A Modified Image Steganography Method based on LSB Technique

Marwa M. Emam
Computer Science Department
Minia university, Egypt

Abdelmgeid A. Aly
Computer Science Department
Minia university, Egypt

Fatma A. Omara
Computer Science Department
Cairo university, Egypt

ABSTRACT

Data hiding techniques are considered very important roles with the rapid growth of intensive transfer of multimedia contents and secret communications. On the other hand, steganography is one of the most important information hiding techniques. By using steganography, information is hidden in carriers such as images, audio files, text files, and video files. In this paper, a modified steganography method based on the spatial domain is proposed. Our proposed method represents the message by six binary bits by using LSBraille method (Braille method of reading and writing for blind people) instead of using the ASCII encoding format. In this method, three bits of the message are hidden in a single pixel, and a true image is composed of three layers (Red, Green, and Blue) layer. Two bits are embedded in the Blue layer, and one bit is embedded in the green layer of the same pixel. In the Blue layer, the message is not only embedded in the least significant bit (LSB), but also the second and the third LSB may be changed. However, during each process of embedding, only one bit of the Blue layer is changed. From the experimental results, it is found that the proposed method achieves a very high Maximum Hiding Capacity (MHC), and higher visual quality as indicated by the Peak Signal-to- Noise Ratio (PSNR).

General Terms

Image Steganography, Data hiding in image.

Keywords

Steganography, Peak Signal-to-Noise Rate (PSNR), Mean Square Error (MSE), LSBraille, Maximum Hiding Capacity (MHC).

1. INTRODUCTION

Since the rise of the Internet, one of the most important factors of information technology and communication is the security of information. Cryptography has been used as a technique for securing the secrecy of communication, and many different methods have been developed to encrypt and decrypt data in order to keep a message secret. However, it is not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The used technique to satisfy that is called steganography [1]. Steganography is a technique used to transport information from one place to another place through public channel in a covert way [2]. The word steganography in Greek means " covered writing" (Greek words "***stegos***" meaning "cover" and "***grafia***" means "writing") [3]. In general, steganography is the art of hiding a message signal in a host signal without any perceptual distortion of the host signal. It hides the secret message within other innocuous looking cover files, called carriers, (i.e. images, text, audio, or video files) so that it can't be observed [4]. The most frequently used carriers are digital images. The using of digital images for steganography makes use of the weaknesses in the human visual system, which has a low sensitivity in random pattern changes and luminance. The human is incapable of discerning small changes in colour or patterns. Because of this weakness, the secret message can be inserted into the cover image without being detected [5].

Image Steganography is classified into two categories; ***spatial domain*** and ***transform domain*** [6, 7, and 8]. According to spatial domain, the secret data or secret message is directly embedded into the LSBs of image pixels. One of the most known examples of spatial domain method is LSB (**L**east **S**ignificant **B**it) insertion [9].while the schemes of transform domain embed the secret data within the cover image that transformed, such as the *Fourier transform*, *discrete cosine transform*, or the *wavelet transform*. Since most images have compressed by manipulating transform domain coefficients, the transform domain techniques add a fair amount of robustness against the destruction of the secret data due to lossy image compression [5]. The work in this paper concerns about the spatial domain.

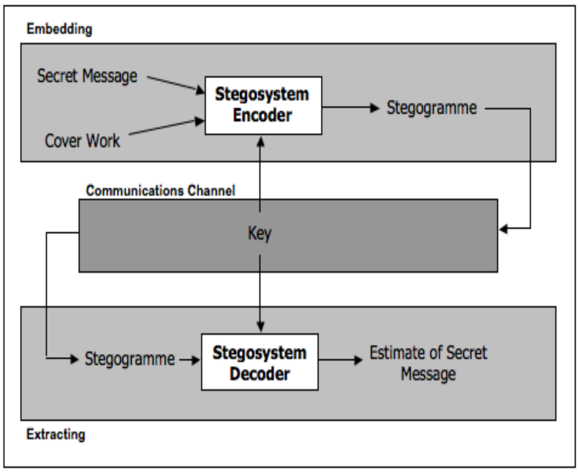

Fig 1: Basic Steganography System [11]

