Secure Steganography System for RGB Images

Fahd Alharbi

Abstract*— Steganography is the process of embedding data into a media form such as image, voice, and video. The Lest Significant Bit (LSB) is consider as the most widely used embedding technique. LSB embeds the secret message's bits into the least significant bit plane of the image in a sequentially manner . The LSB is simple, but it poses some critical issues. The secret message is easily detected and attacked duo to the sequential embedding process. Moreover, embedding using a higher bit plane would degrade the image quality severely. Using more bits for hiding in a gray scale image (8-bit) would result in a poor image quality. Thus, the color image which is represented by three bytes one for each color (Red, Green, Blue) are more suitable for hiding more data bits .To increase the security of the data hiding system, we are using a bit plane decomposition based on Fibonacci numbers to decode the RGB pixels' values. This will allow for using higher bit plane without degrading the image quality. Also, the image's pixels used for embedding data are selected by using a Pseudo Random Number Generator(PRNG).

Keywords*— Steganography, Image, LSB, Fibonacci, PRNG.

I. INTRODUCTION

The objective of the Steganography system is to communicate a secret message in a way that would not be noticeable by others [1-3]. The least significant bit (LSB) data hiding technique is the process of inserting the secret message's data bits into the least significant bits of the image in a sequential manner [4-7]. For illustration, let I be the original RGB image where each pixel is represented by three colors Red, Green, and Blue. Each color is represented by 8-bit, thus each color's value is varies from 0 up to 255. The secret message is simply the letter N with its binary representation as 01001110. We need at least three pixels to hide 8 bits. The three pixels' values in decimal and in binary are shown at Table 1 and Table 2, respectively. The LSB embedding process is shown at Table 3, where pixels and pixels' colors are selected in a sequential manner to be used for data embedding. The secret message's bits are inserted into the least significant bit of the image's pixels in a sequential manner. The LSB data hiding technique is simple and the effect on the image quality is limited and hardly noticed by the human eye duo to the small value of the bit (least significant bit) used for embedding.

TABLE 1. PIXELS' VALUES IN DECIMAL

Pixel #	Color		
	Red	Green	Blue
First Pixel	186	193	82
Second Pixel	172	195	85
Third Pixel	176	199	86

TABLE 2. PIXELS' VALUES IN BINARY

Pixel #	Color		
	Red	Green	Blue
First Pixel	10101000	11000001	01010010
Second Pixel	10101100	11000011	01010101
Third Pixel	10110000	11000111	01010110

TABLE 3. LSB EMBEDDING

Pixel #	Color		
	Red	Green	Blue
First Pixel	1010100**0**	1100000**1**	0101001**1**
Second Pixel	1010110**1**	1100001**0**	0101010**0**
Third Pixel	1011000**1**	1100011**0**	01010110

TABLE 4. LSB EMBEDDING (USING FIFTH BIT)

Pixel #	Color		
	Red	Green	Blue
First Pixel	101**0**1000	110**1**0001	010**1**0010
Second Pixel	101**1**1100	110**0**0011	010**0**0101
Third Pixel	101**1**0000	110**0**0111	01010110

On the other hand, the LSB is easy to be detected and attacked by simply extracting or changing the least significant bits of each color in each pixel. Moreover, using higher bits for embedding the secret message would enhance the security at the price of the image quality. For example, as illustrated at Table 4; using the fifth bit for hiding the secret message would degrade the image quality duo to the fact that the value of the fifth bit is 16 and the impact would be clear.

In this paper, we are using different number decomposition such as Fibonacci number system to allow using higher bit plane without degrading the image color quality. Also, we are enhancing the security of the data hiding system by using Pseudo Random Number Generator to select the next pixel and color used for embedding.

The rest of the paper is organized as follows: Section II discusses the Fibonacci based hiding system; Section III describes enhancing the data hiding system's security by using Pseudo Random Number Generators to select the next pixel and color for embedding; Section IV presents experimental results; we finally conclude in Section V.

