A Novel Approach for Data Hiding Technique Using Interpolation And Braille Method

Kirti Sharma[1], Kamaldeep Joshi[2]
[1]M.Tech. Student, Department of Computer Science and Engineering,
University Institute of Engineering and Technology, M.D. University, Rohtak, Haryana, India
Email- krtbhardwaj1@gmail.com
[2]Assistant Professor, Department of Computer Science and Engineering,
University Institute of Engineering and Technology, M.D. University, Rohtak, Haryana, India
Email- kamalmintwal@gmail.com

***Abstract*— Steganography means concealed writing of secrete information within any cover media. In image Steganography for the purpose of privacy of secrete message, it is embedded within an innocuous image without knowing the existence of information to the intruders. To maintain the privacy and in direction to maximize it, this proposed technique used the Braille method. Braille method is the interpreting technique to scan the words for the blind peoples. So, with regard to make the secrete information invisible to the intruder Braille method helps a lot. In the proposed technique message characters are converted into 6 bits Braille's binary representation and then embed the message bits within the interpolated pixels of cover image. Interpolated cover image is hatched through the actual image by using interpolation method and all message bits are inserted within the interpolated pixels from left to right using the even odd pixel value approach with parity checker. The proposed technique maximizes the message hiding capacity and also improves the PSNR and MSE value as compared to existing techniques.**

Keywords: Image Steganography, Interpolation, PSNR, MSE, Braille method.

I. INTRODUCTION

Information Technology plays a vital role in present era of advancement in technology. Due to rapid advancement in technology, need of secure data transmission (data security) provides great challenges to researchers and also encourages researchers to promote higher level security techniques. These security techniques protect the susceptible data transmission between sender and receiver from intruders to interrupt over network. In this regards, information hiding system provides different techniques to establish secure communication. [1]

Information hiding system approaches two well known techniques named as Cryptography and Steganography. Cryptography technique only concentrates on data hiding by encrypting the confidential message from original to another form but do not able to obscure the existence of the confidential message during communication. But Steganography is an art that aims to intact the private communication by conceal the information in a well suited multimedia cover and reduces the chances of attack via intruders over network compared to cryptography technique. In information hiding system, image Steganography is well-known idea to hide the confidential information via cover image [2][3]. Two common types of Image Steganography are Spatial Domain and Transform Domain. In spatial domain message bits are directly embedded in cover image pixels for example LSB Technique. In transform domain firstly cover image pixels transformed after that message embedded within transformed pixels of image for example DCT, DWT etc [4].

II. LITERATURE REVIEW

N.F. Jonson et al., introduced LSB insertion method. It is much easier approach for insertion of message within cover image to hide the confidential information. In this method, LSB of each pixel flipped with the each message bits in sequence and after the insertion LSB of each pixel reflects the message bit that should have to be hidden [5].

K. Joshi et al., introduced an investigation about PSNR and MSE based upon LSB insertion technique by using distinct message sizes in different gray scale images in spatial domain. This technique provided a basic study about PSNR and MSE evaluation. PSNR is more for small message length and vice-versa. MSE is less for small message length and vice-versa [6].

T. Bedwal and M. Kumar proposed more secured image Steganographic technique using RGB-box mapping that improves previous LSB method. In this technique, a RGB image has to be hidden within another RGB image based upon LSB insertion method. Mapping was applied on RGB image that provides more security to secrete data and also no need of knowledge of mapping techniques [7].

Rajkumar, Rahul Rishi and Sudhir Batra proposed a technique for gray level images in which Parity Checker used for insertion of message bits at LSB bits of pixels. In this technique, pseudo-random generator was used for insertion. To insert ‘0’ as message bit, pixel bits must have odd Parity and to insert ‘1’ as message bit, pixel bits must have even Parity. This method provided better results for message insertion in 1st chances are 98.82% with very less changes in original image [8].

