International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.5, Sep-Oct. 2012 pp-3835-3840 ISSN: 2249-6645

A Comparative Study of Combination of Different Bit Positions In Image Steganography

Ramanpreet Kaur[1], Baljit Singh[2], Ishpreet Singh[3]
[1](Research scholar of Department of CSE and IT, BBSBEC Fatehgarh Sahib, Punjab, India)
[2,3](Associate Prof of .Department of CSE and IT, BBSBEC Fatehgarh Sahib, Punjab, India)

ABSTRACT: *Steganography hides the existence of the data inside any cover file. There are different file formats used in steganography like text, image, audio and video. Out of these file formats image steganography is followed in this paper .One of the major objective of hiding data using image steganography is to hide the data in an image, so that the changes in the intensity of the colors of image must not be visible to, human eye. The focus of this paper is on spatial domain technique i.e. LSB technique of image steganography. Method used in the paper hides the data in combination of LSBs instead of hiding the data only in least significant one bit. Combination of bits used are LSB (1, 2) bits and (2, 3) bits. Results are compared qualitatively and quantitatively using parameters PSNR, MSE, BER, Entropy, Standard deviation.*

Keywords: *BER, Entropy, Image steganography, LSB technique, MSE, PSNR, Std. deviation.*

I. INTRODUCTION

Due to the increase in the use of internet it becomes important to secure the sensitive data and information on internet. Therefore, to secure the sensitive information on the internet various techniques like cryptography, steganography are used to hide the data in digital media. Cryptography only keeps the contents of the message secret but sometimes it is necessary to keep the existence of the message secret. So, a technique which keeps the existence of a message secret is known a steganography [1].

This paper explores the steganography technique for security purpose. Paper presents the LSB technique of image steganography in which data is hidden in the combination of LSBs of image pixels.

II. STEGANOGRAPHY

1. Steganography

Steganography is a method of secret communication that insert the message inside any cover in the way that third party should not be able to find it out that a message is hidden in the cover. The cover can be an image, text, audio or video. The word steganography is derived from the Greek word 'Steganos', which means covered or secret and 'graphy' means writing or drawing, that combined means, "Covered Writing" or "Secret Writing".

The goal of steganography is to hide the sensitive information in a cover so that nobody can guess the existence of it. Information hiding technique becomes important in a number of application areas [2, 3]. The growing need of communications through the internet demands the confidentiality and integrity of data to protect against unauthorized access. Therefore, for the security of data from unauthorized users there is a need of hiding the data. There are various techniques of steganography of which image steganography technique is most useful.

2. Image Steganography

An image is an array of M*N matrix. Each and every pixel has a numerical value which represents the color and light intensity of the pixel [4]. Images are more popular cover files for transmission over the internet due to harmlessness and attraction. In image steganography, data is to be inserted into the cover image that gives the resultant stego-image [5, 6].

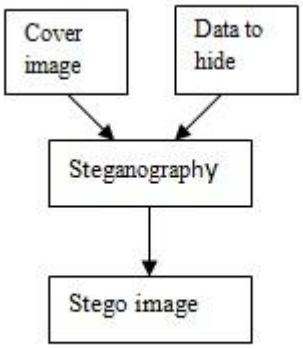


Fig.1. Process of hiding data in image.

There are various steganographic techniques for image file formats are classified as [2]:

1. Spatial domain technique.
2. Masking and filtering.
3. Transform techniques.

Spatial domain technique embeds the message directly in the intensity of the pixels. Spatial domain technique includes least significant bit (LSB).

3. LSB Technique

This is one of the simplest and easiest method of hiding the data in images. In this technique, the data in the binary form is to be hidden into the LSBs of the carrier bytes or in pixels of image. The overall change to the image is so small that human eye would not be able to discover**.** In 24-bit images each 8-bit value refers to the red, green and blue color. But in 8–bit images each pixel is of 8-bits, so each pixel stores maximum 256 colors [7, 8].

For example, in our method to hide a letter A whose binary value is 10000001, in the combination of LSBs of an 8-bit image then we need four pixels.