The basic model of steganography is shown in Figure 1. It consists of two algorithms, one for embedding, and one for extraction [1]. The embedding process consists of *cover file* (carrier), which is defined as the original file into which the required secure message is embedded, *payload* (secret message), and password is known as *stego-key*. The cover file with the secretly embedded is called the *stego*. The extraction process is traditionally a simple process, as it is simply an inverse of the embedding process, where the secret message revealed at the end. The challenge of using steganography in cover images is to hide as much data as possible with the fewest noticeable difference in the stego-image, where the final file is obtained after embedding the payload into a given cover file. It should have similar properties to that of the cover file.

The performance measurements for image distortion due to the embedding are the **M**ean **S**quared **E**rror (**MSE**) and the **P**eak **S**ignal-to-**N**oise **R**atio (**PSNR**) between the cover image and the stego image [10]. PSNR is one of the metrics to determine the degradation in the embedding image with respect to the cover image. MSE measures the difference between two images. PSNR and MSE are defined in equations 1 and 2 [10, 12, 13].

$$MSE = \left(\frac{1}{MN}\right) \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{ij} - X'_{ij}\right)^{2} \text{ ………….. (1)}$$

$$PSNR = 10 \log_{10} \frac{I^2}{MSE} \text{ …………………………….. (2)}$$

Where:

X_{ij} is the i^th row and the j^th column pixel in the original (cover) image, X'_{ij} is the i^th row and the j^th column pixel in the reconstructed (stego) image, M and N are the height and the width of the image, I is the dynamic range of pixel values, or the maximum value that a pixel can be taken, for 8-bit images; I=255.

The rest of this paper is organized as follows; related work will be discussed in section 2, the proposed method will be discussed in details in section 3, experimental results will be given in section 4. Finally, section 5 concludes the paper.

2. RELATED WORK

In [14], the authors have proposed a method that hides the secret message inside the cover image by representing the secret message characters by using Braille method of reading and writing for blind people that can save more than one-fourth of the required space for embedding. The proposed method used the Braille method representations of the characters where each character is represented by only six dots using the six – dots matrix that called (Braille Cell). The method starts by representing these characters (dots) as binary digits, each of which consists of 6 bits only instead of eight bits as in original LSB embedding method that uses the binary representation from the ASCII table. Therefore, by using this representation, two pixels are saved from each secret byte embedding process or more than one-fourth of the maximum hiding capacity for each cover image. Therefore, the maximum hiding capacity (MHC) has been increased and the PSNR of the LSB embedding technique has been enhanced.

In [15], a new approach for hiding message in digital image in spatial domain has been presented. According to work of this paper, a method that embeds two bits of information in a pixel, and alters one bit from one-bit plane has been introduced. However, the message does not necessarily place in the least significant bit of the pixel, the second less significant bit plane, the fourth less significant bit plane can also host the message, and only one alteration bit is allowed to be happen.

In [16], a new steganography technique has been proposed. According to this technique, nine bits of message can be hidden in a single pixel. A true image is composed of three elements R, G, and B components in each component 3 bits of message hidden. So a total of nine bits can be embedded in to a single pixel, i.e. more than one character (usually 8 bits are used to represent the ASCII value of a character). Therefore, the message is not only embedding in the least significant bit (LSB), but also the second LSB, third LSB, and the fourth LSB are susceptible to change. However, during each process of embedding only two bit of each component are changed. To have additional security, this method changes only the even columns of pixels.

