INTERNATIONAL JOURNAL OF ELECTRONICS, MECHANICAL AND MECHATRONICS ENGINEERING
Vol.8 Num.2 - 2018 (1543-1553)

Least Significant Bit Gaped: A New Method for Image Steganography

Waleed TUZA[1], Dr. Öğr. Üyesi N. Gökhan KASAPOĞLU [2]

Abstract - Steganography is an information security technique that provides a solution for hiding information. There are different types of cover mediums that can be used in steganography such as text or image steganography. We chose image steganography as our domain of work where the images are used as cover mediums to be our basis of experiments for the proposed LSBG method. One of the main well-known steganography methods is the least significant bit (LSB), however it has its limitations and therefore many approaches have been proposed to improve it. We propose a new improvement method defined as Least Significant Bit Gaped (LSBG) where the aim is to improve steganography imperceptibility compared to LSB by comparing the histogram analysis of LSB with LSBG methods and MSE measures. The proposed LSBG method will also offer a new key structure that will increase the complexity in secret data extraction and the level of information security.

Keywords: *Steganography, Least Significant Bit, Least Significant Bit Gaped*

1. Introduction

Steganography is the art of hiding data. It is an information security method that can be applied to secure the information by hiding it in a medium where the secret information cannot be observed. Steganography methods, in recent years, have been applied in the digital world where we deal with different digital media such as images, audio, or video data. Digital steganography works by using those digital mediums as cover mediums where the secret message is required to be in a digital data form too. The application of steganography simply consists of embedding secret information data in a selected cover medium to produce a stego medium where it holds the hidden data.

There are wide applications where steganography can be used. Secret and covert communication systems, for instance, the military communications systems need to possess a high level of information security during transmission where steganography takes a place as one of the possible solutions [2]. Some of the widely used applications for steganography are watermarking and fingerprinting, which are used for protecting the copyrights and data property for the owners.

Another possible application area of steganography is the secure storage of information [12]. Steganography can be considered as a useful method to save information data in an undetectable way which is an important element for securing the data.

[1] *Dept. of Electrical and Electronics Engineering, Istanbul Aydin University, Istanbul, Turkey, waleed.tuza@gmail.com*
[2] *Dept. of Electrical and Electronics Engineering, Istanbul Aydin University, Istanbul, Turkey, gokhankasapoglu@aydin.edu.tr*

As mentioned before, steganography can use different types of cover mediums such as text medium, image medium, audio medium, and other types of mediums [7]. Also for secret messages, messages can be any kind of data medium like a text or an image.

1.1. Steganography Elements

As a system, the steganography method can be divided into four main elements as listed below:

- Secret message: it is the message that will be embedded in the cover medium. It is actually the crucial element to be secured by hiding so that it cannot be detected. The secret message can be any type of data such as a simple text message or an image.
- Cover object: it is the medium that will be used as a carrier of the embedded secret data. Selecting a suitable cover medium is very important for concealing the secret based on the steganography method requirements.
- Steganography key: the key can be considered as the control data part that you need when you want to apply the inverse operation of steganography method and extract the secret message. Without the knowledge of the key, you will not be able to extract the secret message from the cover medium.
- Stego object: it is the result carrier medium that contains the embedded secret message hidden inside it.

1.2. Steganography in Communication Systems

In covert communication systems, the most important parameter for steganography to be considered is imperceptibility. The main objective for the hidden data is to raise no suspicion regarding the cover medium being edited [4]. That is why the designer will try to maximize the level of imperceptibility on the expense of having reduced levels of capacity and robustness [3]. Improving imperceptibility can be done by reducing the amount of changes in the data values (pixel intensities) in the cover medium during the embedding of the secret data.

Using steganography as an information security technique can be very useful in communication systems. Especially in communication systems that are used for military applications where the communication of information is considered to be confidential and is very important not to be received and analyzed by third parties. That is why it is important to secure the information so that in case received by a third party, the data cannot be analyzed and that is where encryption and steganography come into play. Those information security techniques can be used as pre-stages in the communication system in order to secure the information signal from being used by a third party.

