pixel i.e. 10100001-10111001-11000011

	Hexadecimal	Decimal	Red	Green	Blue
Original Pixel	A0B8C2	10533058	160	184	194
Updated Pixel	A1B9C3	10598851	161	185	195

Table 3: Result obtained by LSB

The table shows the distortion between original and updated color are of 65793 color on color scale.

By SLSB Algorithm:

It hides the all data into a single color selected by the sample pair analysis i.e. 10100000-10111**111**-11000010. Here data hide into the Green color.

	Hexadecimal	Decimal	Red	Green	Blue
Original Pixel	A0B8C2	10533058	160	184	194
Updated Pixel	A0BFC2	10534850	160	191	194

Table 4: Result obtained by SLSB

The table shows the distortion between original and updated color are 1792 color on color scale. This is much lesser than LSB method.

Ex.3) If the pixels of the carrier image are (Red-Green-blue) C4D5E6. In Binary 11000100-11010101-11100110 and we have to hide a message 111.

By LSB Algorithm:

It hides the each 1 bit into the least significant bit of each color pixel i.e. 11000100-11010101-11100111

	Hexadecimal	Decimal	Red	Green	Blue
Original Pixel	C4D5E6	12899814	196	213	230
Updated Pixel	C5D6E7	12965351	197	214	231

Table 5: Result obtained by LSB

The table shows the distortion between original and updated color are of 65537 color on color scale.

By SLSB Algorithm:

It hides the all data into a single color selected by the sample pair analysis i.e. 11000100-11010101-11100**111**. Here data hide into the Green color.

	Hexadecimal	Decimal	Red	Green	Blue
Original Pixel	C4D5E6	12899814	196	213	230

Updated Pixel	C4D5E7	12899815	196	213	231

Table 6: Result obtained by SLSB

The table shows the distortion between original and updated color is 01 color on color scale. This is much lesser than LSB method and nearly equals to original image.

As above three examples shows the technique of hiding data in only one color is more efficient than that of hiding data in all three colors by LSB algorithm.

The SLSB algorithm filters the carrier image by the default filter and hides the data in those areas gets better rate. The filter applied to MSB of every pixel and leave LSB to hide the data. The retrieval of data is ensures because the bits used for filtering are not changed, When there is need of data retrieval the same bits are get selected.

The distance between original color and steganographic color is calculated by the LSB match method[8] and if the difference is more than certain limit which decided by the number of bits hide, the color decremented to get color closer to the original[9]. This results into reduction of distortion by hidden data inside image [10].

4. ADVANTAGES USING SLSB ALGORITHM

(1) Although the concept of SLSB based on LSB it hides information effectively than LSB.
(2) Uses Sample Pair Analysis for selecting best color from the possible three for data hiding.
(3) Uses Pixel Selection Filter to select best area in image for hide the data.
(4) Uses LSB Match to decrease difference between original image pixel and steganographic image pixel [8][9].
(5) Resist to histogram comparison, as the frequency of steganographic image is nearly similar to original image.
(6) Resist to statistical analysis, as two colors for each pixel are unchanged. So, the final analysis ratio nearly similar to the original image.

5. CONCLUSION

In this paper the two layer security by Cryptography and SLSB Steganography algorithm are used to make the information secure. By combining two techniques it immune to many attacks. Due to use of SLSB algorithm the difference in the carrier image and the Steganographic image is negligible. We are using the Selected Least Significant Bit algorithm which is faster and reliable and compression ratio is moderate compared to other algorithm.

6. REFFERENCES

[1] Atul Kahate (2009), Cryptography and Network Security, second edition, McGraw-Hill.
[2] Ajit Singh, Swati Malik "Securing Data Using Cryptography and Steganography" IJARCSSE Volume3, Issue 5, May 2013.
[3] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Signicant Bit Algorithm" IJERA Volume 2, Issue 3, May-Jun 2012.
[4] G. Sumalatha, P. Madhuravani, " A Novel Steganographic Algorithm and Hashing to Improve Authentication using Mobile Phones". Special Issue of IJCSI Volume 2 Issue 1, 2012.
[5] Juan Jose Roque, Jesus Maria Minguet "SLSB: Improving the Steganographic Algorithm LSB" Universidad Nacional de Educación a Distancia (Spain).
[6] Dumitrescu, S., Wu, X. and Wang, Z.: Detection of LSB steganography via sample pairs analysis. 5th International Workshop on Information Hiding. Noordwijkerhout, Pays-Bas, 7/10/2002. Springer LNCS, vol. 2578, pp. 355-372, 2003.
[7] Fridrich, J., Goljan, M. and Du, R.: Reliable detection of LSB steganography in color and grayscale images. Proc. ACM Workshop on Multimedia and Security, Ottawa, ON, Canada, Oct. 5, 2001, pp. 27-30.
[8] A. D. Ker, "Improved detection of LSB steganography in grayscale images". Proc. 6th Information Hiding Workshop. Springer LNCS, vol. 3200, pp. 97-115, 2004.
[9] A. D. Ker, ―Steganalysis of LSB matching in grayscale images,‖ IEEE Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. 2005.
[10] Goljan, M. and Holotyak, T.: New blind steganalysis and its implications. Proc. SPIE Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072, pp. 1-13, 2006.