Ki-Hyun et al., proposed semi-reversible Steganographic approach which was based upon interpolation and LSB insertion technique. Interpolation technique used to scale up original image and LSB technique used for insertion of secrete data that provided better results with larger capacity to hide and higher quality of image [9]. This method provides higher insertion capacity and invisible distortion in image.

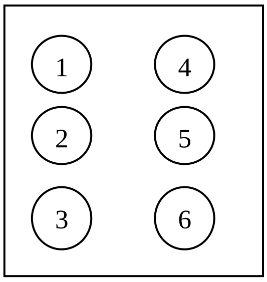
K. Joshi and Rajkumar introduced an approach for hiding the data using XOR for image Steganography by using last three bits of pixels. Here XOR operation is performed on message bits and original image [10]. This method provides higher security to the data from intruders to detect.

Al-Hussien Seddik Saad et al., proposed a method using Zero- Order- Holding Method (ZOH) which resulted as higher PSNR value rather than other LSB methods. In this method, cover image resulted as zoomed out image using ZOH method and using LSB substitution, message is inserted. This technique provided a higher security as well as also maximizes message holding capacity (MHC) comparatively [12].

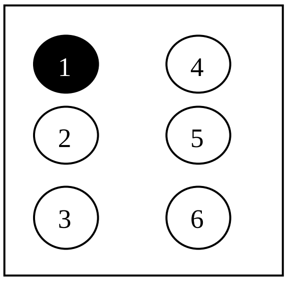
Al-Hussien Seddik Saad et al., proposed an improved technique for previous method as Zero order Holding, by combining LSBraille image Steganographic technique. In this method, firstly secrete message is converted in 6 bits binary representation using Braille method and then used LSB substitution and ZOH method to insert the message. ZOH Braille technique provided much higher PSNR values and increased MHC compared to the previous technique [13].

III. PROPOSED WORK

In the proposed method, firstly modification is done in the confidential message by using Braille method which increase maximum hiding capacity rate. In the Braille (blind people language) method characters representation, each character is represented by 6 dots matrix known as Braille cells. Binary representation of these characters includes only 6 bits rather than 8 bits in ASCII binary representation which directly saves 2 pixels from every byte insertion procedure [15]. Braille Cell represents the characters for example character ‘a’ has dot 1 as dark only.



Braille Cell



Braille representation Of character ‘a’

These six dots consist of total 64 possible combinations. 6 bits representation of characters using Braille method is shown in table below where black dots are represented by 1 and empty dots are used by 0.

TABLE1: Braille's Characters 6 bits representation [11]

Characters	Black dots indexes	6 bits binary digits	Characters	Black dots indexes	6 bits binary digits	Characters	Black dots indexes	6 bits binary digits
A	1	100000	V	1,2,3,6	111001	!	3,4,5,6	001111
B	1,2	110000	W	2,4,5,6	010111	‘	3	001000
C	1,4	100100	X	1,3,4,6	101101	-	3,6	001001
D	1,4,5	100110	Y	1,3,4,5,6	101111	“	4	000100
E	1,5	100010	Z	1,3,5,6	101011	&	1,2,3,4,6	111101
F	1,2,4	110100	0	1,2,3,4,5,6	111111	[	1,2,3,5,6	111011
G	1,2,4,5	110110	1	1,6	100001	@	2,3,4,6	011101
H	1,2,5	110010	2	1,2,6	110001	]	2,3,4,5,6	011111
I	2,4	010100	3	1,4,6	100101	+	2,3,5	011010
J	2,4,5	010110	4	1,4,5,6	100111	=	2,3,5,6	011011
K	1,3	101000	5	1,5,6	100011	<	2,3,6	011001
L	1,2,3	111000	6	1,2,4,6	110101	*	3,5	001010
M	1,3,4	101100	7	1,2,4,5,6	110111	>	3,5,6	001011
N	1,3,4,5	101110	8	1,2,5,6	110011	/	3,4	001100
O	1,3,5	101010	9	2,4,6	010101	)	3,4,5	001110
P	1,2,3,4	111100	,	2	010000	-	3,4,6	001101
Q	1,2,3,4,5	111110	;	2,3	011000	(	4,5	000110
R	1,2,3,5	111010	:	2,5	010010	$	4,5,6	000111
S	2,3,4	011100	.	2,5,6	010011	%	4,6	000101
T	2,3,4,5	011110	?	2,6	010001	Space	Empty	000000
U	1,3,6	101001						

A confidential message M is inserted within a cover image (CI). Cover image is generated from the original image using interpolation method which is discussed below.