In [17], the authors have introduced best approach for least significant bit (LSB) which based on image steganography that enhances the existing LSB substitution techniques to improve the security level of hidden information. The new security conception hides secret information within the LSB of image where a secret key encrypts the hidden information to protect it from unauthorized users. Hidden information is stored in different position of LSB of image depending on the secret key. Therefore, a bit of hidden information placed in either LSB of Green or Blue matrix of a specific pixel, which decided by the secret key. The cover image is divided into three matrices (Red, Green and Blue). The secret key is converted into 1, 0 array of bit stream. Secret key and Red matrix are used only for decision making to replace hidden information into either Green matrix or Blue matrix. Each bit of secret key is XOR with each LSB of Red matrix. The resulting XOR value decides that the 1 bit of hidden information will be placed with either LSB of Green matrix or Blue matrix (i.e. if the XOR value is 1, then the LSB of Green matrix is replaced by the first bit of hidden information. If the XOR value is 0, then the LSB of Red matrix is replaced by the first bit of hidden information). The same process will be continued until the hidden information is finished.

3. PROPOSED METHOD

Our proposed method will concern the spatial domain of the cover image. It is based on hiding six message bits in two pixels, the first three message bits will be hidden in the first pixel and the last three message bits will be hidden in the second pixel (see Figure 2). According to the proposed method, only two bits for each character of the cover image are changed; 1-bit from blue layer and 1- bit from green layer. According to the proposed method, the cover image and the secret message are considered as an input, each byte in the secret message is represented by its binary using LSBraille [14] where the byte from the secret message is represented by 6-bits only. Then, the cover image is converted into three layers (Red, Green, and Blue) layer. After that each pixel in the (Blue, and Green) layers is converted by its binary using the ASCII encoding format. First, we start with the Blue layer, then the Green layer of the same pixel and so on to embed the full secret message. In the Blue layer, two bits per pixel are embedded, the message is not only embedded in the first least significant bit (LSB), but also the second least significant bit, and the third least significant bit are allowed to be changed. However, during each process of embedding only 1-bit of the Blue layer will allowed to change, this process is done by taking the last three bits of the Blue layer pixel and entered it in the XOR Gate, and applying the following equations:

$$B1\ XOR\ B2 = N2 \text{ ……………………………….. (3)}$$
$$B2\ XOR\ B3 = N3 \text{ ……………………………….. (4)}$$

Where, B1 is the first least significant bit, B2 is the second least significant bit, and B3 is the third least significant bit of the Blue layer.

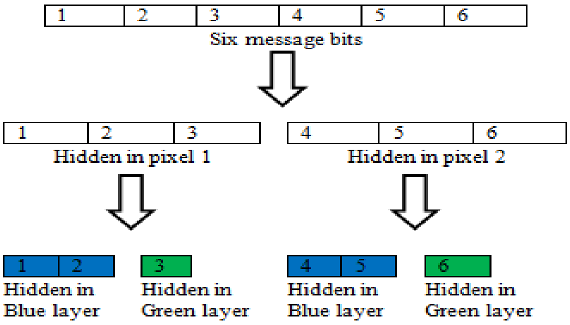

Fig 2: The secret Message Bits

In this method, if the output N2 and N3 are the same as the two secret message bits, then we do not make any change to the pixel. If the message bits, which are embedded, are different from any of those outputs, then we have to change only one bit from the original pixel in a way to cause the output of equations 3, 4 is equal to the embedded bits. The goal is to change only one bit in the pixel of the Blue layer, the two message bits are embedded by changing only one bit, which may be one of the following:

- Least significant bit.
- Second least significant bit.
- Third least significant bit.

Example

Suppose (0 0 0) are the first three less significant bits of the Blue layer from right it is labeled by B1, B2, and B3. By applying equations, 3, and ~~4,~~ N2 is equal 0, and N3 is equal 0. Suppose the secret message to be embedded is (0 0), in this case the two message bits to be embed is equal to N2 and N3. So, the three bit pixels will be changed, thus the cover bits and the stego bits are the same.

