International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

The Least Significant Two-bit Substitution Algorithm for Image Steganography

Serdar Solak[a]*, Umut Altinişik[b]

[a,b]*Department of Informatics, University of Kocaeli , Umuttepe Campus, Kocaeli,41380, Turkey*

[a]*Email: serdars@kocaeli.edu.tr*

[b]*Email: umuta@kocaeli.edu.tr*

Abstract

Steganography hides various data within different file types, which ensures secure communication. In recent years, the science of steganography has gained importance, due to the increase of large data on the internet and the safe transmission of these data. The main objective is to hide a large amount of data into the cover image in secure and incomprehensible manner. In this article, the two-bit least significant substitution (LSB) method is used to hide data on the colored cover images. In experimental studies, two-bit LSB substitution algorithm was performed in the form of LSB R2G2, LSB R2B2 and LSB G2B2 methods. In the classical LSB substitution method, the data are hidden in sequence, while the data are hidden by the shuffling algorithm at the proposed study. In this way, the security of hidden data is provided.

Keywords: Two-bit LSB; Image Steganography; Security; Data Hiding.

1. Introduction

Today, it is very important to have a confidential and secure digital communication. The fact that digital communication is mostly carried out over the Internet has increased the necessity of providing information security. Steganography is an important science which is used to ensure that the data is hidden securely in the cover media. Data are transmitted to the other side in a secure manner, hidden in text, audio, video, picture or protocol files without being perceived by third parties in the steganography science [1-3]. In the image steganography, the data are conveyed by hiding on a cover image. Stego image and key are other important parts of the steganography [3].

----

* Corresponding author.

As a measure of performance evaluation of secret data sent to the other party in image steganography; capacity, security, imperceptibility, computational complexity criteria are used. Least Significant Bits (LSB) Substitution and Pixel Value Difference (PVD) are the most commonly used methods in image steganography [5-10]. The LSB substitution method is a simple and widely used data-hiding method for image steganography. In LSB substitution method, secret data is hidden in the least significant bits in the cover image. There are several articles in the literature on the process of using and developing the LSB substitution method [10-13]. In these studies, LSB substitution method was developed by using different algorithms and the data were concealed. In some of these algorithms, different methods such as two-bit LSB, three-bit LSB, four-bit LSB were used in stego image creation stage by hiding data into cover image. In the image steganography, the ratio of the stego image to the cover image and the quality of the stego image must be high. In 2001, Wang and his colleagues used genetic algorithm to increase data security, reduce high computational complexity and improve system performance [6]. In another study by Swain, the cover image was divided into 3x3 blocks and the pixel value differences were calculated for each block. Because of the calculations, the blocks were divided into four classes in the lower to upper and the data were hidden by using different LSB substitution algorithms in each class. In this method, two-bit LSB substitution method was applied on the data of lower class [11]. In addition, data security is very important in steganography. Joshi and his colleagues proposed a new method which uses two-bit LSB substitution and XOR operation together to provide a secure data transmission. When this method was used, they said that even if data were obtained by third parties, their analysis would not be possible [12]. Solak and Altınışık used LSB three-bit substitution method to hide the large amount of data in their study [13]. In this study, the two-bit LSB substitution method was performed to hide data high-capacity and transmit safely. Lena, Airplane, Baboon, and Fruits color cover images were used to obtain the results. Our paper includes two-bit LSB substitution method in section 2, the experimental studies and results in section 3, and conclusion and suggestion in Section 4.