Suppose the original four pixels are:
00100101
11100101

11001011
01000111
Secret data i.e. A (10000001)
The resulting four pixels are as follows:
00100101
11100100
11001000
01000110
Only 4 bits needed to be changed to embed the secret data into the first 4 pixels of the image. On average, LSB requires that only half the bits in an image be changed to hide a secret message [9, 10, 11].

III. Proposed Work

The proposed work includes the hiding of data in combination of two LSBs. The selected pair of bits (1, 2) or (2, 3) of pixels in image has been replaced with the data bits. The cover image selected is of grayscale.
Procedure:

1. Extract all the characters of secret data and store them in character array.
2. Replace the pair of bits (1, 2) or (2, 3) of selected pixel with length of data and bits of characters of Character-Array.
   Suppose to hide bits of character 8 bits of the first pixel are:

0	0	1	0	0	1	0	0

   To hide character A whose binary value is 10000001 and 2-bits of A are:

1	0

3. Repeat steps till all the characters have been embedded.
4. Obtained image will hide all the characters that we input.
5. Compare pair bits (1, 2) and (2, 3).

We have used performance parameters like PSNR, MSE, BER, entropy, std. deviation to check the impact on image, of replacement of different pair bits.
PSNR stands for peak signal to noise ratio. It used to measure the quality of images. Higher the PSNR value, better the quality of image. It is estimated in decibels (db).It is defined as:

$$\text{PSNR} = 10\log_{10}\frac{R^2}{\text{MSE}} \qquad \textbf{(1)}$$

In grayscale images R is 255.
MSE stands for the mean square error. Lower the value of MSE, better the quality of image. It is defined as:

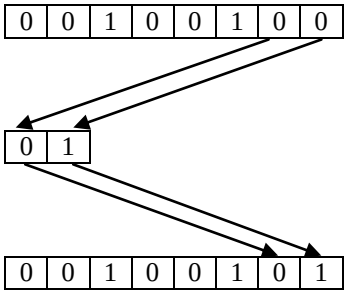
$$\text{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij} - y_{ij})^2 \qquad \textbf{(2)}$$

Here M and N represents the no. of rows and columns of the image respectively. x_{ij} is the original image and y_{ij} is the stego image.

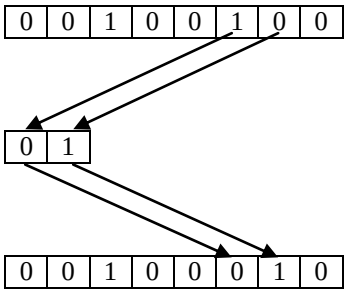
BER is bit error rate. It is explained as:

BER=1/PSNR **(3)**

To replace the pair of bits (1, 2) of first pixel with the data bits:



Similarly, to replace the pair of bits (2, 3) of first pixel with the 2Bits of A are:



Repeat the same process till all the bits of A has been embedded.

Entropy is used to measure the randomness of image.
It is defined by the following equation:

$$\text{Entropy} = -\sum_{i=1}^{l} P_i \log_2(P_i) \qquad \textbf{(4)}$$

Where P_i is the probability of getting a particular intensity and l is the total intensity values.

Standard deviation is defined by the equation:
Standard deviation

$$\sigma_j = \left[\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2\right]^{1/2} \qquad \textbf{(5)}$$

Where $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$

IV. EXPERIMENTAL RESULTS

Experimental results evaluate the performance by hiding the data in LSB bit pairs of pixels in gray scale images using MATLAB. Various performance parameters like PSNR, MSE, BER, entropy, standard deviation have been used to evaluate the performance. The experiment has been taken out on various images which includes both standard and natural images by embedding ASCII characters. Figure 2-10 shows original images, stego-images with data hiding on 1, 2 bit pair and stego-images with data hiding on 2, 3 bit pair. Figures from 11 to 28 shows PSNR, BER, MSE graphs of different images. Table 1 and Table 2 shows the results of three images

Lena, Autumn and Neptune where quality factor is 255.Table 1 shows performance of images on bit pair (1, 2) and Table 2 shows the performance of images on bit pair (2, 3).