- Take two adjacent pixels from original image (I), subtract minimum pixel value from maximum pixel value among both. P= MAX-MIN.
- Divide P by 2 and take floor value (P=P/2).
- Add this value to the min pixel value. P=MIN+P.
- Then interpolated value is generated. If this procedure continues firstly row wise in matrix among each adjacent pixel then follow it column wise.
- Now, resulted pixel matrix as the cover image (CI).
- Let M*N Pixels is the size of the cover image and after the interpolation cover image size becomes (2M-1)*(2N-1) Pixels. These interpolated pixels in cover image are used to hide the secrete message. Insertion and Extraction algorithms are further discussed here as below.

A. *Insertion Algorithm*

Step 1. Initialize original input image (I) of M*N Pixels. Generate cover image (CI) using above method and M is the confidential message which is in converted form of 6 bits by using Braille representation (m_1, m_2….. m_n).

Step 2. Message bits are inserted in cover image interpolated pixels firstly row wise then column wise. For insertion of message take each two adjacent pixels from LSB of message M.

Step 3. If insertion message bits are ‘00’. Then check Pixel (P) value and its parity. If pixel value is even number with odd parity then no any change required in pixel and insert the message bit ‘00’. Else go to Step 7 and insert the message bits ‘00’.

Step 4. If insertion message bits are ‘10’. Then check Pixel (P) value and its parity. If pixel value is even number with even parity then no any change required in pixel and insert the message bit ‘10’. Else go to Step 7 and insert the message bits ‘10’.

Step 5. If insertion message bits are ‘11’. Then check Pixel (P) value and its parity. If pixel value is odd number with odd parity then no any change required in pixel and insert the message bit ‘11’. Else go to Step 7 and insert the message bits ‘11’.

Step 6. If insertion message bits are ‘01’. Then check Pixel (P) value and its parity. If pixel value is odd number with even parity then no any change required in pixel and insert the message bit ‘01’. Else go to Step 7 and insert the message bits ‘01’.

Step 7. Do +1,-1 or +2,-2 to satisfy the pixel value according to given condition.

Step 8. Choose one from step 3 to step 6. Do these steps repeatedly until the length of message is covered or inserted in interpolated pixels.

B. Extraction algorithm

Step 1. Take the stego image S with (2M-1)*(2N-1) Pixels.

Step 2. Extract the interpolated pixels.

Step 3. If Pixel value (P) is even number with odd parity bits then message bits are ‘00’.

