ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (421-426), Month: April - June 2015, Available at: www.researchpublish.com

Stego-System Based On Multi LFSR Generators

Salah T. Allawi[1], Ismael Abdulsattar[2]

[1,2] Dept. of Computer Science, College of Science, AL-Mustansiriyah University

Abstract: **The process of sending confidential information and messages according to their importance and are in many ways, depending on the carrier and the middle mechanism or method of concealment. In this research, we offer a system to hide messages in the color image depends on the production sites random hide are produced using a generator with a linear feedback shift register (LFSR) so that it is feeding those generators based on the cover image data.**

Keywords: **LFSR, Steganography, Map generator.**

1. INTRODUCTION

Steganography means the how to hide data by stopping the detection of hidden data. The word steganography means" covered writing" and was taken from Greek. It has a large array of secret communications ways which hide the data's very existence. These ways: digital signatures, microdots, invisible inks, covert channels, spread spectrum communications, and character arrangement [1].

Steganography and cryptography are widely used and well known ways that treat message in order to hide or cipher their existence. These ways have a lot of applying computer science and any other fields: their use is to save credit card information, e-mail messages, corporate data, etc. [2].

Steganography and cryptography are not the same. The techniques of Cryptographic can be used to make a data vague it means if it is discovered it impossible to be read. Whether any one discovers a cryptographic message it will be known as a piece of hidden information yet it is in disorder so that it is an unknown easily and de-code. Steganography hides the very existence of a data in carriers so that if the method of hiding is successful it generally gives no doubt at all. Carriers can hide using steganography information (i.e text files, audio files, images, data transmissions and videos) [3].

It's cleared the less information hidden into the carriers; gives less chances of detect the hidden data by the embedding process. The choice of the carrier (image) is regarded another important factor. When an image is used as a cover one should avoid images that have a few numbers of colors, images fonts with a sole semantic content, computer art, Gray scale images as the best cover images are recommend by a number of steganographic experts [4].

2. EMBEDDING DATA

To hide data into an image one need two files. Firstly is the cover (image) which will hold the embedded data. Secondly file is the data that will be embedded. The data that will be hidden may be images, plain text, ciphertext, or anything that can be embedded in a carrier. Embedded message in the cover image produces a stego image [1].

The model of steganography contains Message, Carrier, Stego key and embedding algorithm. The model is shown in Figure 1.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (421-426), Month: April - June 2015, Available at: www.researchpublish.com

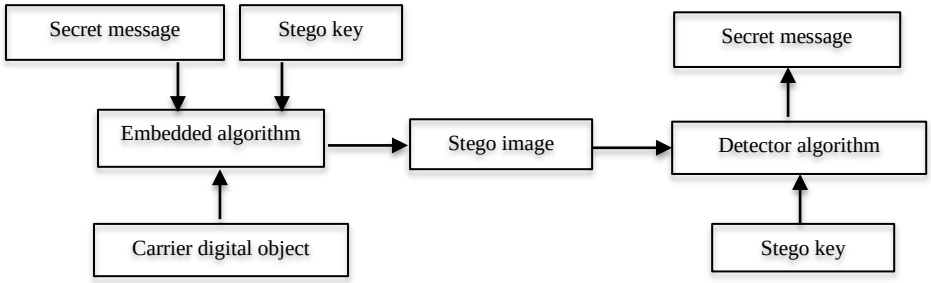

Fig. 1: Shows the model of steganography

Capacity, security and robustness are the three different factors affected by steganography and its usefulness. The quantity of data that can be embedded in the cover medium means capacity. Security refers to an attacker's inability to detect embedded data and robustness refers to the quantity of effect of the stego medium can face any distraction happens to the hidden information that caused by the enemy [5].

3. LEAST SIGNIFICANT BIT INSERTION

Least significant bit (LSB) embedding is a famous and an easy method to hide secret message in a cover image. In this way the LSB of a byte is subsisted by message bits. The fore technique is used successfully with video, audio and image steganography. According To the subjective criterion, the stego-image will seem the same to the cover medium [6].

Usually 8-bit or 24-bit files are used to save digital images. The latter one gives wide space for data hiding; yet, it can be large enough. The three essential colors: blue, green and red shows the colored representations of the pixels. The first two bits of these colors can used to hide information, and then the biggest color change in a pixel could be of 64-color values, the human vision system is unable to distinguish this little change. This simple technique is called as Least Significant Bit (LSB) insertion. This technique is used to hide a large amount of data with invisible destruction of the cover image [7].

The LSB technique works with Audio files that have a large number sounds and that are of a high bit rate, and with picture files that have a high resolution and use a large number of colors, in a best way. The LSB technique usually does not make the file size grater, but relying upon the amount of the data that must be embedded inside the file, the file can become clearly distorted [8].