Using lossless compression as a pre-stage operation of steganography in the communication systems provides the capability of extracting and reconstructing the secret message 100% accurately [5]. Moreover, it is a great solution for reducing the capacity of the secret message. Error detection and correction (EDC) coding is used for ensuring the correct reconstruction of the embedded data. Below, Figure 1 shows a block diagram of the communication system that has encryption and steganography methods used for securing the secret data before transmitting it:

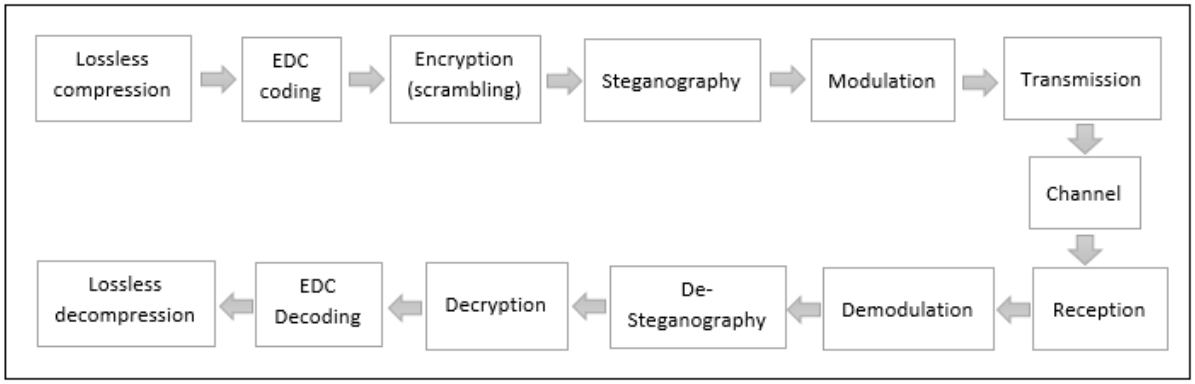


Figure 1: Covert communication system block diagram.

2. Least Significant Bit (LSB)

Least Significant Bit is a steganography method of embedding hidden data by using the least significant bits of the cover medium data bytes (image pixels).To simply summarize the way of embedding data in LSB method, LSB is located as the last bit from the right side of any binary value [7]. In LSB embedding, it is possible to use the last bit, last two bits, or the last three bits in the binary value of the byte or pixel for data embedding. Therefore, if we have a 1-byte pixel size, the minimum LSB capacity is 1 bit per pixel (bpp) [7]. For example, if we have a byte binary value of (11110101), the last LSB is (1), and the last two LSB bits are (01), also if one wants to know, the last three LSB bits are equal to (101).

For instance, let's have three pixels of the cover image with binary values of (11110001 11110000 11110011) and if we want to embed a message of 3 bits as (110) in those three pixels then 1 bit is needed for LSB embedding in each pixel. By that, the result stego pixels are (11110001 11110001 11110010). As you can see for the first pixel, the secret bit is equal to last bit in the pixel and that is why the pixel LSB value is still the same. While in the second and the third pixels, the LSB bits were changed to the value of the second and third bits of the message as seen in red color.

In Figure 2, we have another example to demonstrate the locations of the LSB pixels in a cover image. It is assumed that we have an (8x8) size cover image and we have a secret message that has a capacity of 24 bits. If we have used LSB with embedding two bits in each selected pixel, then we need a total of 12 pixels to carry the secret message. Therefore, the first 12 pixels in the cover image that are highlighted in grey, are used for LSB embedding. The remaining pixels that are highlighted in white in the cover image will be left untouched.

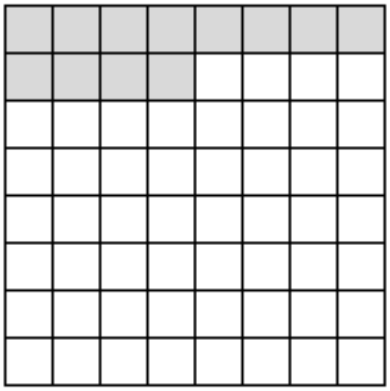


Figure 2: An 8x8 pixel size stego image where the highlighted pixels in gray are the pixels used for LSB method.