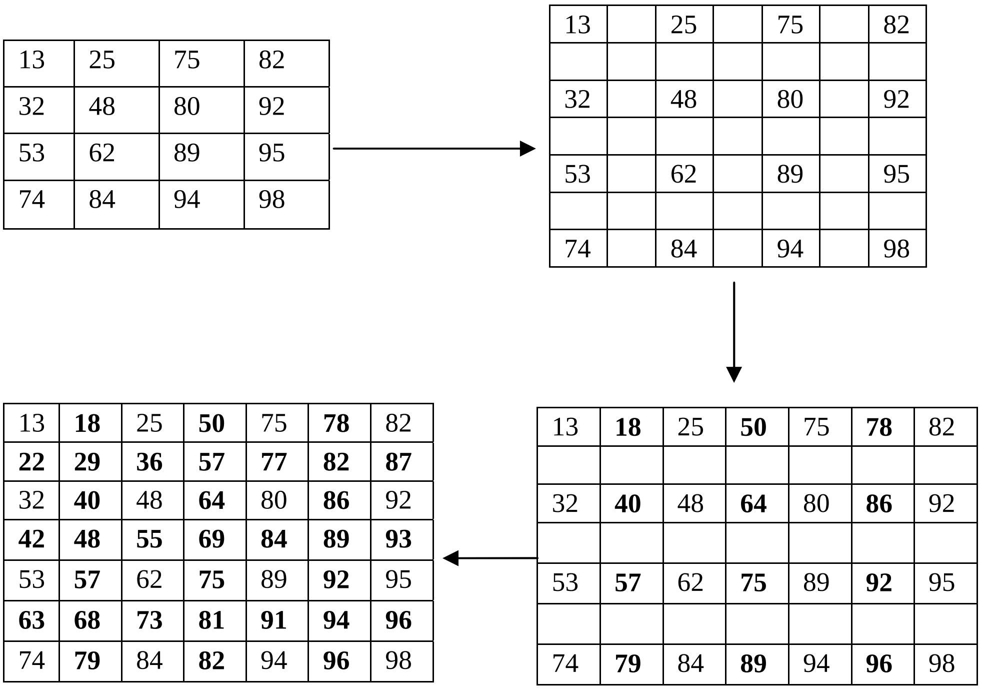
Step 4. If Pixel value (P) is even number with even parity bits then message bits are ‘10’.

Step 5. If Pixel value (P) is odd number with odd parity bits then message bits are ‘11’.

Step 6. If Pixel value (P) is odd number with even parity bits then message bits are ‘01’.

Step 7. Choose from step 3 to step 6 according to requirement. Collect the message bits from these pixels from left to right. Do these steps repeatedly until the complete message bits extracted. After getting the complete extracted message bits convert these message bits into original message by using Braille’s character representation table.

It can be understood through the example. Let us take an original image with size 4*4 pixels then generate the interpolated pixels by following above discussed procedure. We have a message M as 1011010100101101 and interpolated pixels generated as from left to right.



13	25	75	82
32	48	80	92
53	62	89	95
74	84	94	98

13		25		75		82
32		48		80		92
53		62		89		95
74		84		94		98

13	**18**	25	**50**	75	**78**	82
32	**40**	48	**64**	80	**86**	92
53	**57**	62	**75**	89	**92**	95
74	**79**	84	**89**	94	**96**	98

13	**18**	25	**50**	75	**78**	82
22	**29**	**36**	**57**	**77**	**82**	**87**
32	**40**	48	**64**	80	**86**	92
42	**48**	**55**	**69**	**84**	**89**	**93**
53	**57**	62	**75**	89	**92**	95
63	**68**	**73**	**81**	**91**	**94**	**96**
74	**79**	84	**82**	94	**96**	98

Fig 1. Procedure to generate Cover image with interpolated pixels from original image

Interpolated pixels	18	50	78	22	29
Binary values of pixels	00010010	00110010	01001110	00010110	00011101
Secrete message bits	10	11	01	01	00
Stego image pixels	18	49	77	23	28

Fig 2. Insertion of secrete message in cover pixel and obtained result as stego image.

Stego image pixels	18	49	77	23	28
Binary bits of stego pixels	00010010	00110001	01001101	00010111	00011100
Extract message bits	10	11	01	01	00

Fig 3. Extraction of message from stego pixels

This is the explanation part of this proposed algorithm which is discussed above with the help of an example. This algorithm is implemented using MATLAB on distinct datasets of images to analyse this proposed work.

IV. Parameters used for analysis

PSNR: It stands for 'Peak Signal to Noise Ratio'. It is defined as the ratio of maximum possible power to the corrupting noise which affected the image representation. Unit to measure this factor is decibel (DB).