II. FIBONACCI BASED HIDING SYSTEM

In this section, we are presenting using the Fibonacci numbers [8-10] for pixels' values decomposition. The Fibonacci sequence generated using the following formula

$$F_n = F_{n-1} + F_{n-2} \quad , n > 1 \qquad (1)$$

where, $F_0 = 1$ and $F_1 = 1$

The image's pixels' values would be represented as the sum of the non-consecutive Fibonacci numbers[11-12]. To represent the range of 0 to 255, we need 12-bit of Fibonacci digits.

Manuscript received on February 13, 2013.

Fahd Alharbi, King Abdulaziz University/ College of Engineering / Rabigh, KSA.

F_{12}	F_{11}	F_{10}	F_9	F_8	F_7	F_6	F_5	F_4	F_3	F_2	F_1
233	144	89	55	34	21	13	8	5	3	2	1

Now, we represent the pixel value of 88 using Binary and Fibonacci representation as follows

The binary representation is : 01011000

The Fibonacci representation is : 00001010101

Let consider hiding the bit value of 0 using the fifth bit in each decomposition of the pixel value of 88. The result is as following

The binary representation is : 010**0**1000

The Fibonacci representation is : 000010**0**0101

The pixel's value after LSB embedding using the fifth bit is 72, while the pixel's value after embedding using Fibonacci decomposition is 80. It is clear that using the Fibonacci decomposition would result in higher quality data embedding duo to the fact that the Fibonacci bits are less significant than those of the Binary decomposition.

Now, we reconsider the example of hiding the letter N in three pixels (Section I). The three pixels' values in Fibonacci are shown at Table 5. Table 6 shows the result of embedding the letter N into three pixels using Fibonacci decomposition, where the image quality after embedding is better the that achieved using LSB technique duo to the fact that the digits in Fibonacci system are less significant (8) than those in binary system (16).

TABLE 5. PIXELS' VALUES IN FIBONACCI

Pixel #	Color		
	Red	Green	Blue
First Pixel	010010010000	010010100010	000101001001
2nd Pixel	010001001010	010010100101	000101010001
3rd Pixel	010001010100	010100000000	000101010010

TABLE 6. FIBONACCI EMBEDDING (USING FIFTH BIT)

Pixel #	Color		
	Red	Green	Blue
First Pixel	0100100**0**0000	0100100**1**0010	0001010**1**0001
2nd Pixel	0100010**1**0010	0100101**0**0101	0001010**0**0001
3rd Pixel	0100010**1**0100	0101000**0**0000	000101010010

III. PSEUDO RANDOM NUMBER GENERATOR

The LSB technique is simple but not secure. The intruder can easily recovered the hidden message by extracting the least significant bits. On the other hand, using higher bits for embedding would degrade the image quality. In this section, we enhance the data hiding system's security by using Pseudo Random Number Generators to select the next pixel and color for embedding. The Pseudo Random Sequence is generated using Non-Linear forward feedback shift Register (NLFFSR) [13-14]. To start generating the Pseudo Random Sequence, the registers simply loaded with any initial value except zero and with each clock (step) a new Random Number is generated. The feedback function of the Pseudo Random Sequence Generator is designed based on the characteristic polynomial of the Generator. The characteristic polynomial is in the form of

$$P(x) = x^n + a_{n-1}x^{n-1} ..... + a_1 x + a_0 \quad (2)$$

where, n represents the number of registers and the length of the generated sequence is

$$N = 2^n - 1 \quad (3)$$

Let consider an image $I_{R,C,L}$, where C is the number of coulombs, R is the number of pixels (rows) in each coulomb, and L is the number of colors in each pixel. To increase the security of the data hiding system, we use three Random Sequence Generators to select the next pixel and color for embedding $I_{i,j,k}$. The first Generator selects a coulomb j in the image, the second Generator selects a pixel (row) i at the selected coulomb, and the third Generator selects a color k in the selected pixel .

