An Enhanced Method for Data Hiding using 2-Bit XOR in Image Steganography

Kamaldeep Joshi [#1], Rajkumar Yadav [#2] , Gaurav Chawla [*3]

[#] Department of Computer Science and Engineering, University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak-124001, Haryana, India

[1] kamalmintwal@gmail.com

[2] rajyadav76@rediffmai.com

[*] Department of Computer Science and Engineering, Faculty of Engineering and Technology, Jamia Hamdard University, New Delhi-110062, India

[3] chawla.gaurav17@gmail.com

***Abstract*—As we all know security is needed when we want to send data over any medium so this requires a secure medium to send data. That's why steganography comes in mind whose aim is to send data securely without knowing of any hacker. In this paper, a new technique is projected whose aim is to keep secrete communication intact. The proposed method blends the advantage of 2 bit LSB and XOR operation. In this, first we are XORing the 8th, 1st bit of data and 7th, 2nd bit of data after this two bit are obtained. These obtained bits are replaced at the LSB position. However, with some way, any person get know about hidden message and it takes the LSB position bit then there are no chances of getting message as it is not the actual message. An experiment was performed with different dataset of images. Furthermore, it was observed that the proposed method promises good result as the PSNR and MSE are good. When the method was compared with other existing methods, it shows enhancement in the imperceptibility and message capacity.**

Keyword - Steganography, XOR, Information Hiding, LSB

I. INTRODUCTION

As the internet is the basic need in today's life. Internet is the most unsecure platform to communicate but because of its features many users prefer this platform to communicate and that's why the security feature comes in mind. This platform is prone for attacker and because of vast amount of information is transferred an attacker can easily able to identify what goes on. To overcome this one idea is to while communicating we can alter the secret data so that the attacker can't able to detect it and another idea is that we can make the medium so secure that the presence of message can't be revealed. So, the first term is known as Cryptography and the latter is known as Steganography. First technique aim is to change the text in irritable form and latter technique aim is to make the medium so secure that message presence can't be revealed. For steganography technique we use cover object, secret message and using this technique we embed the text in the cover object and this is known as stego-object [1]. Cover object may be any multimedia file like image, text, audio, video etc. For hiding secret data, we can use image as cover object and known as image steganography, we use audio for storing data which is known as audio steganography, similarly video files are also used for embedding the secret data called video steganography. Among these most popular technique is digital image steganography. There are two type of steganography method. They are spatial domain and transform domain [2].

A. Spatial Domain[3]

In this, image pixel value are substituted or changed by new value of secret message. Different techniques are used to substitute message value in the image pixel. When message is hidden into the original image known as cover object and after embedding message a new image is formed known as stego image whose value may be different from the original image pixel. This method includes technique like Least Significant Bit Method [4, 5], Gray Level Modification Method [6], Pixel Value Differencing Method [7, 8], Pixel Indicator Method [9, 10] etc.

B. Frequency Domain [11]

This method includes technique like DCT (Discrete Cosine Transformation) [12], DWT (Discrete Wavelet Transformation) [13], DFT (Discrete Fourier Transformation) etc [14]. With the help of these transform the message is hidden in the cover image.

There are various factors like PSNR, MSE, and robustness of image that determine the effectiveness of a steganography method. A method is effective when it is applied to the cover object it is less susceptible to guess by an attacker whether data is hidden or not. A method is found to be best if image is less distorted means quality of stego image is better when compared to original image this is known as imperceptibility.