3. Least Significant Bit Gaped (LSBG) Methodology

Basically, the concept covers embedding the secret message in certain pixels with a certain rate using LSB method. Also, LSBG method requires gap pixels with a certain rate where there are no data embedded in these pixels. Hence, in the stego medium, the pixels are divided into two parts. First, the LSB pixels that are to be used for LSB embedding are selected. The other part includes the gap pixels which can be defined as the pixels that are not selected for LSB embedding. The reason behind the name "gap pixels" originates from the fact that those pixels not being used for containing any data of the secret message, and that is why they can be considered as gaps. The gapping rate can vary from one LSB pixel to one gap pixel (1LSB to 1G), one LSB pixel to two gap pixels (1LSB to 2G), one LSB pixel to two gap pixels (1LSB to 3G), and so on. The main idea of applying such a method is to have the ability to distribute the secret embedded LSB pixels in the majority of the cover medium area (image pixel area) as much as possible. The ratio of LSB pixels to gap pixels depend on two main factors:

1. The capacity of the secret message to be hidden. The smaller the capacity of the secret message, the more possible gapping rates can be applied in the cover medium.
2. The capacity of the cover medium (cover image). The larger capacity of the cover image offers the capability of applying high variety of (LSB to G) rates.

Studying the previous two factors, we can select a suitable LSB to gap rate based on the capacity of the secret message and the capacity of the chosen cover image to apply LSBG method.

In LSBG method, the ratio of LSB pixels to gap pixels can be performed in either horizontal or vertical axes in the cover image. The selection of the axis can be made by the designer. In Figure 3, same as before, we assume having 12 pixels to carry the secret massage. LSBG method is applied with horizontal gaping and the LSBG gapping rate is 1LSB to 1G.

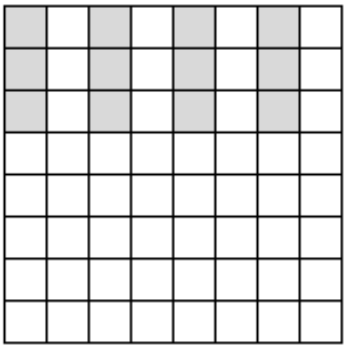


Figure 3: An 8x8 pixel size stego image where highlighted pixels in gray are the ones used for LSBG method with 1LSB /1G ratio in horizontal access.

3.1. Two-Dimensional LSBG (2D LSBG)

The LSBG gapping can be applied in the vertical or in the horizontal axes as explained previously. However, there is also the possibility of applying (two dimensional) LSBG gapping in both vertical and horizontal axes. The 2D LSBG provides a greater LSB pixels distribution in the cover medium.

In Figure 4, we have the same cover image with a size of 8x8 pixels and 2D LSBG method is applied with 1LSB to 1G rate where the gaping is done in both vertical and horizontal axes and the 12 LSB pixels are distributed as shown in the figure below.

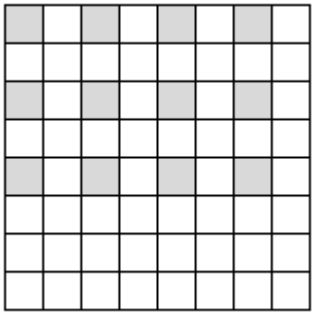


Figure 4: An 8x8 pixel size stego image where highlighted pixels in gray are the ones used for 2D LSBG method with 1LSB /1G ratio.

3.2. Shifting Property for LSBG

Shifting property can be applied to either LSB or LSBG method where the aim is not to apply the steganography technique from the beginning of the cover medium but to shift the starting point (starting LSB pixel) with a certain number that is chosen by the designer. Applying this method will increase the difficulty of extracting the secret information from the LSB pixels by third parties since the starting point is only known by the designer. The shifting property can be used as an additional element to the steganography LSBG key elements.

In Figure 5 where the 2D LSBG method is used with the ratio of 1LSB to 1G, an additional shifting property was applied for placing the start point from the third row from up in the cover image as seen in the figure.

