Block Wise Data Hiding with Auxilliary Matrix

Jyoti Bharti
Deptt. of Computer Science & Engg.
MANIT
Bhopal, India

R.K. Pateriya
Deptt. of Computer Science & Engg.
MANIT
Bhopal, India

Sanyam Shukla
Deptt. of Computer Science & Engg.
MANIT
Bhopal, India

***Abstract*—This paper introduces a novel method based on auxiliary matrix to hide a text data in an RGB plane. To hide the data in RGB planes of image via scanning, encryption and decryption. To enhance the security, the scanning technique combines two different traversals – spiral and snake traversal. The encryption algorithm involves auxiliary matrix as a payload and consider the least significant bits of three planes. To embed the text message would in the form of ASCII values which are similar to the red plane values and least significant value of pixels in blue plane marks the position of pixels. The least significant bit of boundary values of green-plane signifies the message. These three planes are recombined to form the stego-image, to decrypt the message with the help of scanning in the red-plane and blue plane and green plane simultaneously. Performance evaluation is done using PSNR, MSE and entropy calculation and generated results are compared with some earlier proposed work to present its efficiency with respect to others.**

Keywords—Steganography; RGB planes; Scanning; Stego-image; ASCII value

I. INTRODUCTION

Steganography is the process to conceal a message or data in an image which is not detectable by human visual system. Message would be in the form of text, image, audio etc. Unlike cryptography transform the message into another form and hide in an image and then passed over the attack prone network to the receiver; it is more secure, as the existence of the message embedded in the image is concealed [1]. In this paper, a new technique is proposed to hide text message in planes of RGB image, so as to enhance the security of the information being hidden in the image. The accuracy has been evaluated on comparison of MSE and PSNR values. Some of the most popular techniques that have already been discussed in this field in the past years are adaptive data hiding in edge areas of images with spatial lsb domain systems [2], reversible data hiding using integer wavelet transform and companding technique[3], robust image-adaptive data hiding using erasure and error correction [4], reverse data hiding [5] and many more. Steganography is very useful and commercially important application in the digital world for example digital watermarking. In this application, to ensure the integrity or authenticity of intellectual property or product, owner can embed the message hidden in the file. This kind of mechanism is used by intelligence agencies for secret works [6].

II. PROPOSED WORK

In this paper the proposed methodology consists of three Steps- Scanning, Encryption and Decryption.

A. Scanning

Scanning means, In a two dimension array, the way or pattern in which each element or pixel is accessed. As a purpose of security, a hybrid scanning techniques has been used which is based on spiral and snake traversal. The carrier image is divided into smaller size of blocks. Each block contain 50 x 50 pixels. The blocks are accessed in a snake pattern as shown in Fig. 1(a).

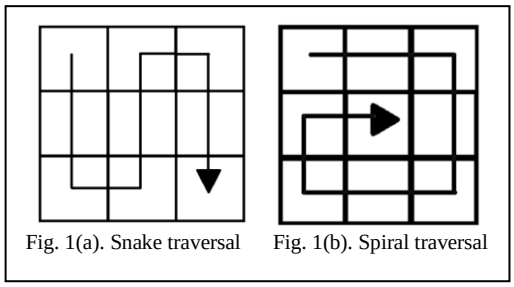

Fig. 1(a). Snake traversal Fig. 1(b). Spiral traversal

Fig. 1. Scanning Traversal

In the snake pattern, starting from the first block, blocks are accessed vertically downwards then accessing the adjacent block then moving vertically upwards. This pattern continues until all the blocks are traversed. Then within each block, pixels are accessed using the spiral technique as shown in Fig. 1(b). In the spiral technique, pixels are accessed starting from the first pixel, moving along the boundary towards the center. Once all the pixels within a block are accessed the technique again initializes the accessing pointer to the first pixel of next block to be accessed in the snake pattern which is shown in Fig. 2