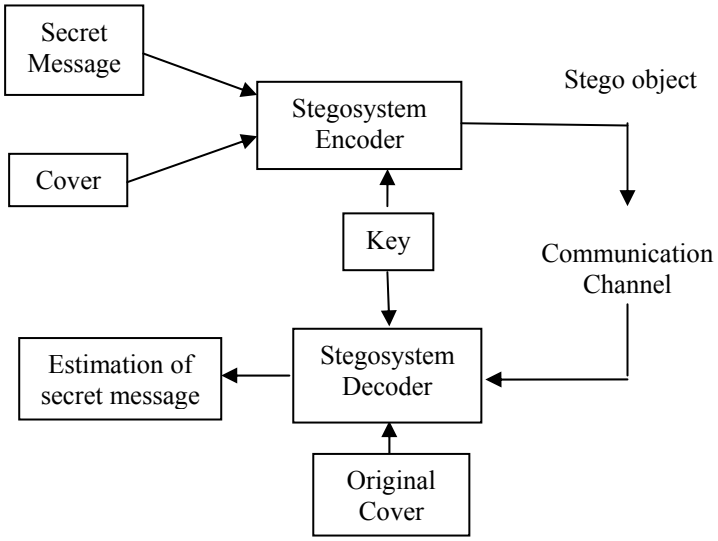


Fig. 1. Basic structure of steganography technique

II. LITERATURE REVIEW

We are using spatial domain methods which include various techniques for hiding data in an image. LSB technique replaces the last significant bit of the pixel value of original image (cover object) with the secret message. This method provides better PSNR value. The image is also less distorted because it hides at LSB position only change done is of value '1'. So, this change can't be detected by human eyes. As the original message is on the LSB, it can be directly accessed by the intruder. Also in 1 bit LSB method only one bit is hidden on a pixel. Khan et al. [15] introducing the concept of HSI image in which the RGB image is first converted into the HSI (hue saturation intensity) color model. The obtained image is divided into three planes: H plane, S plane, I plane. They use I-plane which is divided into 4 parts and then these sub blocks are rotated with different angle value and them also doing encryption on the secret data. On secret data, they are using the MLEA encryption technique and then the cipher text is stored as LSB in the sub block of image and data is stored using the M-LSB substitution (magic LSB) and these sub blocks are combined to make the I-plane and after this the all the three plane (H-plane, S-plane, I-plane) are combined and stego image is formed. This method has low message carrying capacity as only one bit is hidden on a single pixel. Jung and Yoo [16] proposed a new method using the combination of interpolation and LSB technique is used for data hiding. They used the semi reversible technique in which the receiver can obtained without distortion of secret message and also the original image. They first use the concept of interpolation in which they are scaling up the matrix or down the matrix, scaling up result in increase the size of matrix and scaling down result in decreasing the matrix size. After this, secret data is arranged in bit and then 3 bit are stored at 3 LSB position. This method increases the quality and prone to the attack as secret data is hidden after doing interpolation technique. At the receiver end, receiver receives the stego image and data is extracted from the 3 LSB position. The data hidden by this method is also less as the data is hidden on the interpolated values not in the complete image. Abduallah et al. [17] introduces a reversible data hiding scheme based on 3LSB position and mix column transformation is applied. In this, they are dividing the cover image into either 3*3, 5*5, 7*7 blocks. One block is chosen from the cover image matrix and known as block matrix and another matrix known as transformation matrix is chosen randomly which must have an inverse. After this, block matrix element are converted into equivalent binary form and last 3 bit of this matrix element are used and a new matrix is formed. After formation of this matrix, it is multiplied to the transformation matrix and then result is used to make a new matrix which is used for data hiding. Abdul and Gutub [18] proposed a new improved technique that uses the RGB image which is of the 24 bits. They divide these bits in three bytes. To take out the key management system, the method used one channel for indicator. They are using the size of the secret data as selection of criteria for first indicator channel to insert security. This method also does not utilize all the channel of the of the cover image as one channel is used for the indicator channel and only two other channels are used to hide the data.

TABLE I. Indicator Value Based Action

Indicator channel	Channel 1	Channel 2
00	No data to hide	No data to hide
01	**No data to hide**	**Substitute 2 LSB of channel**
10	Substitute 2 LSB of channel	No data to hide
11	**Substitute 2 LSB of channel**	**Substitute 2 LSB of channel**

TABLE II. Indicator Channel Selection Criteria

Type of length(N) of secret message	1 Level selection select indicator channel, first element of sequence	2 level selection binary N parity-bit	
Even	R	GB	BG
Prime	B	RG	GR
Else	G	RB	BR

III. PROPOSED TECHNIQUE

In the proposed technique data is inserted at LSB position based on computation. Suppose I^C is the cover image and its pixel are generated and after this the pixel are converted into its 8bit binary number. This 8 bit binary number is used for computation. Using the 8th bit of present pixel and the 1st bit of secret message, XOR operation is performed and in the same way the 7th bit and next bit of secret message are also XORed. The two bits obtained after XORing the bits. These two computed bits are inserted at the last two LSBs of the present pixel. This cycle repeats until the value of the message becomes zero i.e. message consumed. As this method provide, security against attacks because we are inserting data after performing XOR operation. XOR operation is interesting if we XOR (a, b) = c then XOR (b, c) = a. It means that when XOR two numbers then result obtained is XOR with any operand then result shows another operand.