Fig.2. Original Lena

Fig.3. Original Autumn

Fig.4.Original Neptune

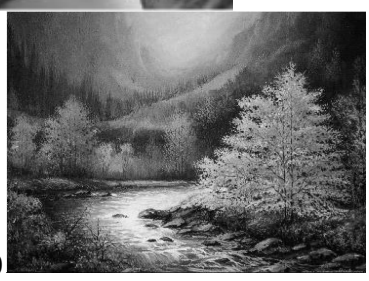


Fig.5.Stego-image (1, 2)

Fig.6.Stego-image (1, 2)

Fig.7.Stego-image (1, 2)

Fig.8.Stego-image (2, 3)

Fig.9.Stego-image (2, 3)

Fig.10.Stego-image (2, 3)

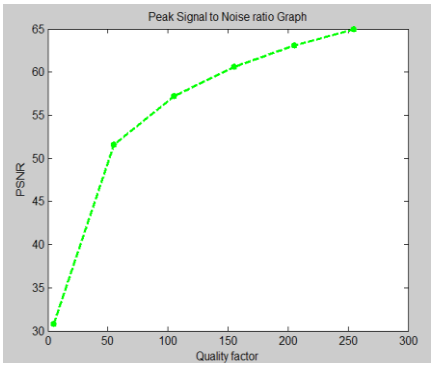


Fig.11.PSNR of Lena (1, 2)

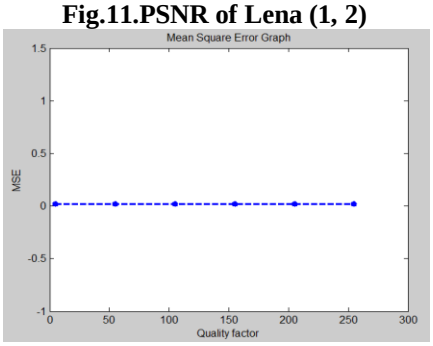


Fig.12.MSE of Lena (1, 2)

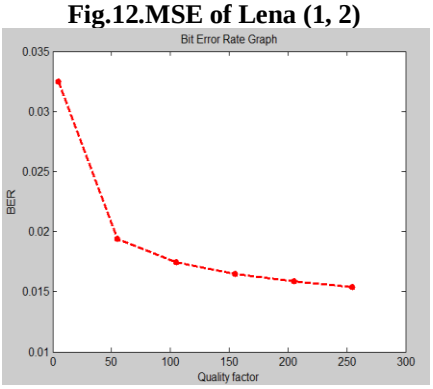


Fig.13.BER of Lena (1, 2)

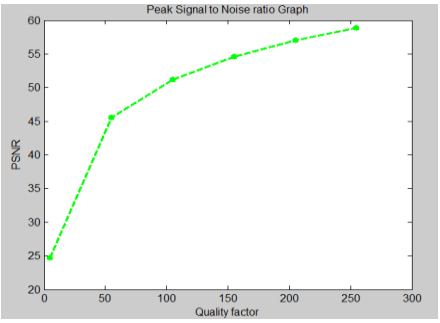


Fig.14.PSNR of Lena (2, 3)

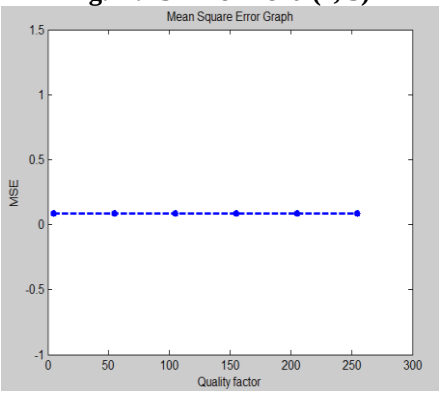


Fig.15.MSE of Lena (2, 3)