Suppose (0 1) are the two bit message to be embedded. The first bit is equal to N2 and the second bit is not equal to N3. Therefore, to embed this message we must change either the first, second, or the third LSB. By changing the third LSB, the stego pixels become (**1** 0 0). Such that N2 and N3 becomes 0 1, which is the same as the message bits to be embed.

Suppose (1 0) are the two bit message to be embedded. The first bit is not equal to N2 and the second bit is equal to N3. Therefore, to embed this message we must change either the first, second, or the third LSB. Then, by changing the second LSB, the stego pixels become (0 **1** 0). Such that N2 and N3 becomes 1 0, which is the same as the message bits to be embed.

Suppose (1 1) are the two bit message to be embedded. The message bits are not equal to N2 and N3. Therefore, to embed this message, we must change either the first, second, or the third LSB. Then, by changing the first LSB, the stego pixels become (0 0 **1**). Such that N2 and N3 becomes 1 1, which is the same as the message bits to be embed.

Suppose (1 0 1) are the first three less significant bits of the Blue layer. Then N2 and N3 are (1 0). If the secret message is (0 1), the message bits are not equal to N2 and N3. Therefore, to embed this message we must change either the first, second, or the third LSB. The stego pixels become (**1** 0 0). Such that N2 and N3 becomes 1 1, which is the same as the message bits to be embed.

Then the third bit of the message in the least significant bit of the Green layer will embedded in the same pixel, and so on as.

The pseudo code of our proposed method is as follows:

Algorithm: Message Embedding using XOR gate and LSBraille method

Input: Cover Image C, Secret Message M.

Output: StegoImage S.

Steps:

```
1.  Split the Cover Image C into three channels Red (R), Green (G), Blue (B).
2.  Convert B, and G into blocks; B= {$b_1, b_2, b_3$ ……$b_n$}, G= {$g_1, g_2, g_3$ ……$g_n$} where each block is only one pixel.
3.  Convert each block from B, and G to its ASCII format.
4.  Split M into characters, M= {$m_1, m_2, m_3$ ……..$m_n$}.
5.  Take $m_i$ from M, and Convert it into Braille 6-bit representation by using LSBraille method [14].
6.  i =1                // where i is B and G counter.
7.  Take $b_i$ from B, and $g_i$ from G.
8.  Take the last three bits from $b_i$ .
9.  Apply the equation (2) and (3) to obtain the output N2, N3.
10. If ($m_i$ (1)=N2 & $m_i$ (2)=N3) Then
     b (i,6:8)=b(i,6:8)            // no change occurs to $b_i$
     g (i, end)= $m_i$ (3)            // Apply LSB
       i= i+1
    Else If ($m_i$(1) ! = N2 & $m_i$(2) = N3) Then
       b (i, 7:7)= NOT ( b(I, 7:7) )
       g (i, end)= $m_i$ (3)
       i= i+1
    Else If ($m_i$(1) = N2 & $m_i$(2) ! = N3) Then
        b (i, 6:6) = NOT ( b(i, 6:6) )
        g (i, end)= $m_i$ (3)       // Apply LSB
        i= i+1
    Else If ($m_i$(1) ! = N2 & $m_i$(2) ! = N3) Then
        b (i, 8:8) = NOT ( b (i, 8:8) )
        g (i, end)= $m_i$ (3)          // Apply LSB
        i=i+1
    End if
    End if
    End if
    End if
11. Repeat steps 9, and 10,  but on step 10 change the message bits $m_i$ by the last three bits ; m(4), m(5), m(6)
12. Repeat steps from 6 to 11 until the whole M has been embedded in C.
13. Convert B, and G from binary to decimal.
14.  Merge the three channels R, G, B again to construct the stegoImage S.
```

Therefore, each byte from the secret message will hide in two pixels only. This will satisfy a very high embedding capacity. We can calculate the maximum number of bytes that can be hidden in any image (Maximum Hiding Capacity) by using this formula:

$$Maximum\ Hiding\ Capacity(MHC) = (Image\ width \times Image\ height)/2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

Suppose we have an **(512 x 512)** cover image, by using equation 5 we can hide **131,072** bytes or more than **1,048,576** bits, which approximately is equal to **30** pages of word file at font size 12 (depending on the font settings).