IV. EXPERIMENTAL RESULTS

In this section, we are using a color 512 × 512 × 3 image for data hiding. The quality of the embedding techniques are evaluated by the Peak Signal to Noise Ratio (PSNR), where it is defined as

$$PSNR = 10 \log_{10} \left(\frac{I_{MAX}^2}{MSE} \right) \quad (4)$$

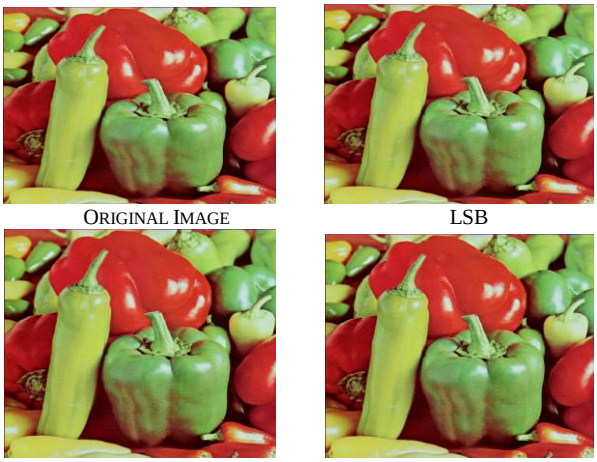
where, I_{MAX}^2 is the maximum possible value of each color in a pixel. I_{MAX}^2 is equal to 255. The Mean Square Error (MSE) is computed as follows

$$MSE = \frac{1}{R \times C \times L} \sum_{i=1}^{R} \sum_{j=1}^{C} \sum_{k=1}^{L} \left(\left| I_{i,j,k} - I'_{i,j,k} \right| \right)^2 \quad (5)$$

Where, $I_{i,j,k}$ is the original image's pixel value and $I'_{i,j,k}$ is the image's pixel value after embedding.

The performance of the proposed technique is evaluated in different setup. We study the performance of the data hiding techniques using different bit planes for embedding the secret message's bits. The original image used for embedding is a color image with size of 512 × 512× 3. The hiding capacity of the original image is 98304 data bytes, where each pixel is used for hiding three data bits. We vary the bit plane used for embedding from the second bit up to the sixth bit and in each case we hide 98304 data bytes. For performance evaluation, we compute the PSNR for each case.

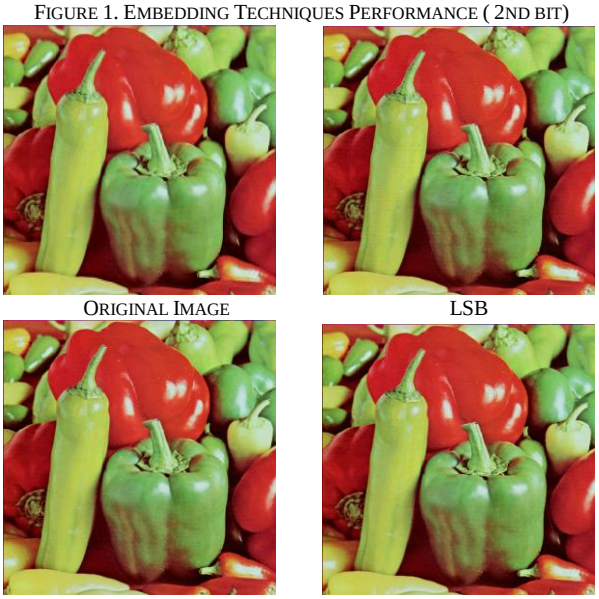
The performance of the Embedding Techniques is shown at Figures(1-3). The higher the bit plane used for embedding the higher the impact of the hiding process on the covered image quality. The quality of the covered image using the LSB hiding technique is degrade by using higher bit plane for embedding. On the other hand, Fibonacci and Fibonacci plus PRNG maintain a better image quality for all cases. Table 4 shows that Fibonacci hiding technique always outperforms the LSB and achieves better Signal to Noise Ratio duo to the fact that digits in Fibonacci number system are less significant than those in binary system. Moreover, using Fibonacci hiding technique along with the Pseudo Random Sequence Generators enhances the image quality and increases the data security.