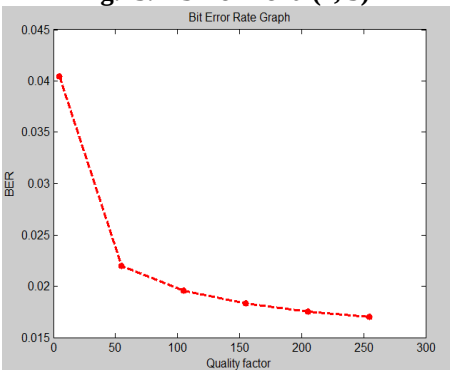


Fig.16.BER of Lena (2, 3)

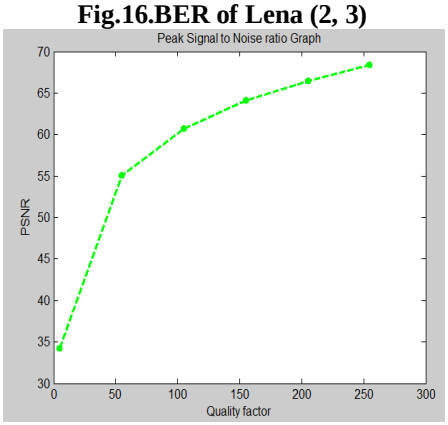


Fig.17.PSNR of Autumn (1, 2)

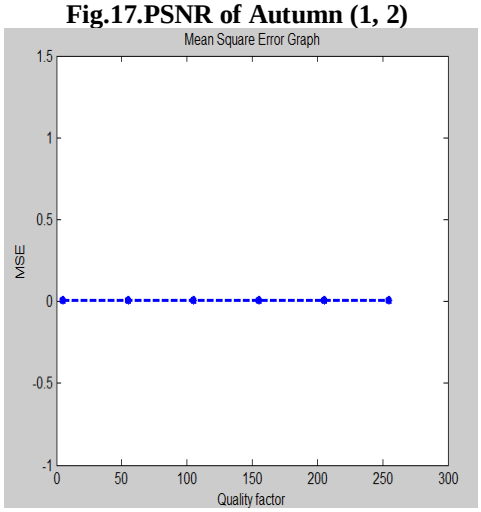


Fig.18.MSE of Autumn (1, 2)

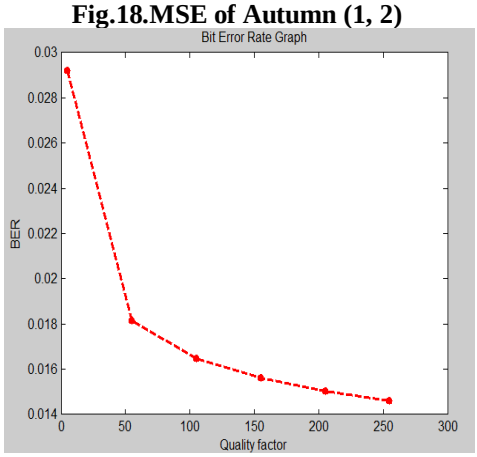


Fig.19.BER of Autumn (1, 2)

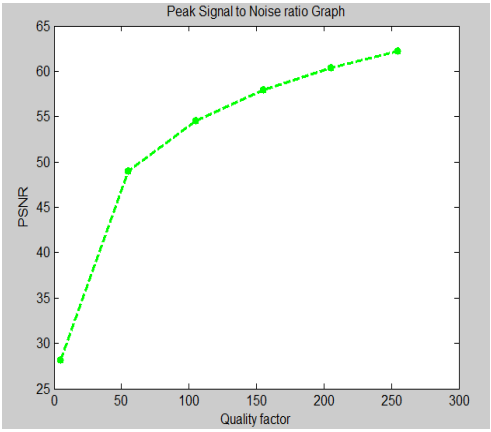


Fig.20.PSNR of Autumn (2, 3)

Fig.21.MSE of Autumn (2, 3)

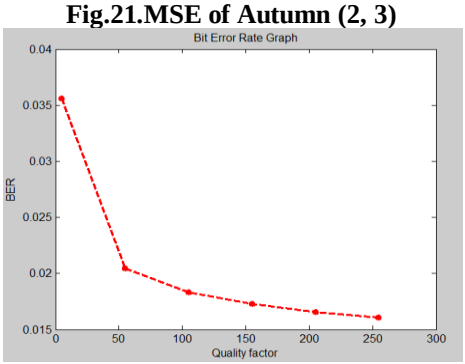


Fig.22.BER of Autumn (2, 3)