4. EXPERIMENTAL RESULTS

In this section, the proposed method will be implemented and evaluated by comparing it with SLDIP and ESLDIP, DWT methods, as well as, the method in [16] using different messages with different lengths and hiding them in some cover images (i.e., standard images). The proposed and SLDIP methods are implemented using MATLAB 11.1.0 software running on a personal computer with a 2.27 GHz Intel (R) Core (TM) i3 CPU , 4 GB RAM and windows 7 as the operating system.

The results of the comparative study between our method and the SDLP[5] and ESLDP[18] methods by using different number of characters (bytes) secret message and 512 x 512 cover images (e.g., Lena, Baboon, Pepper) are presented in Table 1, and Table 2, and Figures 5, 6.

Table 1: Comparison between PSNRs of method SLDIP [5] and our proposed method

	Cover image	Message capacity (bytes)	PSNR (dB)	
			SLDP	Proposed method
512 x 512	Lena	75.836	40.4019	49.1564
	Baboon	82.407	40.0712	47.7283
	Pepper	75.579	40.5886	47.4422

Table 2: Comparison between PSNR of method ESLDIP [18] and our proposed method

	Cover image	Message capacity (bytes)	PSNR (dB)	
			ESLDIP	Proposed method
512 x 512	Lena	75.836	45.72295	49.1564
	Baboon	82.407	45.33670	47.7283
	Pepper	75.579	45.42819	47.4422

According to the comparative results, it is found that the PSNR of our method is better than that the SLDIP, and ESLDI. In addition, the stego image quality of our method is very high relative to the SLDIP, and ESLDIP methods. According to the results in Table1 and Table 2, the average improvement of SLDIP method and ESLDIP are 40.3539 % and 45.49 % respectively, while the average improvement of our method is 48.19 %. So, the average improvement of our method relative to SLDIP and ESLDIP methods are 7.84%, 2.7% respectively.

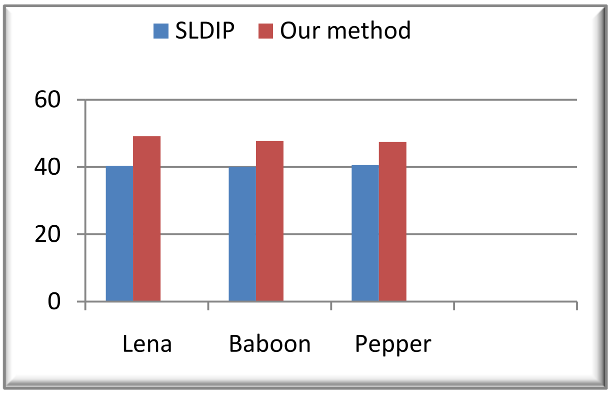

Fig .3: comparison between PSNR values of Table1

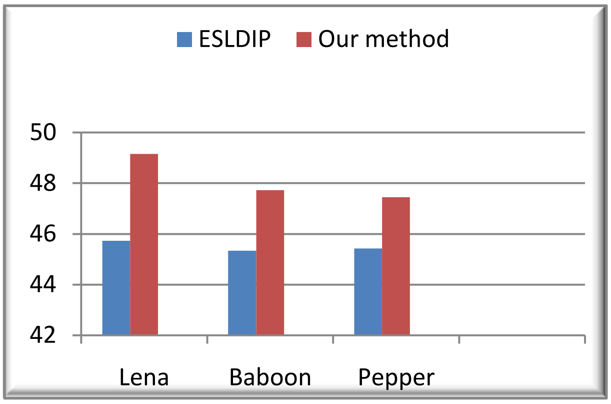

Fig .4: comparison between PSNR values of Table 2

Table 3, and Figure 5 represent the comparative results of our method and DWT [19] method by using (1000) byte (secret message character) and 256 x 256 cover image (Lena, Baboon, and Pepper).