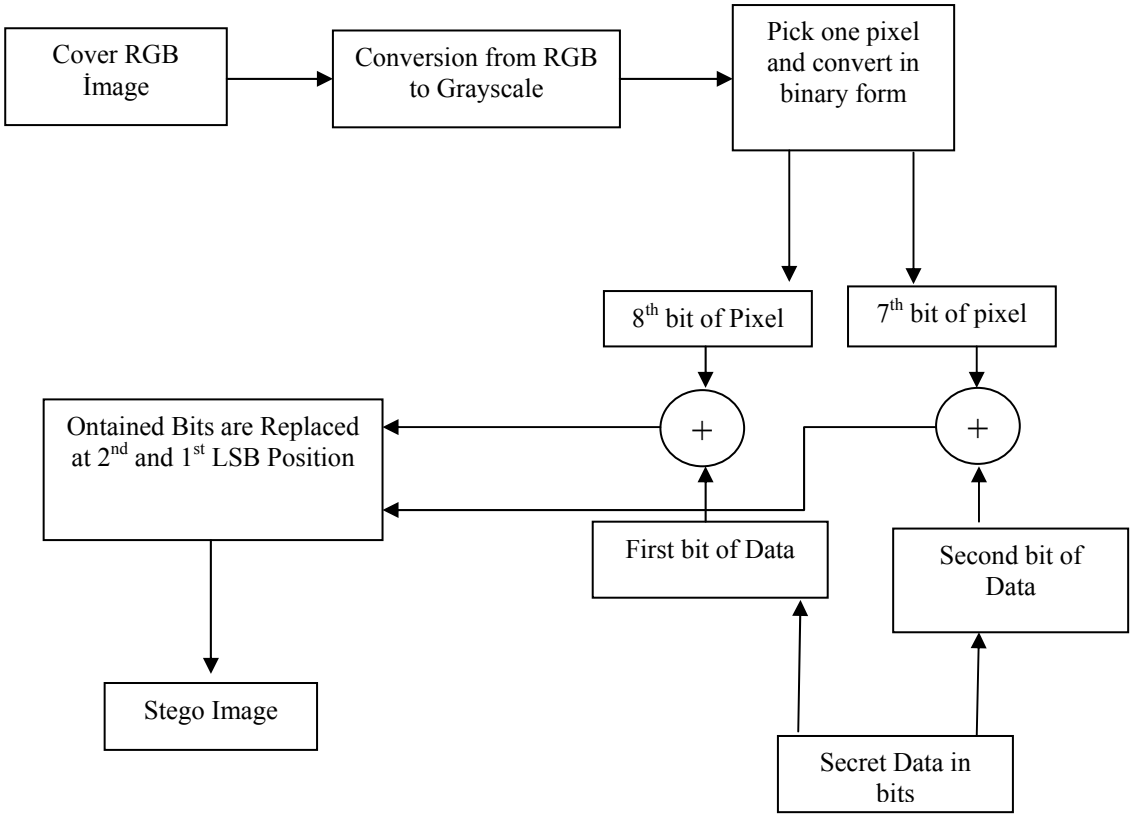


Fig. 2. A detailed pictorial representation of the proposed technique.

A. (Algorithm 1) Embedding Algorithm

Input – Cover Image (I^C),
Secret Message and Secret Key (K^{Key})

Output– Stego Image (I^s)

1. Initialize I^C ←Cover Image, D ←Secret Message, K^{Key} ←Secret Key
2. While Counter <= size of the message block do
3. For each pixel
    a. Pick a pixel I (x, y) from the image and convert it into 8 bit binary number.
    b. Find the 8th bit and 7th bit of the pixel value.
    c. Find secret message first and second bit
    d. Perform XOR on 8th bit of pixel with first bit of secret message and also perform XOR on 7th bit of pixel with second bit of secret message.
    e. Store the obtained bit at 2nd and 1st LSB position of the present pixel.
4. Counter=Counter+1
5. Repeat step 3 for each pixel until the message is terminated.

Output – Stego Image (I^s)

B. (Algorithm 2) Embedding Algorithm

Input – Stego Image (I^s)
Secret Key (K^{Key})

Output – Message
Original image

1 Initialize I^s ←Stego image,
K^{Key} ←Secret Key

2 For each pixel
    a. Pick a pixel I (x, y) from the image and convert it into 8 bit binary number.
    b. Find the 8th, 7th, 2nd, 1st bit of the pixel value.
    c. Perform XOR on 8th , 2nd bit and also on 7th, 1st bit
    d. Calculated bit are the message bit and arrange message in 8 bit form and convert it into equivalent ‘character’ value.