2. Two-bit LSB Substitution Method

In the classical LSB substitution method, secret data is transmitted to the receiver by changing the least significant bit of cover image pixels. In this method, the least significant bit of the Red Green Blue (RGB) color channels located in a color cover image pixel is changed in a specific order for one bit of secret data to be hidden. This allows three bits data to be embedded in a pixel area for colored image. In the two-bit LSB substitution method, the secret data is embedded using the least significant last two-bit of color cover image. In our paper, four-bit data is hidden in a pixel of colored cover image using two-bit LSB substitution method. The two-bit LSB substitution method was first performed by the so-called LSB R2G2, which is two bits to the red color channel and two bits to the green color channel. Similarly, when LSB R2B2 is created by hiding two bits data in red and blue color channels, LSB G2B2 method is composed by embedding two bits data to green and blue color channels. In the method, we converted from decimal format of cover image pixel value to binary number format for used each color channels. The secret data is converted to binary number format and is hidden in four bits in one pixel. When performing the embedding process, the first two bits of four bits data are usually hidden in bits 7 and 8 of the first color channel, while bits 3 and 4 are hidden in bits 7 and 8 of the second color channel. In order to ensure that secret data can be transmitted more safely to the receiver, the first bit of four bits secret data is hidden to the 8th-bit of the first color channel, the second-bit to the 7th-bit of the second-color channel, the third-bit to the 8th-bit of the second-color channel, and the fourth-bit is hidden in the 7th bit of the first color channel. Thus, the content of the secret data is rendered inconceivable by third parties. Figure 1 shows a block diagram illustrating the operation of the two-bit LSB substitution method. In figure, the first four bits of the 128 x 128 in size gray-scale cameraman image are hidden by LSB R2G2 at 512 x 512 size Lena colored cover image. When the first four bits of data (1000) obtained from the cameraman image is hidden to the color values (226, 137, 125) of the first pixel of the Lena cover image, the first pixel values of the stego image (225,136,125) are obtained.

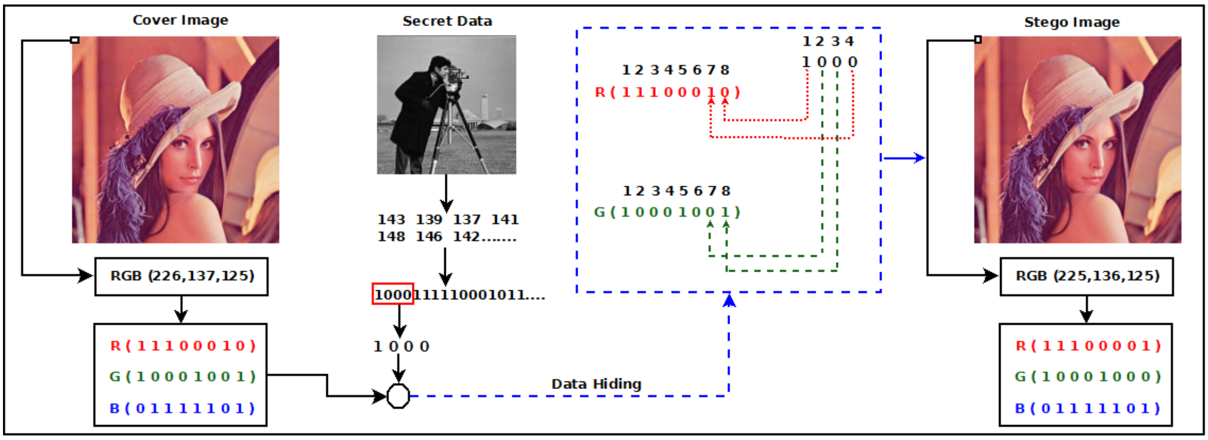

Figure 1: Block diagram for data hiding with two-bit LSB substitution

3. Experimental Studies

We used colored cover images as Lena, Airplane, Fruits and Baboon in size 512 x 512 at experimental studies. Figure 2 shows colored cover images of 512 x 512 sizes used in experimental studies.

(a) Lena (b) Airplane (c) Fruits (d) Baboon

Figure 2: Colored cover images used in experimental studies

We obtained the results by embedding 4 bpp data with LSB R2G2, LSB R2B2 and LSB G2B2 methods in colored cover images. The results were obtained by using Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) criteria. The PSNR value determines the quality of the stego image while SSIM gives the similarity ratio between the cover image and the stego image.

The PSNR [14] and SSIM [15] are presented respectively in Equation 1 and Equation 2.

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{Max}^2}{\mathrm{MSE}}\right) \tag{1}$$

$$\mathrm{SSIM(x,y)} = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c1)(\sigma_x^2 + \sigma_y^2 + c2)} \tag{2}$$

LSB R2G2 method is used to hide data while red and green color channels are used. Table 1 shows the general PSNR values, PSNR values of red and green channels, and the SSIM values. These values are obtained while 1048576 bits data is hidden in the colored cover image. The mean PSNR value is 46.4790, the red channel PSNR 44.8806, the green channel PSNR 44.5614 and the SSIM value 0.9969.