Table 3: Comparison between PSNR of DWT [19] method and our method

	Cover image	Message capacity (bytes)	PSNR (dB)	
			DWT	Proposed method
256 x 256	Lena	1000	60.3033	63.0432
	Baboon	1000	60.2393	63.0220
	Pepper	1000	60.1	63.0535

According to the comparative results in Table3, Figure 5, the average improvement of DWT [19] method is 60.2142%, while average improvement of our method is 63.04%. So, the average improvement of our method relative to DWT [19] method is 3.2%.

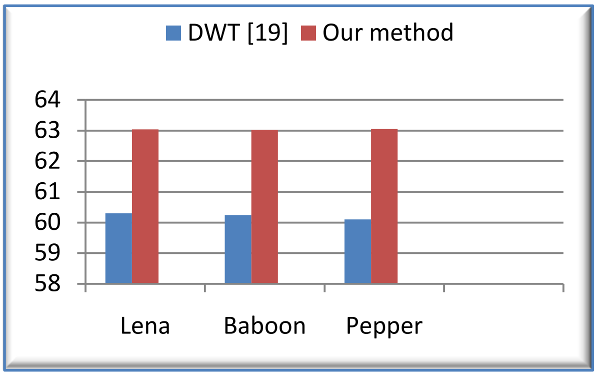

Fig.5: comparison between PSNR values of Table 3

Finally, Table 4 represents the comparative result of our method and method in [16] by using different messages as seen in cases 1, 2, 3, and case 4, and 512 x 512 cover image (Pepper).

Table 4: comparison between PSNR of method in [16] and our method

Cover image Pepper 512 x 512	Message Cases	PSNR (dB)	
		Method in [16]	Proposed method
	Case 1	72	77.0270
	Case 2	69	74.2454
	Case 3	67	72.3467
	Case 4	65	66.5551

Where, case1, 2, 3, and 4 are the hidden message which are used in [16].

The message in case 1; "Steganography seeks to provide a covert communication channel between two parties."

The message in case 2; "Steganography seeks to provide a covert communication channel between two parties. It is commonly framed as the prisoners' problem. Two prisoners, Alice and Bob,"

The message in case 3; "Steganography seeks to provide a covert communication channel between two parties. It is commonly framed as the prisoners' problem. Two prisoners, Alice and Bob, are permitted to communicate between one another, while under the surveillance of a Warden."

The message in case 4; "Steganography seeks to provide a covert communication channel between two parties. It is commonly framed as the prisoners' problem. Two prisoners, Alice and Bob, are permitted to communicate between one another, while under the surveillance of a Warden. Steganography seeks to provide a covert communication channel between two parties. It is commonly framed as the prisoners' problem. Two prisoners, Alice and Bob, are permitted to communicate between one another, while under the surveillance of a Warden."

Figure 6 shows the image that is used as a cover image and the histogram of its R, G, and B layers which are used to embed the message given in case 3. Figure 7 shows the stego image which is obtained after embedding that message and its corresponding histograms.