3 Repeat step 2 for each pixel of stego image.

For example:-

155	120	56
123	28	90
68	134	255

Secret Message:-
00111001

For embedding secret message:-
Pick 1st pixel and convert it into 8 bit binary number.

155= 10011011
Pick 8th and 7th bit of message and also two bit of Secret data
8th bit=1 1st bit of message=0
7th bit=0 2nd bit of message=0
XOR (8th, 1st bit) =1
XOR (7th, 2nd bit) =0
Insert the calculated value at 2nd and 1st LSB position
New pixel after message insertion
10011010=154
Pick 2nd pixel and convert it into 8 bit binary number.
120=01111000
Pick 8th and 7th bit of message and also two bit of Secret data

8th bit=0 1st bit of message=1
7th bit=1 2nd bit of message=1
XOR (8th, 1st bit) =1
XOR (7th, 2nd bit) =0
Insert the calculated value at 2nd and 1st LSB position
New pixel after message insertion
01111010 = 122
Pick 3rd pixel and convert it into 8 bit binary number.
56= 00111000
Pick 8th and 7th bit of message and also two bit of Secret data
8th bit=0 1st bit of message=1
7th bit=0 2nd bit of message=0
XOR (8th, 1st bit) =1
XOR (7th, 2nd bit) =0
Insert the calculated value at 2nd and 1st LSB position
New pixel after message insertion
00111010=58
Pick 4th pixel and convert it into 8 bit binary number.
123= 01111011
Pick 8th and 7th bit of message and also two bit of Secret data
8th bit=0 1st bit of message=0
7th bit=1 2nd bit of message=1
XOR (8th, 1st bit) =0
XOR (7th, 2nd bit) =0
Insert the calculated value at 2nd and 1st LSB position
New pixel after message insertion
01111000=120
Other pixel left because of data is not left.
So, the new matrix become

154	122	58
120	28	90
68	134	255

Extraction is done in the same way
Pick first pixel and convert it into 8 bit binary number
154=10011010
Find 8th, 7th, 2nd, 1st bit
8th bit =1 2nd bit=1
7th bit=0 1st bit=0
Perform XOR
XOR (1, 1) =0
XOR (0, 0) =0
Bit of data extracted are 00
Pick Second pixel and convert it into 8 bit binary number
122=01111010
Find 8th, 7th, 2nd, 1st bit
8th bit =0 2nd bit=1
7th bit=1 1st bit=0
Perform XOR

XOR (0, 1) =1

XOR (1, 0) =1

Bit of data extracted are 11

Pick Third pixel and convert it into 8 bit binary number

58=00111010

Find 8th, 7th, 2nd, 1st bit

8th bit =0 2nd bit=1

7th bit=0 1st bit=0

Perform XOR

XOR (0, 1) =1

XOR (0, 1) =0

Bit of data extracted are 10

Pick fourth pixel and convert it into 8 bit binary number

154=01111000

Find 8th, 7th, 2nd, 1st bit

8th bit =0 2nd bit=0

7th bit=1 1st bit=0

Perform XOR

XOR (0, 0) =0

XOR (1, 0) =1

Bit of data extracted are 01

The extracted bits are arranged in and divided it into 8bit and then converted into equivalent character value.

00111001

So, the hidden message is 00111001

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed technique is simulated using MATLAB 2010b

C. Data Set

We used different images for obtaining the result and did analysis with to the proposed method. We use different Dimension of images like 128×128,256×256, 512×512. Images used are like baboon, Lena, Girl, River, Pepper of 512×512 and 256*256 , 128×128 images like Tree, House, Girl, Couple etc.

D. Quantitative Evaluation

We used different cases. According to case 1, secret message of 8 KB is embedded in different grayscale images having size 256×256. The second case is to embed message of distinct sizes in the same images having dimension (256×256 in pixels). In third case multiple images with different resolution (128×128, 256×256, and 512×512) were used. The size of data is same as case1. We are using different existing scheme for comparison. They are Classical LSB, SCC [19], PIT [9], FMM [20], and CST [21].

We used different parameters on which quality of the proposed method was analysed. They are PSNR (Peak Signal to Noise Ratio), MSE (Mean Squared Error), STD (Standard Deviation), MEAN (Mean of the original image) etc.