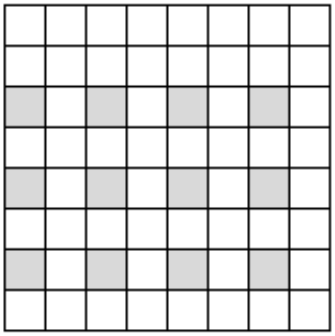


Figure 5: An 8x8 pixel size stego image where highlighted pixels in gray are the ones used for 2D LSBG method with 1LSB /1G ratio and shift property.

3.3. LSB and LSBG capacity

The formula for finding the maximum possible capacity of LSB method in a cover image is shown in formula (1) below:

$$Max\{C_{LSB}\} = n_P . n_b \tag{1}$$

Where n_P is total number of pixels and n_b is total number of bits used per pixel. While the maximum possible capacity of LSBG method in a cover image is shown in formula (2) below:

$$Max\{C_{LSBG}\} = \frac{n_P . n_b}{(n_g + 1)} \tag{2}$$

Where n_g is the number of gaps in the gapping rate. Finally, the maximum possible capacity of 2D LSBG method in a cover image is given in formula (3) below:

$$Max\{C_{2D\ LSBG}\} = \frac{n_P . n_b}{(n_g + 1)^2} \tag{3}$$

For a cover image of a selected pixel size of 256 x 256, Table 1 demonstrates the maximum capacity of the secret data to be embedded when using LSB and LSBG at different possible gapping rates for 1 byte pixel capacity for LSB and LSBG.

Table 1. Maximum capacity for cover image with 256x256 pixel size.

Method	Max. capacity
LSB (2 bpp)	131,072 bits (16,384 byte)
LSBG (2 bpp) (1LSB to 1G)	65,536 bits (8,192 byte)
LSBG (2 bpp) (1LSB to 3G)	32,768 bits (4,096 byte)
LSBG (2 bpp) (1LSB to 7G)	16,384 bits (2,048 byte)
LSBG (2 bpp) (1LSB to 15G)	8,192 bits (1,024 byte)
LSBG (2 bpp) (1LSB to 31G)	4,096 bits (512 byte)
LSBG (2 bpp) (1LSB to 63G)	2,048 bits (256 byte)
LSBG (2 bpp) (1LSB to 127G)	1,024 bits (128 byte)

As it can be noticed that the more you increase the gapping rate the less capacity it can support for embedding the secret message. From the given secret message capacity, a suitable gapping rate that supports a greater embedding capacity is selected for carrying the secret message .

3.3. LSBG Key Elements

One of the main improvement points of LSBG over LSB is the complexity of the key elements of LSBG method. In LSBG method, the length of the secret message and the LSB method's embedding rate per pixel are not enough alone. One actually needs to have all the elements of the LSBG key to be able to extract the embedded secret message successfully. The LSBG key elements can be defined as follows:

- The capacity of the secret message (Total number of the bits of the secret bit stream).
- The selection of number of bits to be embedded in each pixel by the designer.
- The selection of the ratio of LSB pixels to gap pixels to be used for data embedding.
- The selection of the start point of LSBG embedding. An additional applicable element by using shifting property.
- The LSB sequence number in the LSB to G ratio. (In case multiple messages multiplexing is used).
- The possible usage of encryption (scrambling) before applying LSBG method as pre-stage. Adding the key of encryption will cause the secret bits to be embedded in a non-sequential way in the selected LSB pixels.
- The possible usage of Lossless compression method for the secret message before applying LSBG method. Adding the key of compression as a pre-stage will help reduce the capacity of the secret message and also the secret message cannot be analyzed during extraction from LSBG unless it is decompressed
- Band selection for LSBG method. This is applicable certainly; if multiple bands colored images are used like RGB images. This way one band would be selected while the other band will remain the same.

4. Designed Experiments and Results

The used secret image is a 50x50 pixel size white background image with fixed pixel value of 255 (the binary value of 11111111). This secret image was selected as a severe case as it causes a high amount of deviation in the stego histogram which is important since it requires applying different methods that are used in the experiments, demonstrating the great difference clearly in the stego histogram between the each embedding method used. The used cover image is a grayscale watch image with the size of 256x256 pixels.

Embedding methods used in this case:

- Least Significant Bit method, (LSB) (2 bpp).
- Least Significant Bit Gaped method, (2D LSBG) (2 bpp) (1LSB to 1G).