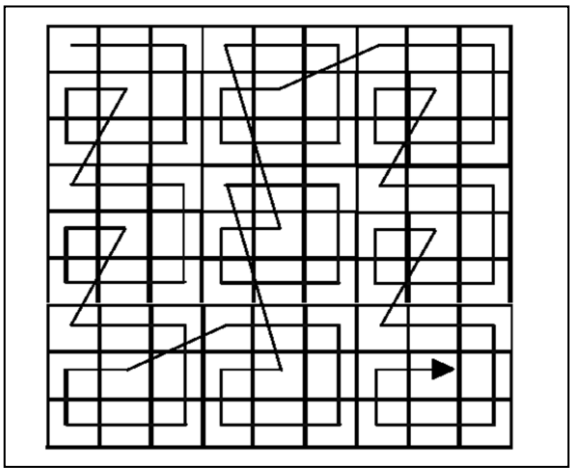

Fig. 2. Block wise path traversal of pixels in an image

B. Encryption

Encryption is the technique of hiding the text message in the carrier image. For this method RGB image is taken as the carrier image. The text message can be in any language. Here, English language is taken for the text message. The ASCII values can be mapped with the pixel intensities of RGB plane as ASCII values of English alphabets i.e. 0-127 lie within the range of pixel intensities i.e. 0-255. RGB image consists of three planes – red plane, green plane and blue plane, each playing a specific role in the proposed method that is described later in the paper. Pixels in the plane comprises of 8 bits which shows the intensity values within the range of 0 to 255.

In this methodology, RGB image is divided into three planes, namely: Red plane, Blue plane and Green plane. The LSB planes of blue and green plane are extracted using bit plane slicing. Along with this, an auxiliary matrix with size equal to the size of the image is maintained with all values set to 0. Auxiliary matrix stores the positions/ indices of the letters in the message. For example if the message is "HELP" then index of H is 1, E is 2, L is 3 and P is 4. To hide the message in RGB plane, it requires four steps.

1) Convert each letter of the message into its ASCII values as shown in Fig 3.

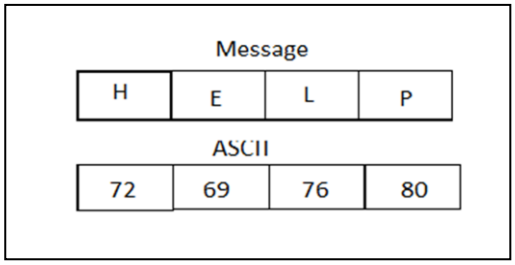

Fig. 3. Payload: The message to hide

2) The red plane is scanned using the proposed scanning technique (Originally the image size will be large enough to implement the proposed scanning technique, but for demonstration, here an image of size 5X5 pixel is taken, which smaller than 50X50, then spiral technique is applied. In the red plane, ASCII value of each letter in the message is compared with the pixel intensities of the red plane. If any pixel intensity in red plane is matched with ASCII value, then, its position is marked in LSB of blue plane using the method in step 3. If no such pixel intensity is found then, closest pixel intensity to the ASCII value is searched in the red plane and it is replaced with the ASCII value of the letter being searched. The position of this modified pixel is also marked in blue plane using the method in step 3.

3) Least significant bits of the blue plane act as an indicator plane and that signifies that the red plane contains the message. LSB of blue plane is set to 0 indicating no modification in pixel intensity or pixel intensity is not equal to ASCII value of message. After scanning the red plane, if the pixel intensity matches the ASCII value of the letters in the message or any closest pixel intensity is replaced by the ASCII value of the letter then the corresponding pixel in blue-plane is marked by setting the LSB of that pixel, i.e. LSB 0 is turned to 1.

Step 2 and 3 are repeated for each letter in the text message. Hence, all the ASCII values of the letters in the message will be available in the red plane. It is shown in Fig 4.

Red plane of carrier image

71	68	50	69	52
59	61	63	89	42
72	41	73	88	59
41	102	116	99	80
77	76	84	58	79

LSB of Blue Plane after Scanning

0	0	0	1	0
0	0	0	0	0
1	0	0	0	0
0	0	0	0	1
0	1	0	0	0

Fig. 4. ASCII value Comparison in red plane and converting the corresponding LSB of blue plane as 1

Auxiliary matrix is traversed simultaneously with red plane. When the ASCII value is found or nearest ASCII value is found then the index of that letter is set in auxiliary matrix (in the same position as in the LSB of blue plane). So auxiliary matrix holds the indices of the letters in the message in the exact position where the LSB of blue plane is set to 1, this is shown in the Fig. 5.

The auxiliary matrix is traversed with the scanning technique proposed earlier so as to get a jagged sequence of indices. These indices are converted into their binary forms as shown in Fig. 6.