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{I^2}{\mathrm{MSE}}\right]$$

MSE: It stands for 'Mean Square Error' which can be evaluated as the difference measuring function between original certified image pixels and stego image pixels. MSE is a risk function which can be calculated as expected squared error value.

$$\mathrm{MSE} = \frac{1}{[P \times Q]^2}\sum_{i=1}^{P}\sum_{j=1}^{Q}(R_{ij} - S_{ij})^2$$

V. Experimental Result

This proposed algorithm is evaluated to take its advantage over the already existing works. Different sample of images are tested for the comparison purpose of this algorithm to the existing algorithms.

Results for image Lena

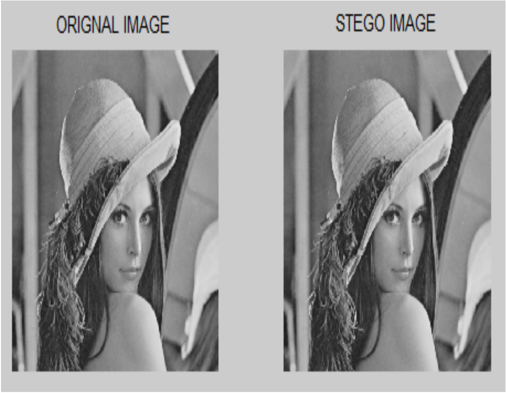


Fig 4. Original and stego image

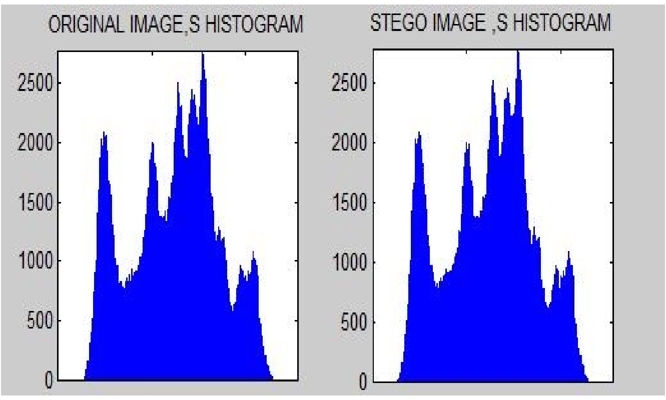


Fig 5. Histogram for message size 1024 bits for message size 1024 bits

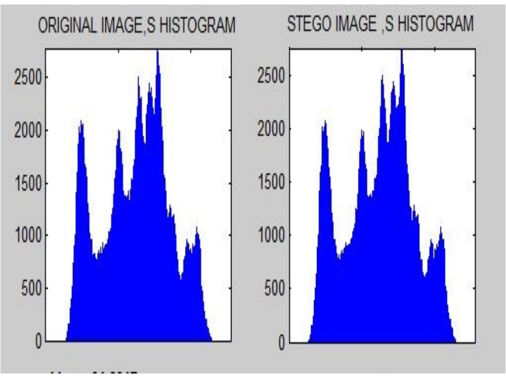


Fig 6.Histogram for message size 2048 bits

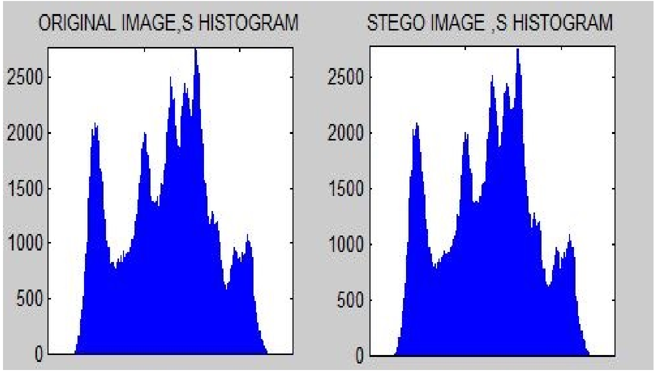


Fig 7. Histogram for message size 4096 bits

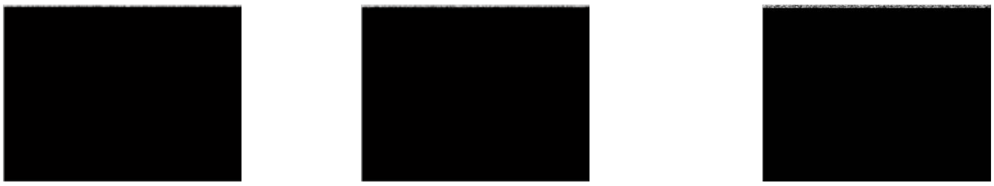


Fig 8. Difference between Original and stego image for message size 1024, 2048 bits and 4096 bits