Table 1: LSB R2G2 maximum bits PSNR and SSIM values

Cover Image 512 x 512	**Embedded Bits (Payload)**	**LSB R2G2**			
		PSNR	**PSNR R**	**PSNR G**	**SSIM**
Lena	4 bpp	46.4935	44.9064	44.5655	0.9995
Airplane	4 bpp	46.4778	44.8875	44.5527	0.9909
Fruits	4 bpp	46.4406	44.8157	44.5478	0.9981
Baboon	4 bpp	46.5039	44.9129	44.5795	0.9991
Average	**4 bpp**	**46.4790**	**44.8806**	**44.5614**	**0.9969**

LSB R2B2 method is used to hide data while red and blue color channels are used. Table 2 shows the general PSNR values, PSNR values of red and blue channels, and the SSIM values. The mean PSNR value is 46.4932, the red channel PSNR 44.8806, the blue channel PSNR 44.5890 and the SSIM value 0.9961.

Table 2: LSB R2B2 maximum bits PSNR and SSIM values

Cover Image 512 x 512	**Embedded Bits (Payload)**	**LSB R2B2**			
		PSNR	**PSNR R**	**PSNR B**	**SSIM**
Lena	4 bpp	46.5105	44.9064	44.5983	0.9993
Airplane	4 bpp	46.4812	44.8875	44.5592	0.9884
Fruits	4 bpp	46.4726	44.8157	44.6102	0.9977
Baboon	4 bpp	46.5084	44.9129	44.5881	0.9989
Average	**4 bpp**	**46.4932**	**44.8806**	**44.5890**	**0.9961**

Table 3: LSB G2B2 maximum bits PSNR and SSIM values

Cover Image 512 x 512	Embedded Bits (Payload)	LSB G2B2			
		PSNR	PSNR G	PSNR B	SSIM
Lena	4 bpp	46.4982	44.8809	44.5983	0.9994
Airplane	4 bpp	46.4722	44.8688	44.5592	0.9906
Fruits	4 bpp	46.4828	44.8365	44.6102	0.9982
Baboon	4 bpp	46.4954	44.8859	44.5881	0.9992
Average	**4 bpp**	**46.4872**	**44.8680**	**44.5890**	**0.9969**

LSB G2B2 method is used to hide data while green and blue color channels are used. Table 3 shows the general PSNR values, PSNR values of green and blue channels, and the SSIM values. The mean PSNR value is 46.4872, the green channel PSNR 44.8680, the blue channel PSNR 44.5890 and the SSIM value 0.9969.

The secret data is embedded into each image in the range of 100000 bits to 1000000 bits for each two-bit LSB substitution methods. Table 4 shows the payload and PSNR values for Lena cover image. The two-bit LSB substitution algorithm is observed that PSNR values are close to each other in all methods.

Table 4: Lena PSNR values of two-bit LSB methods

Bits	Payload (bpp)	LSB R2G2	LSB R2B2	LSB G2B2
100000	0.38	56.5748	56.5521	56.5193
200000	0.76	53.5552	53.5276	53.5028
400000	1.53	50.5217	50.5193	50.5149
600000	2.29	48.7375	48.7459	48.7372
800000	3.05	47.494	47.4997	47.4906
1000000	3.81	46.5316	46.5368	46.5217

Figure 3 is a graph showing the performance analysis of PSNR values obtained using the LSB R2G2 method of Lena cover image. In the graph, the payload is between 0.38 and 3.81 and the PSNR values are between 56.5748 and 46.5316.

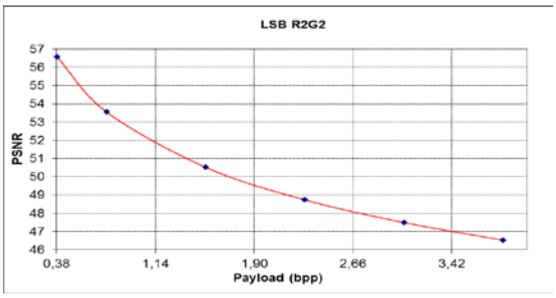

Figure 3: Lena PSNR values for LSB R2G2

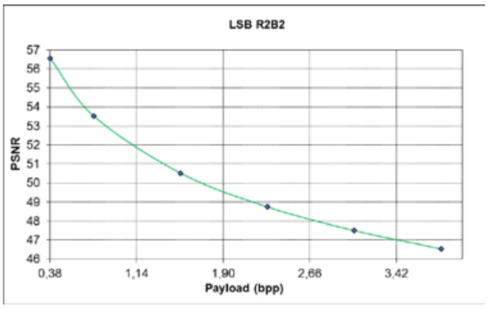

Figure 4: Lena PSNR values for LSB R2B2

Figure 4 is a graph showing the performance analysis of PSNR values obtained using the LSB R2B2 method of Lena cover image. In the graph, the payload is between 0.38 and 3.81 and the PSNR values are between 56.5521 and 46.5368. Figure 5 is a graph showing the performance analysis of PSNR values obtained using the LSB G2B2 method of Lena cover image. In the graph, the payload is between 0.38 and 3.81 and the PSNR values are between 56.5193 and 46.5217.