Auxillary array showing indices

0	0	0	2	0
0	0	0	0	0
1	0	0	0	0
0	0	0	0	4
0	3	0	0	0

Fig. 5. Auxiliary matrix to hide the indices of payload

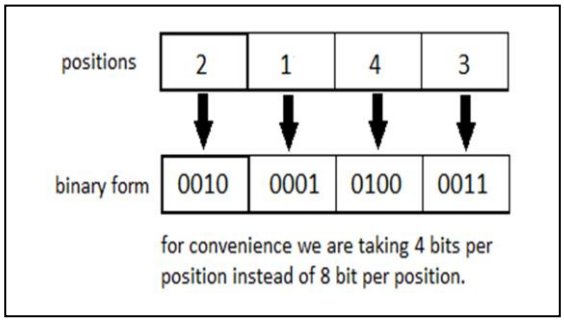

Fig. 6. Positions of indices of payload retrieved after scanning the auxiliary matrix and convert it into an 4 bit binary number

4) The LSB of green plane is used to hide the indices of letters in the message in their binary forms. The indices obtained after scanning the auxiliary matrix, are converted into their 8 bit binary format as shown in Fig 8 and substituted in the LSB of green plane at its boundary as shown in Fig 7. The whole LSB substitution is only done on the boundary values of the plane ensuring least modification in the LSB of green plane. These indices are hidden contiguously in the boundary of green plane at LSB positions.

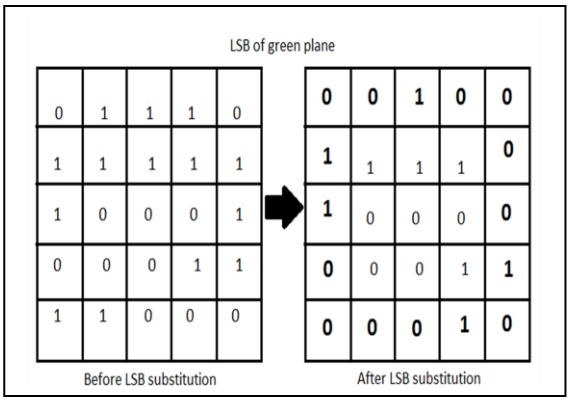

Fig. 7. LSB Substitution in Green plane

LSB of blue plane and LSB of green plane are merged with the higher bit blue plane and green plane respectively. To produce the Stego-image all the three planes are merged together. At the receiver end, the message retrieved from Stego-image using the Decryption technique.

C. Decryption

Decryption is a technique to decipher the information hidden in the Stego- image. Since the message is confidential, it is assumed that, the technique is known to the concerned sender and receiver only. In order to retrieve the message, the Stego-image is again divided into three planes-red plane, green plane and blue plane. The LSB of blue plane and green plane is extracted to retrieve the ASCII values of the letters in the message using red plane and to extract indices of those ASCII values respectively. Using the scanning technique proposed above, the red plane and the LSB of the blue plane is searched simultaneously, for the hidden letters. In case, a pixel intensity is found in the red plane such that its corresponding LSB of the blue plane is 1, then that intensity value (belonging to red plane) is stored in an array. Similarly the whole red plane and LSB of blue plane is searched and such values are extracted. These values are the ASCII values of letters in the message. These values are stored in an array in the same order as extracted from red plane. Hence the array contains a random sequence of ASCII values. To retrieve the message from Stego-image, these values are arranged in the same order as they were present in the original message. For this, the indices of the letters, which are hidden in green plane are extracted. The LSB of boundary pixels in green plane are processed, eight pixels at a time and an 8 bit binary number is formed. These binary numbers are converted into their decimal forms. These decimal numbers are the indices of the random ASCII values retrieved from the red plane earlier. These are stored sequentially into another array. Following the same procedure, indices for all the intensity values are extracted. After this, the intensity values are rearranged according to their indices. These intensity values are converted into their corresponding ASCII characters. The decrypted string of characters forms the original message hidden in the Stego-image.

III. ALGORITHM

A. Encryption technique

- Load an RGB Image.
- Extract red, green and blue plane. Store it in matrix red, matrix blue, matrix green.
- Extract LSB of green and blue planes and store it in matrix green1, matrix blue1 respectively.
- Extract size of image in variables rows, cols.
- Convert LSB of blue plane to zeros so that values in matrix blue1 are 0.
- Create an auxiliary matrix aux with all values 0.
- Input message from console and store in message array.
- Traverse the message from beginning to end one letter at a time
- Store letter in variable k;
- Flag stores the search result after scanning. Flag is set to 1 if ASCII value is found else set to 0.
- Call function of Scanning_technique and pass variables:- flag, pos_x and pos_y.
- pos_x and pos_y stores position where ASCII values are found or intensity values are the closest.
- If ASCII value matches pixel intensity value of red plane then set the corresponding position of the blue1 plane to 1.
- Store the position of the character in the auxiliary matrix.
- If the ASCII value does not match pixel intensity value then find the pixel intensity value closest to the ASCII value.