Example:

The character 'B' has coded to 66 in decimal system, which is 1000010 in binary system. Three concatenated pixels form color image to embed the letter 'B' will need:

TABLE 1: Shows the pixels values before hiding character "B"

Red	Green	Blue
10000000	10100100	10110101
10110101	11110011	10110111
11100111	10110011	00110011

TABLE 2: Shows the pixels values after hiding character "B"

Red	Green	Blue
10000000	1010010**1**	1011010**0**
1011010**0**	1111001**0**	1011011**0**
1110011**0**	10110011	00110011

(The values in **bold** shows the locations where the change occurred)

When the fore example is applied on a gray scale image (8-bit) would have needed 8 pixels:

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (421-426), Month: April - June 2015, Available at: www.researchpublish.com

TABLE 3: Shows the 8 pixels values before and after hiding character "B"

Pixels values before hiding	Pixels values after hiding
10000000	10000000
10100100	1010010**1**
10110101	1011010**0**
10110101	1011010**0**
11110011	1111001**0**
10110111	1011011**0**
11100111	1110011**0**
10110011	10110011

(The values in **bold** shows the locations where the change occurred)

We get a result from these examples that 1-LSB hide usually has a 50% chance to alter a LSB every 8 bits, thus cause less distortion to the cover picture. According to images with 24-bit the distortion can be larger sometimes the 2 or even the 3 LSBs will be invisible. Images with 8-bit instead have a much more limited space where to choose colors, so it's usually possible to change only the LSBs without any change can be seen [9].

4. LINEAR FEEDBACK SHIFT REGISTER

A set of cells joined one to other and connected to each other based on join function is known as LFSR. Seeds are the first bits initialize these cells, because LFSR mixed from set of limited number of cells that will cause repeating cycle. That is why well-chosen of join function to give a sequence of bits which seems random with very long cycle. To produce random numbers of the LFSR some of the results are linked in exclusive-OR configuration which shapes a feedback mechanism (a bit pattern generation technique).

The shape of the LFSR will rely upon initial value and the count of the shift registers that will be used. The advantage of LFSR produces random numbers, where the numbers will be non-repetitive till the initial value again produced from the LFSR [10][11].

5. PROPOSED SYSTEM FOR HIDING SECRET MESSAGE

The proposed system takes the secret message as an input (text file) and the cover image which is color image (BMP). The system produces the result as a stego image (BMP). Figure 2 shows the block outline of the proposed system.

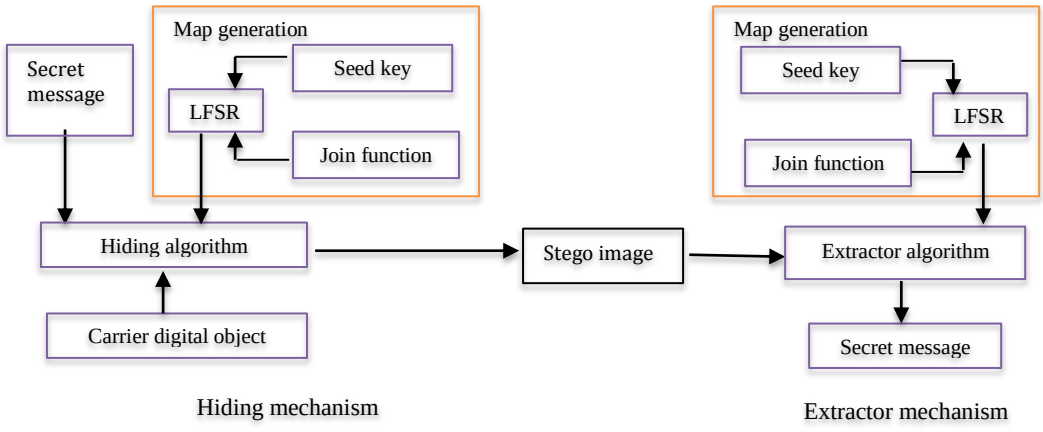

Fig. 2: Block outline for proposed system

The system uses a set of registers (LFSR) to generate bits of sites that will be used to hide the message. It's to choose between two of the first three (3LSB) in each pixel. To increase the amount of the secret message each character is converted to a decimal number and then converted to binary system consists of 6 bits per character. Each pixel is used to hide one character (2 bits per color). Figure 3 shows the proposed algorithm.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (421-426), Month: April - June 2015, Available at: www.researchpublish.com

Algorithm

1- Input
   - Cover image (BMP)
   - Secret message (text)

2- Output
   - Stego-object (BMP)

- **Process**

1- Read the cover image (c).
2- Input secret message and then convert each character in the secret message (SM) to binary format (6 bits for each character).
3- In each pixel (RGB) do the following:
   - Split the color pixel into three bands (Red, Green, Blue)
   - Convert each band value into binary format (8 bits).
   - Take 5 MSB's bits of each byte fore step and combined with the height of the cover image as seed key to feed LFSR.
   - Produce two different numbers by using LFSF to select the target position (for hiding).
   - Get the new decimal value after hiding secret message bits for each band.
   - Combine (RGB) pixels to set the stego object (image).
4- Back to the step (3) until a secret message (SM) ends.