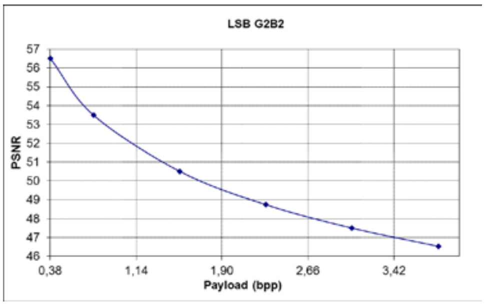

Figure 5: Lena PSNR values for LSB G2B2

4. Conclusion

LSB substitution we applied as a changing for the least significant two-bit is a commonly method in image steganography in this paper. We used LSB R2G2, LSB R2B2 and LSB G2B2 methods to hide data which randomly generated 1048576-bit data, at the colored cover images. While data hiding is performed, it is ensured that the data in stego image can incomprehension when it is obtained by third parties. The PSNR values obtained from the three methods are very similar. The two-bit LSB substitution method is hiding high capacity data into colored cover images according to the classic LSB method. However, it can be detected by third parties that the presence of secret data is inside stego image. The two-bit LSB substitution method can be combined with the other image steganography methods to more secure and efficient new methods can be created.

References

[1] Cheddad A., Condell J., Curran K., and Mc Kevitt P., (2010), "Digital image steganography: Survey and analysis of current methods", Signal processing, 90(3), 727-752.

[2] Bender W., Gruhl D., Morimoto N., and Lu A., (1996), "Techniques for data hiding", IBM systems journal, 35(3,4) 313-336.

[3] Zaw Z. M., and Phyo S. W., (2015), "Security Enhancement System Based on the Integration of Cryptography and Steganography", International Journal of Computer (IJC), 19(1), 26-39.

[4] Johnson N. F., and Jajodia S., (1998), "Exploring steganography: Seeing the unseen.", Computer, 31(2).

[5] Chan C. K., and Cheng L. M., (2004), "Hiding data in images by simple LSB substitution", Pattern recognition, 37(3), 469-474.

[6] Wang R. Z., Lin C. F., and Lin J. C, (2001), "Image hiding by optimal LSB substitution and genetic algorithm", Pattern recognition, 34(3), 671-683.

[7] Chang C. C., Lin M. H., and Hu Y. C., (2002), "A fast and secure image hiding scheme based on LSB substitution", International Journal of Pattern Recognition and Artificial Intelligence, 16(04), 399-416.

[8] Zhang X., and Wang S., (2004), "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security", Pattern Recognition Letters, 25(3), 331-339.

[9] Solak S., and Altınışık U., (2018), "LSB Substitution and PVD performance analysis for image steganography", International Journal of Computer Sciences and Engineering, 6(10), 1-4.

[10] Wu D. C., and Tsai. W. H., (2003), "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, 24(9-10), 1613-1626.

[11] Swain G., (2014), "Digital image steganography using nine-pixel differencing and modified LSB substitution", Indian Journal of Science and Technology, 7(9), 1444-1450.

[12] Joshi K., Yadav R., and Chawla G., (2017), "An Enhanced Method for Data Hiding using 2-Bit XOR in Image Steganography", International Journal of Engineering and Technology (IJET).

[13] Solak S., and Altınışık U., (2018), "A data hiding method using least significant three-bit substitution for colored cover image", International Marmara Science and Social Sciences Congress (IMASCON), Turkey.

[14] Wang Z., Simoncelli. E. P., and Bovik. A. C., (2003), "Multiscale structural similarity for image quality assessment", The Thrity-Seventh Asilomar Conference on Signals Systems & Computers, 2003, 1398-1402.

[15] Hore A., and Ziou D., (2010), "Image quality metrics: PSNR vs. SSIM", Pattern recognition (icpr), 20th international conference on IEEE, 2366-2369.