- Replace pixel intensity value with the new intensity value and set the corresponding location in the blue1 plane to 1 and then store the position of the character in the auxiliary matrix.
- Create an array- bit_arr.
- Scan auxiliary matrix using the proposed scanning technique.
- If a non-zero element is found then store the element in array in binary form.
- Store the bit array in the boundary values of green1 plane.
- Merge green1 and green plane.
- Merge blue1 and blue plane.
- Merge red, blue and green to get the StegoImage.

B. Scanning technique

- Divide the image into 50 X 50 blocks.
- Snake technique: In the snake technique, the image matrix is traversed block wise. From the first block, move vertically downwards until all the blocks are traversed in a column and then the adjacent block are traversed and move vertically upwards.
- Spiral technique: In the spiral technique, a 50 X 50 block is traversed starting from the first pixel and moving towards the boundary and moving inside towards the center pixel.

C. Decryption technique

- Load Stego-Image
- Extract red, green and blue plane.
- Extract size of the image.
- Initialize message array, position array and bit_arr array to store the ASCII value of the message, position in decimal and position in binary respectively.
- Call Scanning technique for red and blue planes.
- Consider the LSB of green plane and traverse the boundary values and 8 pixels at a time.
- Store 8 LSB values in bit_arr array.
- Convert bit_arr array into decimal and store into position array.
- Arrange message array according to the position array.
- Message array is our original message.

IV. Result And Analysis

The security analysis compares the Original image with the Stego-image based on the histogram of the images. If the change in histogram is minimal, then the encryption algorithm is considered secure. Fig.8(a)& (b) shows the size of original image size 200 x 450 pixels and Stego-image created after embedding the message using the above proposed technique.

The modified image (Stego-image) after applying the proposed algorithm does not release any identifiable visual difference. The histograms of the original and stego images are shown in Fig.9. Both the histograms show no such significant changes.

The experimental results obtained are subjected to various statistical techniques, to evaluate the performance parameters of the steganographic images viz., (i) PSNR values of the Stego-image (ii) Mean Square Error (iii) Entropy.

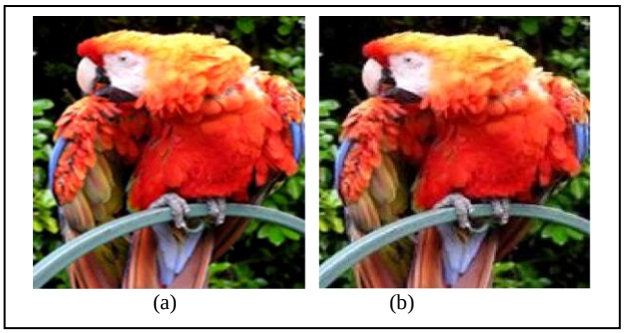

Fig. 8. (a). Original Image (b). Stego-image

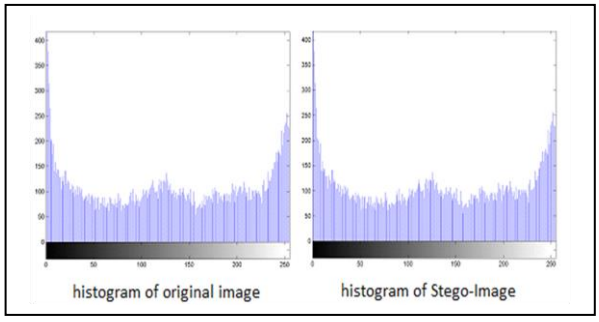

Fig. 9. Histogram original and stego-image

PSNR as a metric computes the peak signal-to-noise ratio, in decibels, between two images [7]. The higher the PSNRvalue, the better degraded image has been reconstructed. To match the original image and the stego-image calculate the PSNR value using (1) [8].

$$\text{PSNR} = 10 \times \log_{10}\left(\frac{R^2}{MSE}\right) \quad (1)$$

Where, R is the maximum pixel intensity value for an image.

The MSE represents the average of the squares of the "errors" between our actual image and our noisy image. The error is the amount by which the values of the original image differ from the degraded image [8] . It is given in (2) [9].

$$MSE = \left(\frac{1}{(m \times n)}\right) \times \sum_i \left(\sum_j (f - g)^2\right) \quad (2)$$

where, f: matrix data of our original image. g: matrix data of our degraded image. m: number of rows of pixels of the images . i: index of that row. n: number of columns of pixels of the image. j: represents the index of that column.