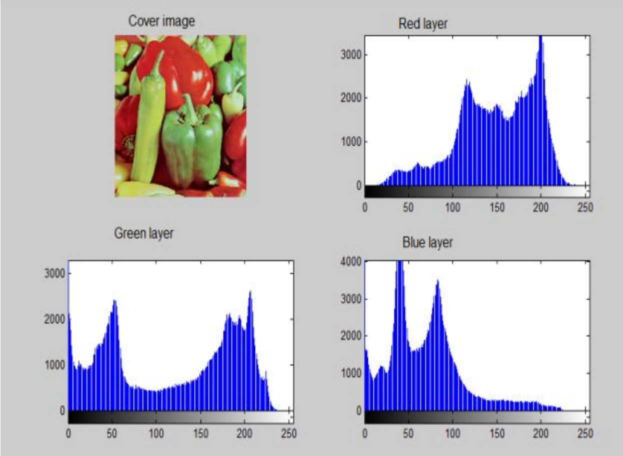

Fig. 6: cover image and histograms

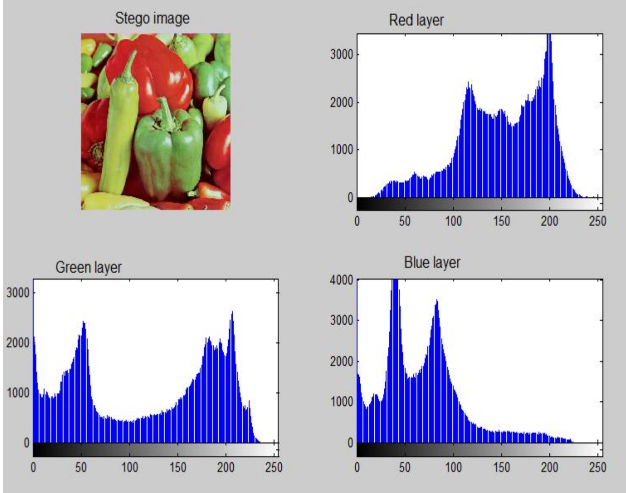

Fig.7: stego image and histograms

The comparative results of our method and method in [16] are presented in Figure 8.

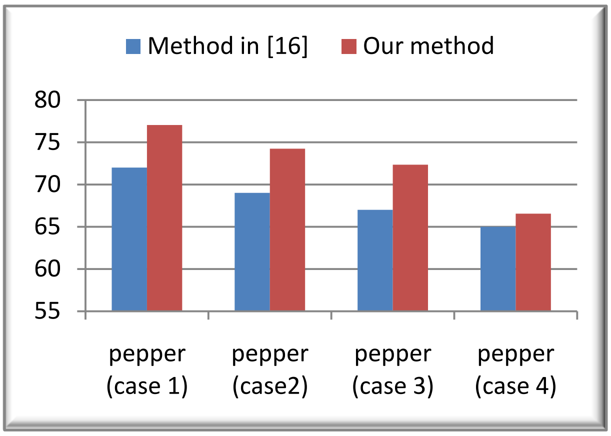

Fig.8: comparison between PSNR values of Table 4

According to the comparative result in Table 4, and Figure 8, it is found that our method has more PSNR value than that the method in [16] which means the stego image quality of our method is also higher. Therefore, the average improvement of method in [16] is 68.25 %, while the average improvement of our method is 72.6%. So, our method outperforms the method in [16] by 4.35%.

Generally, our method outperforms the DWT [19], method in [16], and SLDIP and ESLDIP methods by producing high quality stego image.

5. CONCLUSION

In this paper, a new Steganographic method has been proposed, which uses the LSBraille method to improve the capacity of the hidden data, and provides high embedding capacity and PSNR. To evaluate the proposed Steganographic method, a comparative study has been done among our proposed method, SLDIP, ESLDIP, and DWT methods, as well as, with the method in [16]. According to the experimental results, it is found that the proposed method is considered an effective Steganographic method because it satisfies the Steganographic system goals with high quality and PSNR.

6. REFERENCES

[1] S. Deepa and R. Umarani, “A Study on Digital Image Steganography”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 1, PP. 54-57, January 2013.

[2] K.Nitin K and N. Ashish V, “Comparison of Various Images Steganography Techniques”, International Journal of Computer Science and Management Research, Vol. 2, Issue 1, PP. 1213-1217, January 2013.