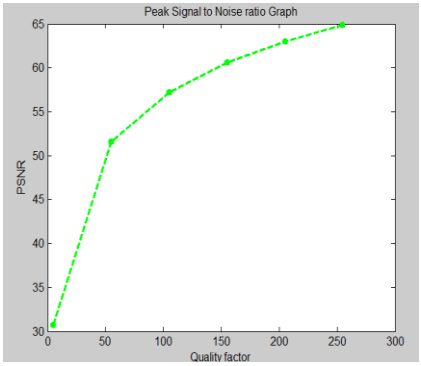


Fig.23.PSNR of Neptune (1, 2)

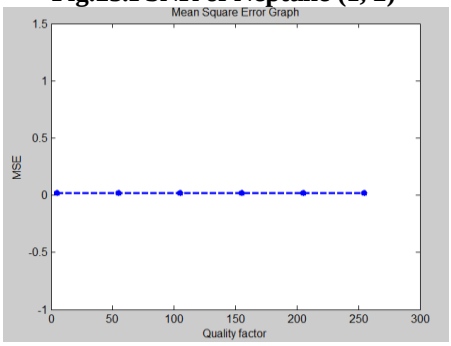


Fig.24.MSE of Neptune (1, 2)

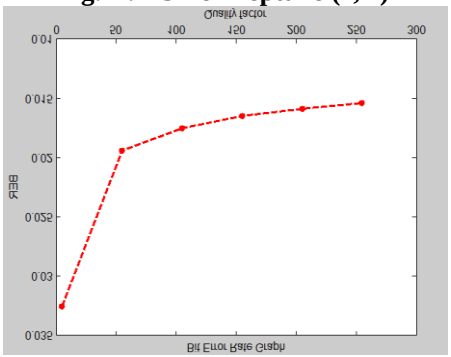


Fig.25.BER of Neptune (1, 2)

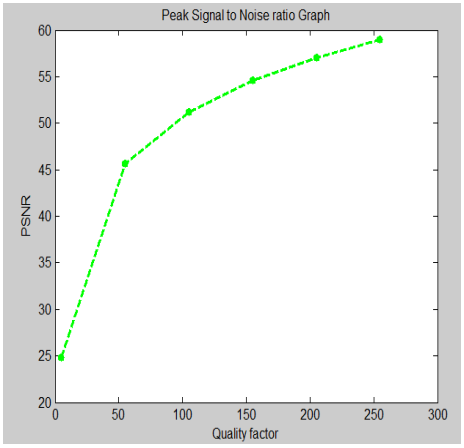


Fig.26.PSNR of Neptune (2, 3)

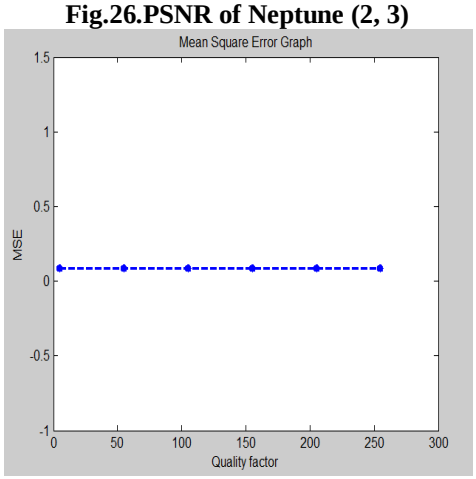


Fig.27.MSE of Neptune (2, 3)

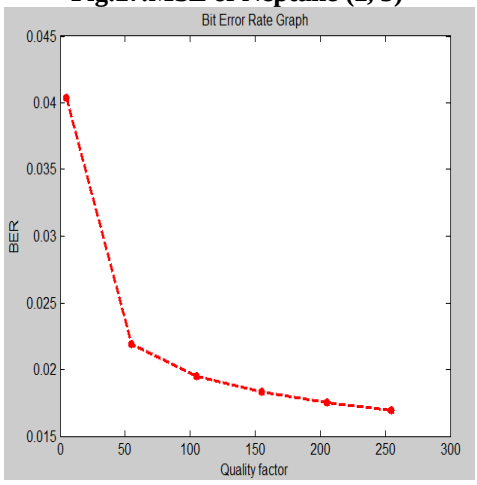


Fig.28.BER of Neptune (2, 3)