The more data hidden in a file, the higher that file's entropy. That is, if bits are too disorderly and data are too random, steganography may be suspected [10]. Entropy is defined as:

$$E = -\sum P \times \log(P) \quad (3)$$

For the above case of parrot image PSNR value comes out to be 52.65, MSE comes out to be 0.35 and entropy value comes out to be 0.19. The simulation done with other images viz. Lena, Baboon, Pepper and Butterfly. The results of the simulation for these images, the histogram analysis and the results based on the quality metrics (i.e. values of the PSNR, MSE and Entropy) are tabulated in table-I and shown in the following Fig.10-13.

TABLE I. PSNR, MSE AND ENTROPY OF IMAGES OF THE PROPOSED ALGORITHM.

Figure no. and name	PSNR	MSE	Entropy
Lena	52.19	0.39	0.00
Baboon	52.44	0.37	0.00
Pepper	53.50	0.29	0.11
Butterfly	52.99	0.33	0.66

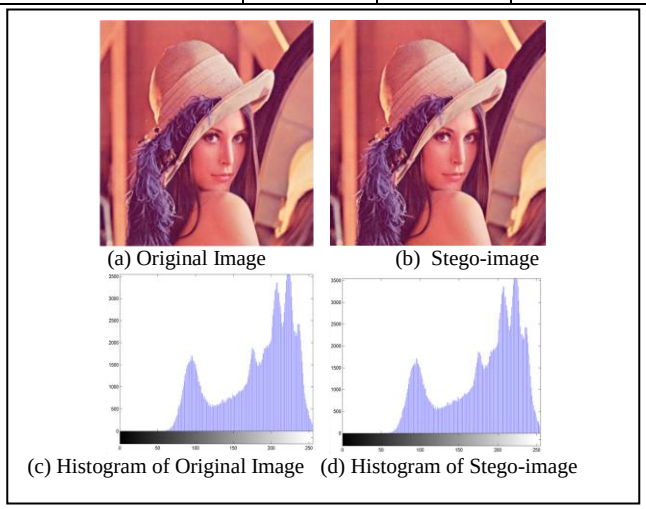
(a) Original Image (b) Stego-image
(c) Histogram of Original Image (d) Histogram of Stego-image

Fig. 10. Result for Lena

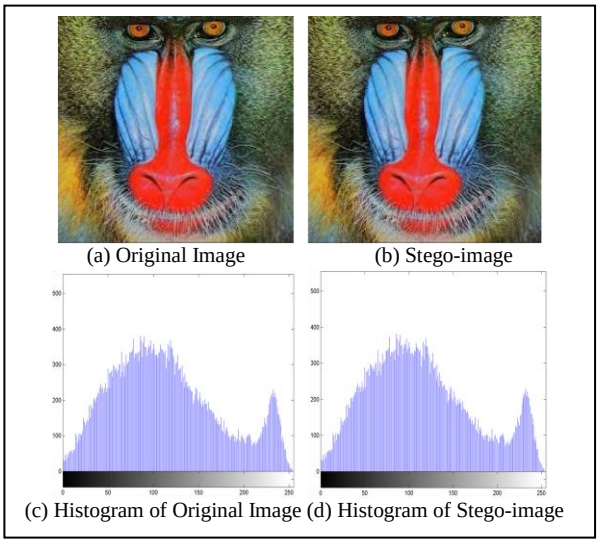
(a) Original Image (b) Stego-image
(c) Histogram of Original Image (d) Histogram of Stego-image

Fig. 11. Results for Baboon

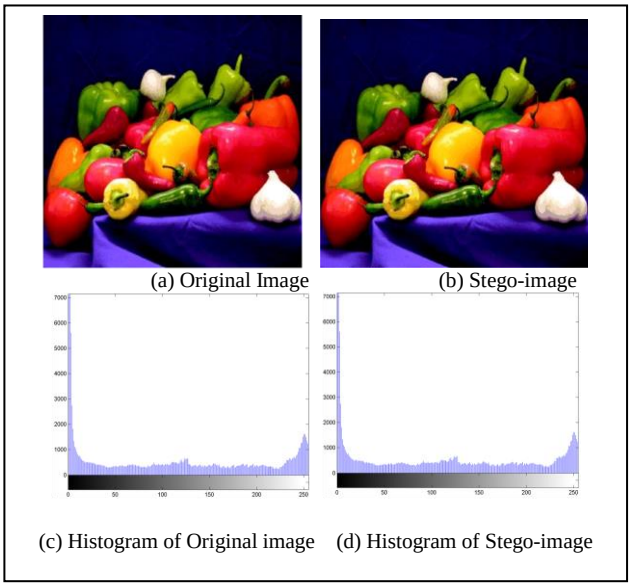
(a) Original Image (b) Stego-image
(c) Histogram of Original image (d) Histogram of Stego-image