The evaluation process is conducted by analyzing the histograms of the stego images and making a comparison of the histograms of LSB and LSBG methods. Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR) are measured to determine the amount of change between the cover and stego mediums for both LSB and LSBG methods. The less MSE value indicates less difference between the cover image and stego image and by that the imperceptibility level is increased.

The following figure is composed in six subfigures, the selected secret white image is shown in Figure 6 (a). Watch image is the selected cover image in the experiment as seen in Figure 6 (b). A demonstration figure with the cover image pixel size was generated to highlight the selected pixels for embedding in white and remaining unchanged pixels in black. In Figure 6 (c) we can see the demonstration figure of selected pixels for LSB embedding and in Figure 6 (d) the demonstration figure of selected pixels for 2D LSBG embedding. Figure 6 (e) shows the result stego image after using LSB embedding and Figure 6 (f) shows the result stego image using 2D LSBG method.

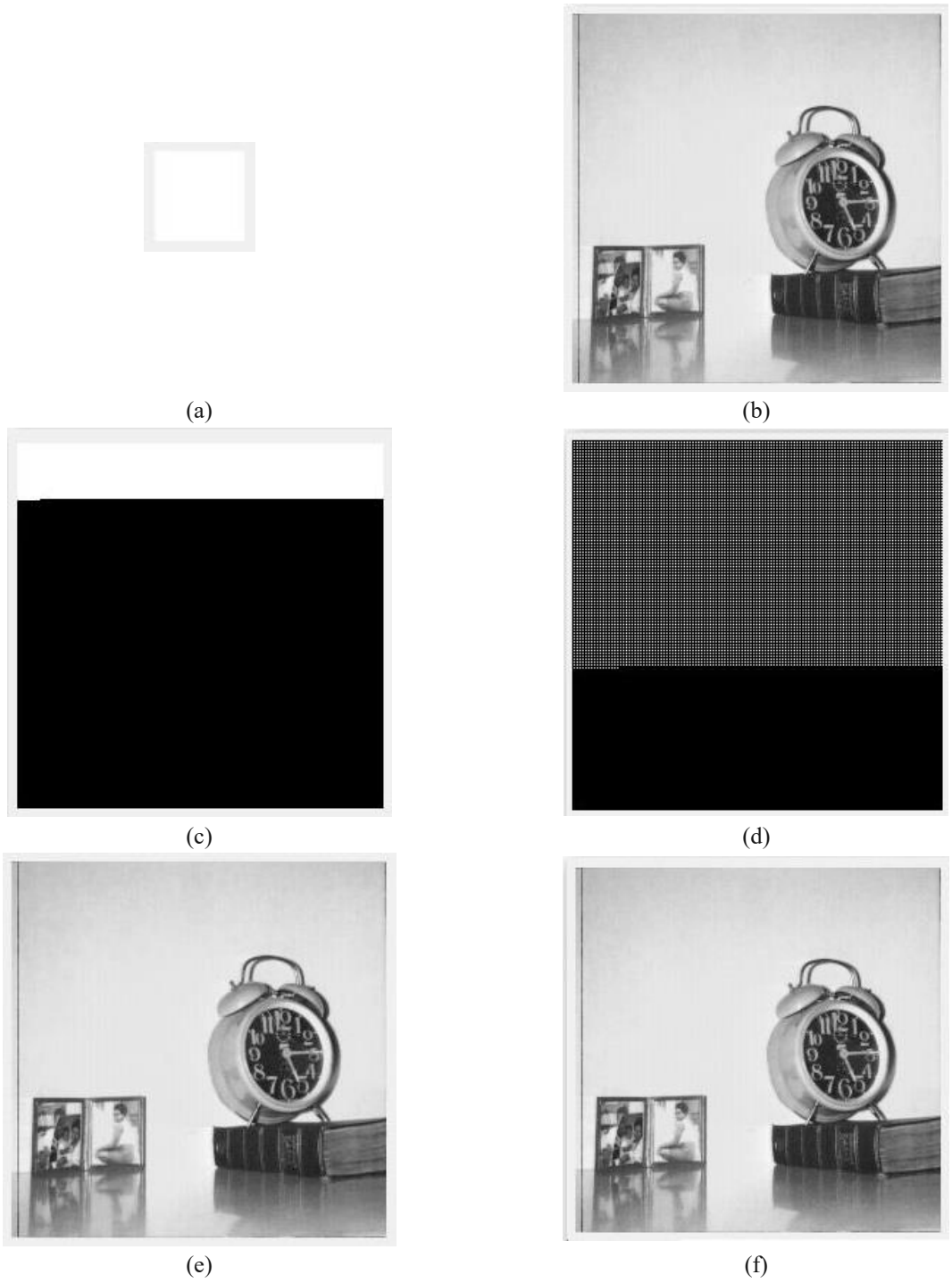
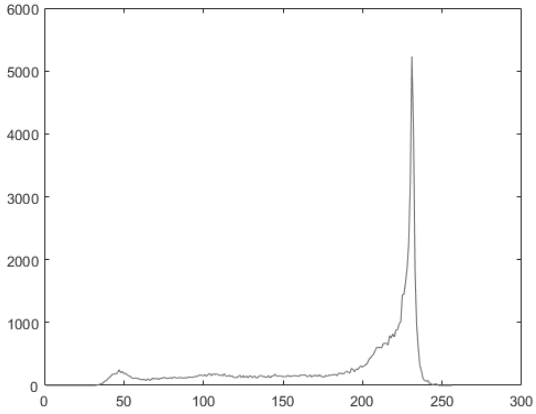
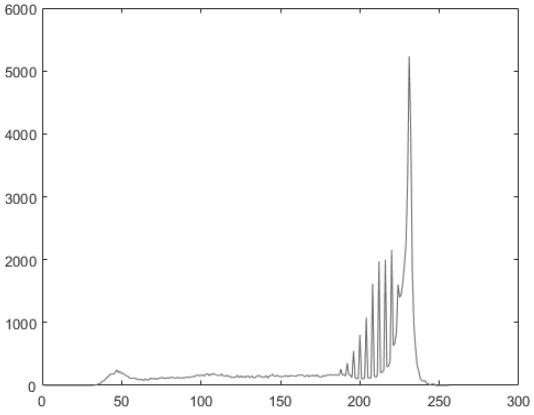