[3] A. Nag, S. Ghosh, S. Biswas, D. Sakar, and P.P. Sakar, “An Image Steganography Technique using X-Box Mapping”, IEEE- International Conference On Advances In Engineering, Science and Management(ICAESM-2012), Vol. 3, Issue 12, PP. 709-713, March 2012.

[4] A. A. Ali and A. H. Seddik, “New Image Steganography Method By Matching Secret Message With Pixels Of Cover Image (SMM)”, International Journal of Computer Science Engineering and Information Technology Research (IJCSITR), Vol. 3, Issue 2 ,PP. 1-10, Jun 2013.

[5] A. A. Radwan, A. Swilem, and A.H. Seddik, "A High Capacity SLDIP (Substitute Last Digit In Pixel) ", Fifth International Conference on Intelligent Computing and Information Systems (ICICIS 2011), Ain Shams University, Egypt, 30 June - 3 July,PP . 156 – 160, 2011.

[6] S. Nazari, A-M. Eftekhari, and M. Sh. Moin, “Secure Information Transmission using Steganography and Morphological Associative Memory”, International Journal of Computer Applications, Vol. 61, No. 7, PP. 23-29, January 2013.

[7] S. Arora and S. Anand, “A Proposed Method for Image Steganography using Edge Detection”, International Journal of Emerging Technology and Advanced Engineering, Vol. 3, Issue 2, PP. 296-297, February 2013.

[8] C. Vanmathi and S. Prabu, “A Survey of State of The Art Technique of Steganography”, International Journal of Engineering and Technology (IJET), Vol. 5, No. 1, PP. 376-379, Feb-Mar 2013.

[9] Y. K. Jain and R. R. Ahirwal, “A Novel Image Steganography Method with Adaptive Number of Least Significant Bits Modification Based on Private Stego-Key”, International Journal of Computer Science and Security, Vol. 4, Issue 1, PP. 40-94, March 2010.

[10] S. Sharda and S. Budhiraja, “Image Steganography: A Review”, International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol.4, Issue 1, PP. 707-710, January 2013.

[11] A. A. Ali and A. H. Seddik, “New Text Steganography Technique by using Mixed-Case Font”, International Journal of Computer Applications, Vol. 62, No. 3, PP. 6-9, January 2013.

[12] J. Jasril, I. Marzuki, and F. Rahmat, “Modification Four Bits of Uncompressed Steganography using Least Significant Bit (LSB) Method”, Advanced Computer Science and Information Systems (ICACSIS), IEEE, PP. 287-292, 2012.

[13] G. Swain and S. K. Lenka, “A Novel Approach to RGB Channel Based Image Steganography Technique”, International Arab Journal of e-Technology, Vol. 2, No. 4, PP. 181-186, June 2012.

[14] A. A. Ali and A. H. Seddik, “Image Steganography Technique By Using Braille Method of Blind People (LSBraille)”, International Journal of Image Processing (IJIP), Vol. 7, Issue 1,PP. 81-89, 2013.

[15] A. Daneshkhah, H. Aghaeinia, and S. H. Seydi, “A more Secure Steganography method in Spatial Domain”, Second International Conference on Intelligent System, Modelling and Simulation, IEEE, PP. 189-194, 2011.

[16] S. A. Raj and T. Soumya, “A Youthful Procedure for Spatial Domain Steganography”, Third International Conference on Advances in Computing and Communications, IEEE, PP. 300-303, 2013.

[17] S. M. M. Karim, M. S. Rahman, and M. I. Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 201 I) , Dhaka, Bangladesh, PP. 286-291, December -2011.

[18] A. H. Seddik, “Enhancing the (MSLDIP) Image Steganographic method (ESLDIP Method)”, International Conference on Graphic and Image Processing (ICGIP), Vol. 8285, 2011.

[19] A. Rana, N. Sharma, and A. Kaur, “Image Steganography Method based On KOHONNEN Neural Network”, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, PP. 2234-2236, 2012.