Results for image Baboon

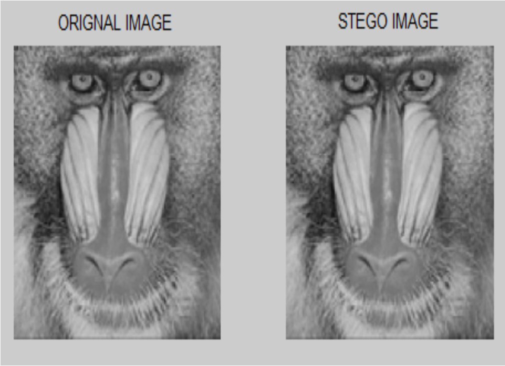


Fig 9. Original and Stego Images.

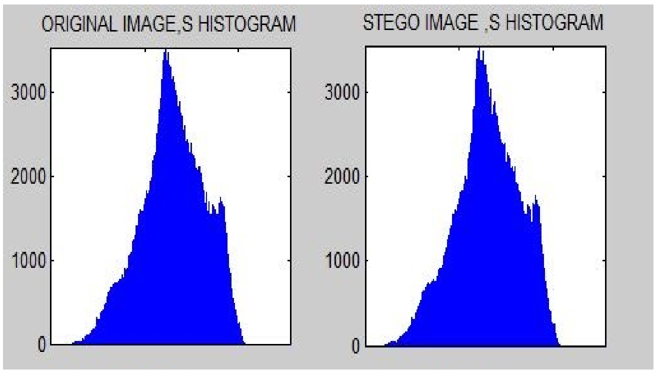


Fig 10. Histogram for message size 1024 bits.

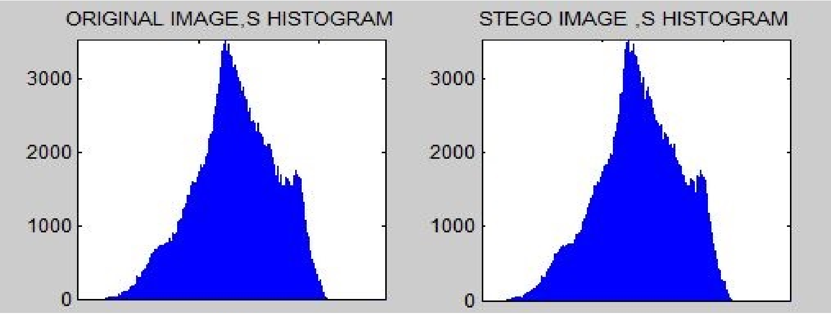


Fig 11. Histogram for message size 2048 bits

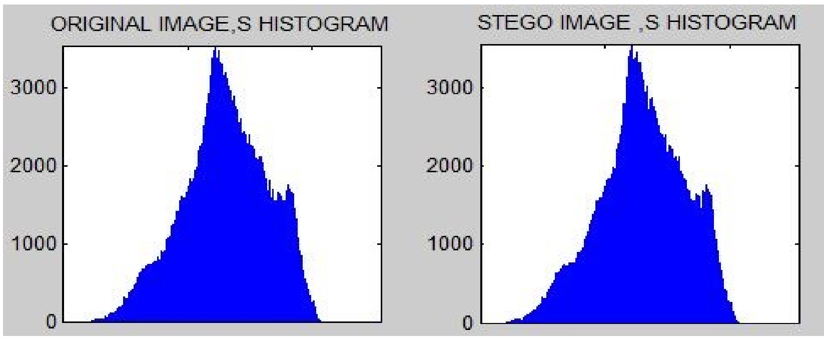


Fig 12. Histogram for message size 4096 bits

Fig 13. Difference between Original and stego image for message size 1024, 2048 and 4096 bits