Fig. 3: Shows proposed algorithm

LFSR consists of three registers length of 14 bits. The initial values of these registers are obtained through the 5 last bits (5MSB) of the value of each color (Red, Green and Blue) respectively and the value of the height of the cover image (converts the height into binary system 9 bits). Figure 4 shows one of the LFSRs.

Red color =189 =10111101 Height of cover image=232= 011101000

Height of cover image									**Red color value**				
14	13	12	11	10	9	8	7	6	5	4	3	2	1
0	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	**1**

Fig. 4: Shows one of the LFSRs

To produce two different sites LFSR should be moved into two or more cycles. These sites will be used to hide one character in each pixel and so on. The initial values of each LFSR will be changed after hiding each character. Figure 5 illustrates the generation process the site number.

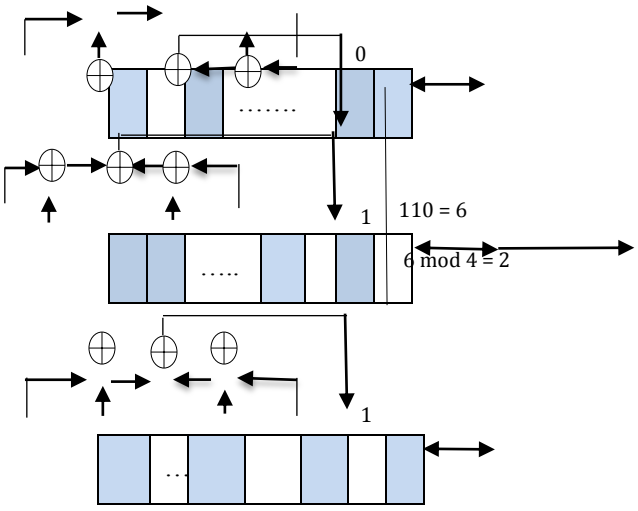

Fig. 5: Illustrate the generation process the site number

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (421-426), Month: April - June 2015, Available at: www.researchpublish.com

After selecting the site number, the three bits of the character will be replaced by the site value in each color (red, green and blue) sequentially. Thus another site is chosen to hide the remaining of the character three bits. TABLE 4 shows the process of hiding 3 bits from the character in the colors of the pixel.

TABLE 4: Shows the process of hiding 3 bits

Secret message = K = 11 = 001**011**			
Site number = 2			
Color band	**Before**	**After**	**Change**
Red	1011110**1**	1011111**1**	0
Green	1001011**0**	1001011**0**	-
Blue	1010011**1**	1010010**1**	1
Change of ratio			2

The hiding of the message characters process will continue until the completion of all the characters. Figure 6 shows the practical steps to hide a character in pixel.