Figure 6: (a) Secret image; (b) cover image before embedding; (c) a demonstration figure of the selected pixels for embedding in white for LSB method (d) a demonstration figure of the selected pixels for embedding in white for 2D LSBG (1LSB to 1G) method; (e) the stego image using LSB (f) the stego image using LSBG (1LSB to 1G).

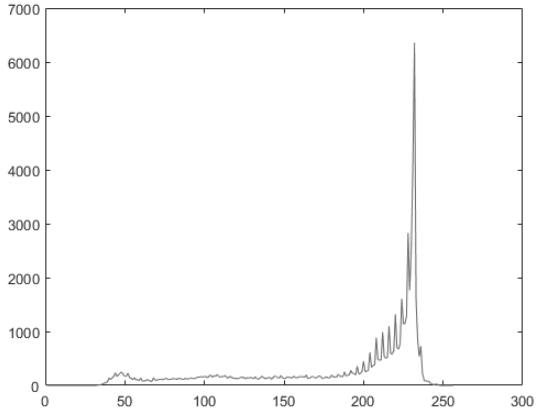
In Figure 7 which is composed of three subfigures, the histogram is generated for the selected cover image before embedding as seen in Figure 7 (a). The generated histogram of the resulting stego image acquired by using LSB method is shown in Figure 7 (b). Finally, in Figure 7 (c), we can observe the generated histogram of the resulting stego image acquired by the 2D LSBG method.



(a)



(b)



(c)

Figure 7: (a) Histogram of the cover image before embedding; (b) Histogram of the stego image after LSB embedding; (d) Histogram of the stego image after 2D LSBG (1LSB to 1G) embedding.

From the analysis of the histogram results with the cases applied, we can see the stego histogram having a high deviation that is in a specific range of the histogram and can only be noticed when compared to the cover histogram in a simple LSB method. In 2D LSBG method, on the other hand, the deviation in stego image histogram spreads in a higher range and the range cannot be accurately defined.