TABLE 2: Comparison between proposed work and existing methods

Technique	**Image**	**Image Size**	**PSNR on Message= 1024 bits**	**PSNR on Message= 2048 bits**	**PSNR on Message= 4096 bits**
LSB Technique	Lena	512*512	53.6442	50.1237	42.5700
LSB Technique	Baboon	512*512	53.3499	50.2320	47.2027
Chaotic Approach	Lena	512*512	38.6432	35.5419	32.5876
Chaotic Approach	Baboon	512*512	34.1444	31.3183	28.2366
Proposed Method	Lena	512*512	60.415	55.556	52.568
Proposed Method	Baboon	512*512	59.456	55.123	51.562

VI. Conclusion

In image Steganography, different techniques have been already in uses which are proposed earlier by many of the researchers or authors with respect to the concealed message transformation between sender and receiver by obscuring the message within cover media i.e. image. In this perspective to enhance the security to the confidential information, this paper introduced a novel technique for obscuring the data. This paper provides a novel Steganography technique which uses Braille's method for message conversion and even odd pixels values and parity checker for message hiding purpose. It concludes with the higher capacity, PSNR and MSE values and future work may improve this technique.

REFERENCES

[1] A K Singh, J Singh, Dr. H V Sigh, “Steganography in Images Using LSB Technique”, International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol.5 Issue 1 January 2015.

[2] Shweta Maurya et al., "An Improved Novel Steganographic Technique for RGB and YCbCr Colorspace.", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, Page no 377-381, May- 2014,.

[3] Sharda, Shikha, and S Budhiraja, "Image Steganography: A review." International Journal of Emerging Technology and Advanced Engineering 3.1 Page no 707-710, 2013.

[4] S Goel, A Rana & M Kaur, “A Review of Comparison Techniques of Image Steganography”, Global Journal of Computer Science and Technology, Vol. 13 Issue 4 Version 1.0 , 2013.

[5] N. Johnson, Z. Duric, and S. Jajodia, “Information Hiding: Steganography and Watermarking Attacks and Countermeasures”. Boston: Kluwer Academic Publishers, 2000.

[6] K Joshi, R Yadav, and S Allwadhi, "PSNR and MSE based investigation of LSB." Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on. IEEE, 2016.

[7] Bedwal, Tushina, and M Kumar, "An enhanced and secure image Steganographic technique using RGB-box mapping." Confluence 2013: The Next Generation Information Technology Summit (4th International Conference) IET, 2013.

[8] Rahul Rishi, and S Batra. "A new steganography method for gray level images using parity checker." International Journal of Computer Applications 11, no. 11 , 2010.

[9] Jung, Ki-Hyun, and Kee-Young Yoo, "Steganographic method based on interpolation and LSB substitution of digital images." Multimedia Tools and Applications 74, no. 6 , 2015.

[10] K Joshi et al.,” An Enhanced Method for Data Hiding using 2-Bit XOR in Image Steganography”, International Journal of Engineering and Technology (IJET), 2016.

[11] Abdelmgeid, A., et al., "New Image Steganography Method using Zero Order Hold Zooming" International Journal of Computer Applications 133.9 , Page no. 27-31, 2016.

[12] AA, Abdelmgeid, Tarek AA, Al-Hussien Seddik, and M. H. Shaimaa, "Improving ZOH Image Steganography Method by using Braille Method." International Journal of Computer Applications (0975-8887) Vol. 151- no. 7, October 2016.

[13] Ali, Abdelmgeid Amin, and Al–Hussien Seddik Saad. "Image Steganography Technique By Using Braille Method of Blind People (LSBraille)" International Journal of Image Processing (IJIP) 7, no. 1, Page no. 81-89, 2013.