Fig. 12. Result for Pepper

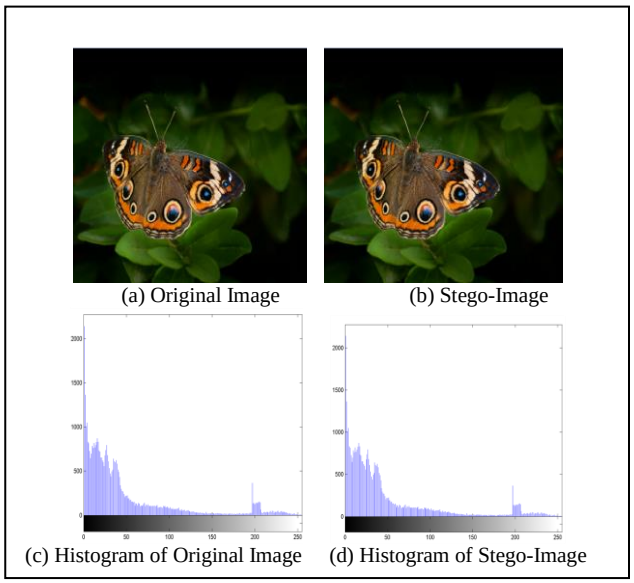

Fig. 13. Result for Butterfly

A. *Effect of message length*

Increase in the length of the message causes, manipulation of more number of pixel intensities. This results in decrease in PSNR values with increase in message length. The probability of error within a region increases with more number of modifications in pixel intensities, hence the value of MSE with increase of message length increases. The messages are embed in to a parrot image The change in PSNR and MSE values are shown in fig. 14 & 15.

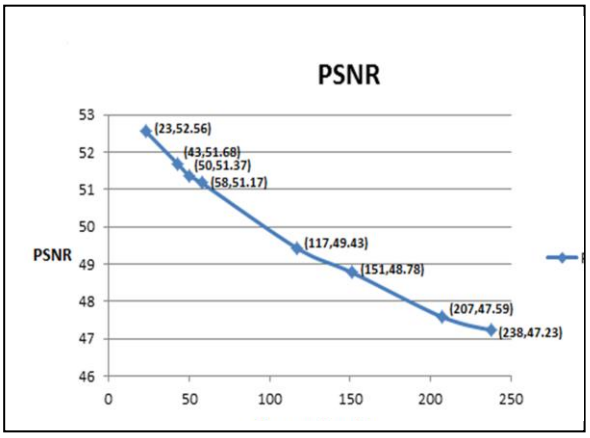

Fig. 14. Change in PSNR values with increase in message length for image 'Parrot'

Fig.14 shows the PSNR values for image Parrot. PSNR values lie on the Y-axis and message length on X-axis. For message length ranging from 25 to 250, PSNR values for the proposed method, lie within 47 to 53. The PSNR value decreases on enhancing size of the message lenght.

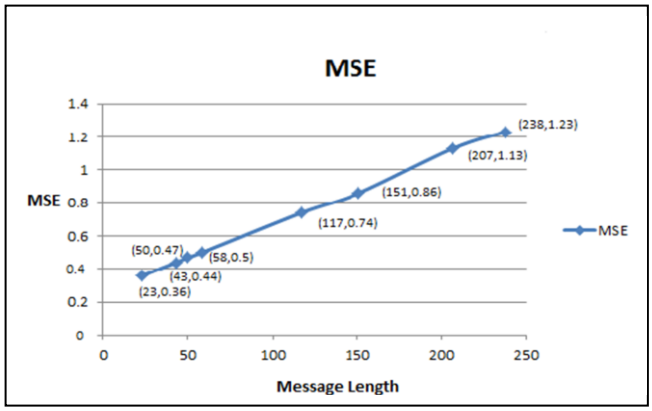

Fig. 15. Graph of change in MSE values with increase in message length for image 'parrot'

Fig. 15 MSE values lie on the Y-axis and message length on X-axis. For message length ranging from 25 to 250, PSNR values for the proposed method, lie within 0.2 to 1.3 for the image "parrot".

B. *Comparitive Study*

Results obtained for the proposed method are compared with the results of some Steganographic techniques proposed earlier in well-known research papers and journals, on the basis of quality metrics MSE and PSNR values for different images (based on the availability of the results). It is observed, the proposed algorithm provides better results than all the previous schemes. The results of comparison for the MSE and PSNR values of images- "Lena" and "Baboon" are shown in Table II-IV.