The MSE and PSNR measurements of the given cases are listed below in Table 2:

Table 2. MSE & PSNR Results.

Secret	Cover image	Method	MSE	PSNR
White image	Watch image	LSB (2 bpp)	0.5467	50.7528
White image	Watch image	2D LSBG (2 bpp) (1LSB to 1G)	0.5011	51.1307

If we study the MSE and PSNR results above, we notice the improvement achieved by LSBG method by reducing the MSE value and increasing the PSNR value compared to the applied LSB method.

5. Conclusion

Compared to LSB, applying LSBG method distributes and spreads deviation in a higher range in the histogram of the stego image. The interesting improvement is that the deviation effect is getting reduced since the deviation itself has been stretched and distributed in the histogram range.

For MSE and PSNR results of the given case, we can conclude that the LSBG method improved the system performance compared to LSB method by reducing the MSE value and logically increasing the PSNR value. As mentioned before, MSE improvement indicates an imperceptibility improvement in the stego image. For some other cases and experiments using other cover images, we did not have the same improvement in the MSE and PSNR values. This specific point shows the importance of selecting a suitable cover image for LSBG method which ensures the MSE and PSNR improvement.

According to our study, we recommend selecting a cover image with a narrow dynamic range histogram in order to ensure the improvement of the performance in applying LSBG method. We suggest using multiple options for cover images and applying multiple LSBG rates to them and analyzing the results, the case with the best result can be chosen. One recommendation that can be made is to apply the highest LSBG rate possible to ensure a greater distribution of LSB embedded pixels in the selected cover image. Another recommendation is to apply the shifting property of LSBG to enhance the key complexity of the used steganography method.

References

[1] R. J. Anderson and F. A. P. Petitcolas, "On the Limits of Steganography," *IEEE Journal on Selected Areas in Communications,* vol. 16, no. 4, pp. 474 - 481, 1998.

[2] Petitcolas, F. A. P. R. J. Anderson and M. G. Kuhn, "Information Hiding - A Survey," *Proceedings of the IEEE,* vol. 87, no. 7, pp. 1062 - 1078, 1999.

[3] L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread Spectrum Image Steganography," *IEEE Transactions on Image Processing,* vol. 8, no. 8, pp. 1075 - 1083, 1999.

[4] N. Nikolaidis and I. Pitas, "Digital Image Watermarking: an Overview," in *Proceedings IEEE International Conference on Multimedia Computing and Systems*, 1999.

[5] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," *IEEE, Computer ,* vol. 31, no. 2, pp. 313 - 336, 1998.

[6] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding," *IBM Systems Journal,* vol. 35, no. 3.4, pp. 313 - 336, 1996.

[7] G. L. Smitha and E. Baburaj, "A Survey on Image Steganography Based on Least Significant Bit Matched Revisited (LSBMR) Algorithm," in *International Conference on Emerging Technological Trends (ICETT)* , 2016.

[8] T. Shelare and V. Powar, "A Secure Data Transmission Approach Using B+trees In Steganography," in *International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, 2016.

[9] J. Kumar, "A Novel Approach to Image Steganography using Quadtree Partition," in *2nd International Conference on Next Generation Computing Technologies (NGCT)*, 2016.

[10] A. Abuadbba and I. Khalil, "Walsh-Hadamard Based 3D Steganography for Protecting Sensitive Information in Point-of-Care," *IEEE Transactions on Biomedical Engineering,* vol. 64, no. 9, pp. 2186 - 2195, 2017.

[11] V. Sharon, B. Karthikeyan, S. Chakravarthy and V. Vaithiyanathan, "Stego Pi : An Automated Security Module for Text and Image Steganography using Raspberry Pi," in *International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, 2016.

[12] A. A. J. Altaay, S. b. Sahib and M. Zamani, "An Introduction to Image Steganography Techniques," in *International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, 2012.

[13] M. Kude and M. Borse, "Skintone Detection Based Steganography Using Wavelet Transform," in *International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, 2016.

[14] J. Fridrich, M. Goljan and R. Du, "Detecting LSB Steganography in Color and Gray-Scale Images," *IEEE MultiMedia,* vol. 8, no. 4, pp. 22 - 28, 2001.