ORIGINAL IMAGE LSB

FIBONACCI FIBONACCI + PRNG

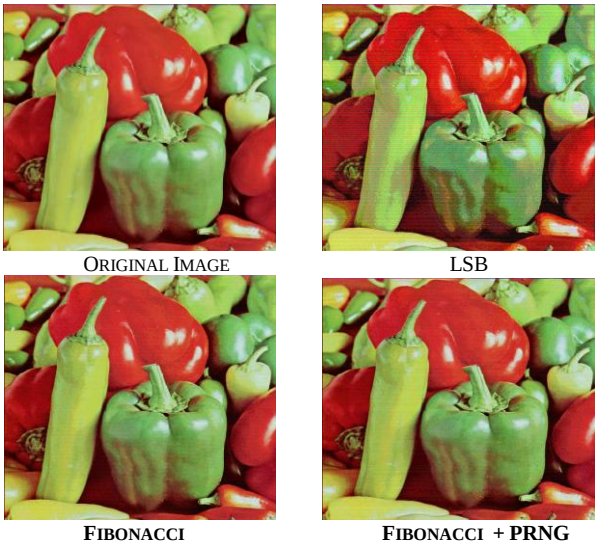
FIGURE 1. EMBEDDING TECHNIQUES PERFORMANCE (2ND BIT)



ORIGINAL IMAGE LSB

FIBONACCI FIBONACCI + PRNG

FIGURE 2. EMBEDDING TECHNIQUES PERFORMANCE (4TH BIT)



ORIGINAL IMAGE LSB

FIBONACCI **FIBONACCI + PRNG**

FIGURE 3. EMBEDDING TECHNIQUES PERFORMANCE (6TH BIT)

TABLE 4. EMBEDDING TECHNIQUES PERFORMANCE (PSNR)

Bit plane	Peak Signal to Noise Ratio (PSNR)		
	LSB	Fibonacci	Fibonacci + PRNG
2nd	45.1731	46.9311	46.9266
4th	33.1340	38.5244	38.5319
6th	21.0898	30.1709	30.1659

V. CONCLUSIONS

The goal of the Steganography system is to communicate a secret message in a way that would not be noticeable by an intruder. The least significant bit (LSB) is the most widely used technique for data hiding. The LSB process is simple but not secure. Also, using higher bit plane for hiding data would degrade the covered image's quality. In this paper, we improved the covered image's quality by using different decomposition such as Fibonacci number system where digits are less significant than those in binary system. Moreover, the LSB is not secure and data can easily be retrieved or attacked by extracting or changing the least significant bit of each pixel in a sequential manner. We enhanced the data hiding security by using the Pseudo Random Sequence Generators to select the next pixel and color for embedding in the RGB images.

REFERENCES

1. S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.
2. W. Bender, D. Gruhl, N. Morimoto, A. Lu, ―Techniques for data hiding‖ IBM Syst. J. 35 (3&4) (1996) 313–336.
3. Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.: Digital Watermarking and Steganography, 2Nd Ed. ISBN: 978-0123725851
4. Chi-Kwong Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469–474, Mar. 2004.
5. Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.: Digital Watermarking and Steganography, 2Nd Ed. ISBN: 978-0123725851
6. Swanson, M. D., Kobayashi, M., Tewfik, A. H.: Multimedia Data-Embedding and watermarking Technologies, Proc. IEEE, vol. 86, 1064 – 1087, 1998
7. N. Johnson, Digital Watermarking and Steganography: Fundamentals and Techniques , The Computer Journal. (2009)
8. A. Hordam, "A generalized Fibonacci sequence", American Mathematical Monthly, no. 68, pp 455 — 459, 1961.
9. Sigler, Laurence E., "Fibonacci's Liber Abaci", Springer-Verlag, translation, 2002.
10. Vorobiev Nikolai N., Mircea M., "Chapter 1. Fibonacci Numbers", Birkhauser, pp. 5–6. ISBN 3- 7643-6135-2, 2002
11. Brown, J. L. Jr. "Zeckendorfs Theorem and Some Applications", Fib. Quart. 2, 16 3-168, 1964.
12. Phillips G.M., "Zeckendorf representation", in Hazewinkel, Michiel, Encyclopaedia of Mathematics, Springer, ISBN 978-1556080104, Picione, 2001.
13. L. T. Wang and E. J. McCluskey, "Linear feedback shift register design using cyclic codes," IEEE Trans. Comput., vol. 37, pp. 1302-1306, Oct. 1988.
14. A. Fuster and L. J. Garcia, "An efficient algorithm to generate binary sequences for cryptographic purposes," Theoretical Computer Science, vol. 259, pp. 679-688, May 2001.