TABLE II. COMPARISON OF MSE VALUES FOR LENA

S.No	Steganography Technique	MSE
1.	Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems [2]	7.337
2.	OLS Technique [10]	2.34
3.	OLSGA Technique [10]	2.34
4.	Proposed method	0.39

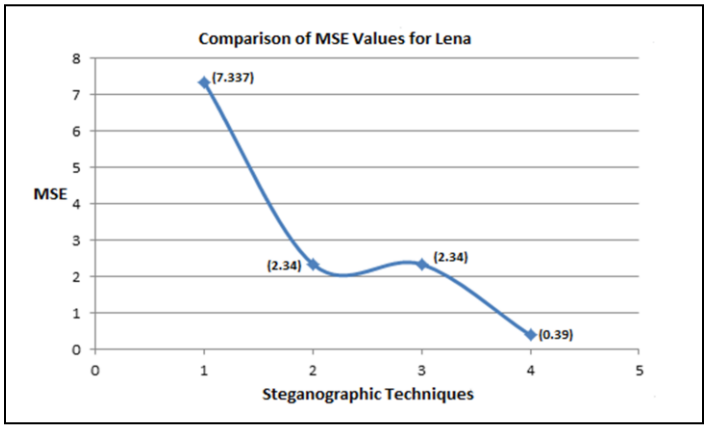

Fig. 16. Graph for MSE values for Lena

TABLE III. COMPARISON OF PSNR VALUES FOR LENA

S.No	Steganography Technique	PSNR
1	Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems [2]	37.61
2	Robust Image-Adaptive Data Hiding Using Erasure and Error Correction [4]	41.43
3	Reversible Data Hiding using integer wavelet transform and campanding technique. [3]	46.23
4	A Variable Depth LSB Data Hiding Technique (3k message length) [11]	46.35
5	Reversible data hiding [5]	48.20
6	A DWT based approach for image steganography[12]	50.8021
7	Proposed method	52.19

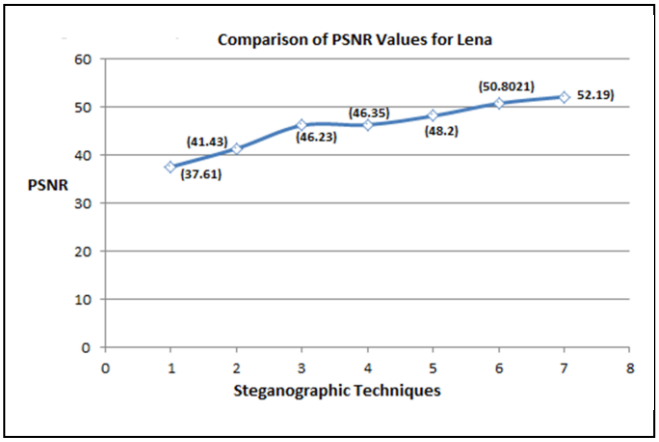

Fig. 17. Graph for PSNR values for Lena

The Fig.16 is a graphical representation of the Table.II. which presents comparative study between different Steganography techniques proposed earlier and the proposed method here, on the basis of MSE generated on the image "Lena". For the graph X- axis represents serial numbers of methods mentioned in Table.II and Y- axis represents their corresponding MSE values. It can be observed, the proposed method produces the least MSE value for "Lena" compared to rest.

The Fig.17 is the graphical representation of the Table III, on the basis of PSNR generated on the image "Lena". For the graph X- axis represents serial numbers of methods mentioned in Table III and Y- axis represents their corresponding PSNR values. It can be observed, the proposed method produces the comparatively higher PSNR value i.e 52.19 for "Lena

TABLE IV. COMPARISON OF PSNR VALUES FOR BABOON

Steganography Technique	PSNR
1. Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems [2]	34.26
2. Robust Image-Adaptive Data Hiding Using Erasure and Error Correction [4]	35.98
3. Reversible Data Hiding using integer wavelet transform and campanding technique. [3]	39.66
4. Reverse data hiding [5]	48.2
5. Proposed method	**52.44**