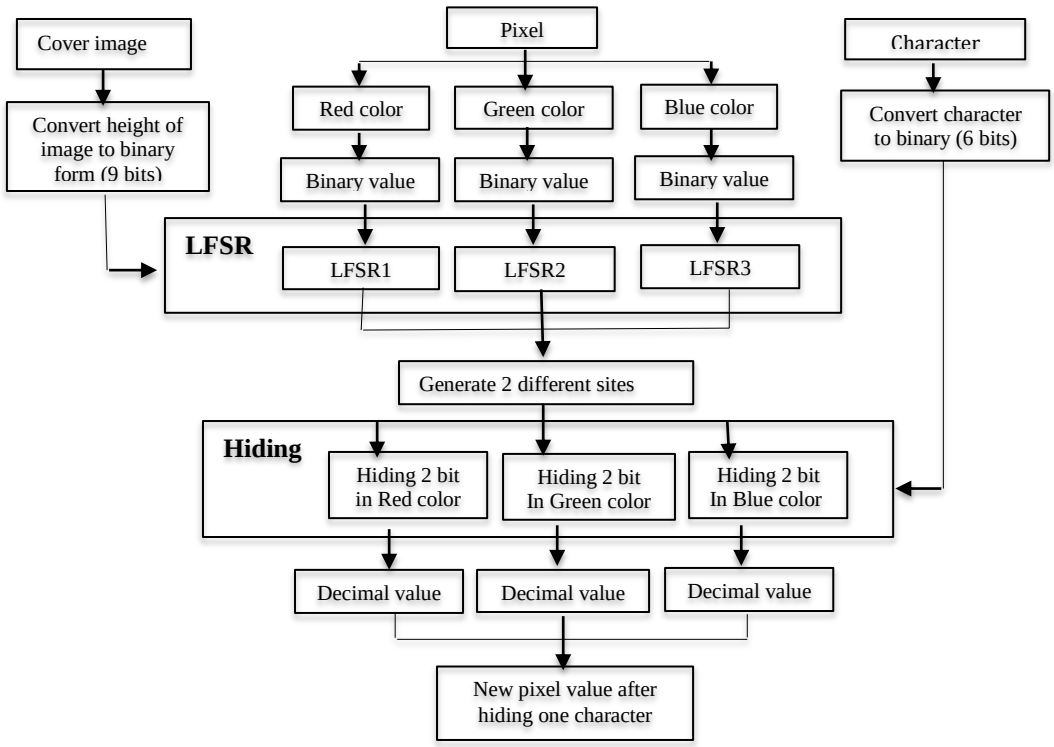

Fig. 6: Represents the steps of hiding secret message

6. EXPERIMENTAL RESULTS

In this example colored cover image (BMP) is used to carry the secret message (Lena). Figure 7 shows the cover image. The size of the cover image is (352*288) pixels. A secret message of different lengths is used in this example. TABLE 5 shows the result for this example.

Fig. 7: Shows the cover image

TABLE 5: Represents the result of hiding secret message

Length of secret message (character)	MSE			PSNR		
	red	green	blue	red	green	blue
14455	1.08	1.03	0.95	47.41	47.8	48.54
19507	1.24	1.2	1.1	46.21	46.49	47.24
25363	1.4	1.37	1.26	45.16	45.35	46.11
41305	1.76	1.74	1.59	43.21	43.31	44.07
82611	2.42	2.43	2.23	40.44	40.4	41.13

7. CONCLUSION

In our proposed system (flexible) both coding and hiding mechanism will be fed from the current data (nothing to share among sender and receiver) of the cover and in case of the LFSR which construct the required maps for hiding side by side with cover dimensions, in LFSR will not only provide complex random streams but also will guide hiding mechanism through the generating maps. Utilization of the capacity for the cover will hide one character (coded with 6 bits) in one pixel and this is good enough for hiding secret message of variable size, which never exceeds that limits.

REFERENCES

[1] Neil F. Johnson, Sushil Jajodia "Exploring Steganography: Seeing the Unseen", (26-34 IEEE February 1998).

[2] Domenico Bloisi and Luca Iocchi "Image Based Steganography and Cryptography", Departmento di Informatica e Sistemistica Sapienza University of Rome, Italy.2004

[3] Kevin Curran, Karen Bailey "An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence, fall 2003, Volume 2, Issue 2

[4] Jessica Fridrich, Miroslav Goljan, Rui Du "Reliable Detection of LSB Steganography in Color and Grayscale Images", SUNY Binghamton, Department of SS&IE, Department of EE, Department of EE.

[5] . A. Joseph Raphael, Dr. V. Sundaram, Head & Director "Cryptography and Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630, 2012

[6] Mamta.Juneja and Parvinder S. Sandhu " An improved LSB based Steganography with enhanced Security and Embedding/Extraction", 3rd International Conference on Intelligent Computational Systems (ICICS'2013) January 26-27, 2013 Hong Kong (China).

[7] József LENTI, "Steganographic Methods", Periodica Polytechnica SER. EL. ENG. VOL. 44, NO. 3–4, PP. 249–258 (2000)

[8] Aelphaeis Mangarae [Zone-H.Org] " Steganography FAQ ", March 18th 2006

[9] A. Swathi, Dr. S.A.K Jilani, Ph.D "Video Steganography by LSB Substitution Using Different Polynomial Equations", International Journal of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5, 2012

[10] Asghar S. Khashandarag[1] , Akbar S. Khashandarag[2], Amin R. Oskuei[3], Hamid H. Mohammadi[4], Mirkamal Mirnia[5] " A Hybrid Method for Color Image steganography in Spatial and Frequency Domain" , IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011.

[11] S. Bhargav Kumar1, S.Jagadeesh2, Dr.M.Ashok3 "LFSR Based Watermark and Address Generator for Digital Image Watermarking SRAM", International Journal of Computer & Organization Trends –Volume2Issue3- 2012.