Table.1. Results of (1, 2) bit

Parameters	Images		
	Lena	Autumn	Neptune
PSNR	58.8896	62.2717	58.9339
BER	0.0169809	0.0160587	0.0169682
MSE	0.0839691	0.0385403	0.0831168
Entropy	7.44642	7.65937	7.52104
Std. Dev.	12.5371	9.97252	13.8436

Table.2. Results of (2, 3) bit

Parameters	Images		
	Lena	**Autumn**	**Neptune**
PSNR	64.9506	68.3888	64.9057
BER	0.0153963	0.0146223	0.015407
MSE	0.0207977	0.00942315	0.0210141
Entropy	7.44612	7.65929	7.52059
Std. Dev.	12.5384	9.97278	13.842

V. Conclusion

This paper shows the results of comparison of hiding the data in LSB (1, 2) bit pair and in (2, 3) bit pair. It is concluded that hiding the data in the (1, 2) bit pair shows better results than hiding the data in (2, 3) bit pair. Test is made on various images which includes both standard and natural images of which three are shown, using more than one parameter. The parameter implies that hiding the secret message in (1, 2) bit pair is less visible to human eye i.e. quality of image is better as compare to the second one. In future, we can also extend this method for more combination of bit positions and this can also be performed on the color images.

References

[1]. T. Morkel, J.H.P. Eloff, M.S. Olivier, 2005. "An Overview of Image Steganography", in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa.

[2]. Muhalim Mohamed Amin, Subariah Ibrahim, Mazleena Salleh and Mohd Rozi Katmin, 2003. "Information Hiding using Stegnography", Department of Computer System & Communication Faculty of Computer Science and Information system, universiti teknologi malaysia.

[3]. Arvind Kumar and Km. Pooja, 2010. "Steganography- A Data Hiding Technique", International Journal of Computer Applications, Vol. 9, No.7.

[4]. Neil F. Johnson, Sushil Jajodia 1998. "Exploring Steganography: Seeing the Unseen", Dept. of Information and Software Systems Engineering, George Mason University, Fairfax.

[5]. Jagvinder Kaur and Sanjeev Kumar, 2011"Study and Analysis of Various Image Steganography Techniques", International Journal of Computer Science and Technology (IJCST), ISSN: 2229-4333(Print)|ISSN:0976-491(Online),Vol.2,Issue3.

[6]. Kaveh Ahmadi, 2011. "A New Method for Image Security and Data Hiding in Image", American Journal of Scientific Research ISSN 1450-223X Issue 38(2011), pp. 41-49.

[7]. Beenish Mehboob and Rashid Aziz Faruqui, 2008. "A Stegnography Implementation", Department of Computer Science and Engineering, Bahria University, Karachi, Pakistan, 1-4244-2427-6/08/$20.00 ©2008 IEEE.

[8]. Jassim Mohmmed Ahmed and Zulkarnain Md Ali, 2011. "Information Hiding using LSB technique", IJCSNS International 18 Journal of Computer Science and Network Security, Vol.11, No.4.

[9]. A.E.Mustafa, A.M.F.ElGamal, M.E.ElAlmi and Ahmed.BD, 2011. "A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit", Research Journal Specific Education Faculty of Specific Education, Mansoura University, Issue No. 21.

[10]. Vijay Kumar Sharma and Vishal Shrivastava, 2012. "A Steganography Algorithm for hiding image in image by improved LSB substitution by minimize detection", Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645, Vol. 36, No.1.

[11]. Amanpreet Kaur, Renu Dhir, and Geeta Sikka, 2009. "A New Image Steganography Based On First Component Alteration Technique", International Journal of Computer Science and Information Security (IJCSIS), Vol.6, No.3.