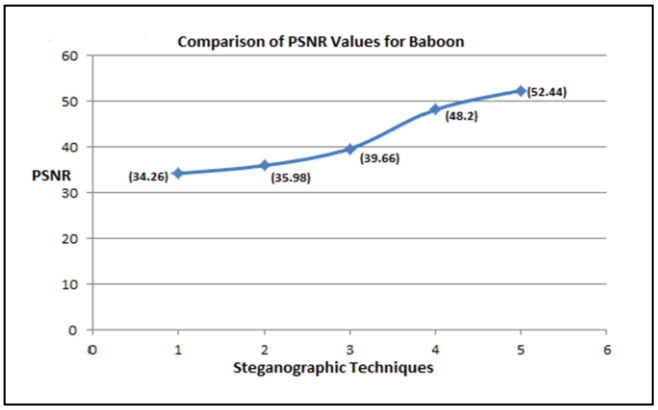

Fig. 18. Graph for PSNR values for Baboon

The Fig.18 is the graphical representation of comparison PSNR with other. For the graph X- axis represents serial numbers of methods mentioned in Table IV and Y- axis represents their corresponding PSNR values. It can be observed, the proposed method produces the comparatively higher PSNR value i.e 52.44 for "Baboon".

V. CONCLUSION

In this paper, the proposed is a new steganography technique to hide a text message in an RGB image with minimum manipulation with the intensity values and LSB of the pixel. Instead of hiding the ASCII value of the letter, which would have taken 8 bits, it tries to search the pixel in the red plane whose intensity value matches the ASCII value of each letter of the message and changes the LSB value of the corresponding pixel in the blue plane resulting in a change of only one bit of the pixel. This results in less modification of bits resulting in less randomness in the image. As per the experimental results shown on different images, it is found that the PSNR value ranges between 50 and 55 which is near to ideal, the entropy values are closer to 0.0 and the MSE values are less. These experimental analysis shows that after embedding the data, less distortion in the stego image is not noticeable as the histogram of the cover image and stego image are very similar which accounts for better stego image quality. Comparing with other techniques as well, it is found that this proposed technique gives better results for PSNR and MSE values.

REFERENCES

[1] S.Ashwin, S.Aravind Kumar, J.Ramesh, K.Gunavathi, "Novel and secure encoding hiding techniques using image steganography : A survey", IEEE International Conference on Emerging Trends in Electrical Engineering and Energy Management (ICETEEEM-2012), pp. 171-177, December 2012.

[2] [Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, "Adaptive data hiding in edge areas of images with spatial lsb domain systems", IEEE Transactions On Information forensics And Security, vol. 3, pp. 488-497, September 2008.

[3] GuorongXuan, Chengyun Yang, Yizhan Zhen,Yun Q. Shi, and Zhicheng Ni, "Reversible data hiding using integer wavelet transform andcampanding technique", Third International Workshop(IWDW-2004), Springer Verlag Berlin Heidelberg, pp. 115 – 124, 2005.

[4] Kaushal Solanki, Noah Jacobse,Upamanyu Madhow, Shivkumar Chandrasekaran,"Robust image-adaptive data hiding using erasure and error correction", IEEE Transactions On Image Processing, vol. 13, pp. 1627-1639, December 2004.

[5] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari,and Wei Su, "Reversible data hiding", IEEE transactions on circuits and systems for video technology, vol. 16, No. 3, March 2006.

[6] [6]. Gary C. Kessler, "An overview of steganography for the computer forensics examiner", Issue of Forensic Science and Communication, Vol 6 - Number 3, February 2004 [updated February 2015]

[7] Gabriel Macharia Kamua, Stephen Kimani,Waweru Mwangi, "An enhanced least significant bit steganographic method for information hiding", Journal of Information Engineering and Applications, ISSN 2224-5782 (print) ISSN 2225-0506 (online), vol 2, No.9, 2012.

[8] Z.Wai, S. Than, "Data hiding techniques depended on pseudorandom sequences",International Journal of Scientific Engineering and Research, vol. 1, Issue 2, October 2013.

[9] Sudipta Kr Ghosal, "A new pair wise bit based data hiding approach on 24 bit color image using steganographic technique", Proceedings of IEMCON-2011,, Kolkata, West Bengal, India, pp.123–129, January 2011

[10] Xiaoyan Qiao, "A new method of steganalysis based on image entropy", Springer Verlag Berlin Heidelberg, CCIS 2, pp. 810-815, 2007.

[11] Smo-hui liv, Tun-hang chen, Hongxunyao, Wen gao, "A variable depthlsb data hiding technique in images", Proceedings of the third Intemational conference on Machine Learning and Cybernetics, Shanghai, pp. 26-29, August 2004.

[12] Po-Yueh Chen and Hung-Ju Lin, "ADW based approach for image steganography", International Journal of Applied Science and Engineering, vol. 4, pp. 275-290, 2006.