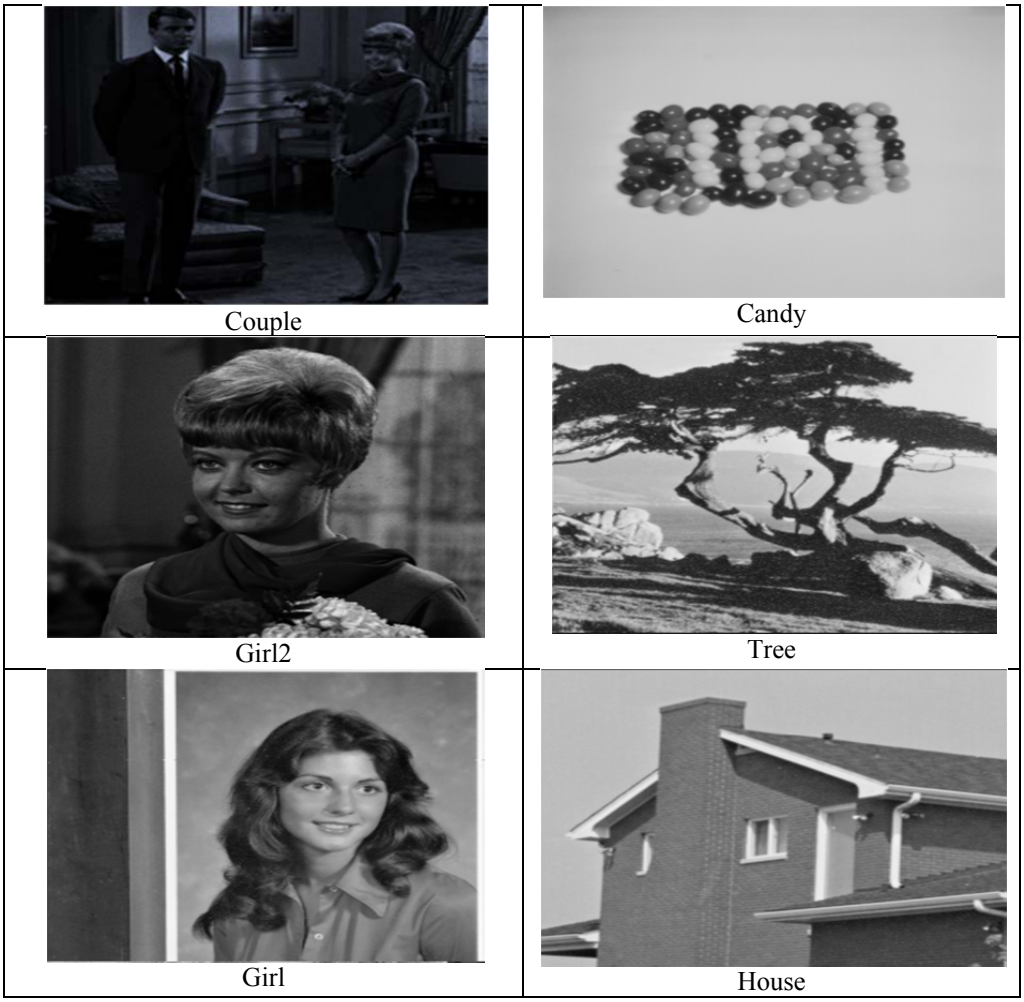


Fig. 3. Original image which we have used for analysis for case 1

TABLE III. Different Cases for Evaluation of Proposed Method

Cases	Message Size	Size of Image (in pixels)	Images
Case 1	Equal, 8KB	256*256	Different
Case 2	Variable (2KB, 4KB, 6KB, 8KB)	256*256	Same
Case 3	Equal , 8KB	(128*128),(256*256), (512*512)	Different

PSNR

This calculates the PSNR. Higher the value of PSNR, higher the quality of image. İt is measured in decibels.

$$\text{PSNR} = 10\log_{10}\left[\frac{(2^b-1)^2}{\text{MSE}}\right] \quad (1)$$

MSE

Lesser the value of MSE better the quality of stego image.

$$\text{MSE} = \frac{1}{[N \times M]}\sum_{i=1}^{N}\sum_{j=1}^{M}(X_{ij} - Y_{ij})^2 \quad (2)$$

Where N, M is the size of image, x_{ij} are ijth pixel of original image and y_{ij} are ijth pixel of stego image. b is the total no of bit in a pixel for example in gray scale image the value of b is 8.

Case 1 Different Images of 256×256 with 8 KB Data

In this case we are using different images of same resolution for embedding the secret message. Embedding text is 8 Kb in size. We have use the image like house, tree, girl, candy and couple for evaluation and analysis is done on this behalf. The analysis requires the use of various factors for affecting a steganography method. The method performance is calculated on the basis of these factors. How these factor work a method is applied on it.

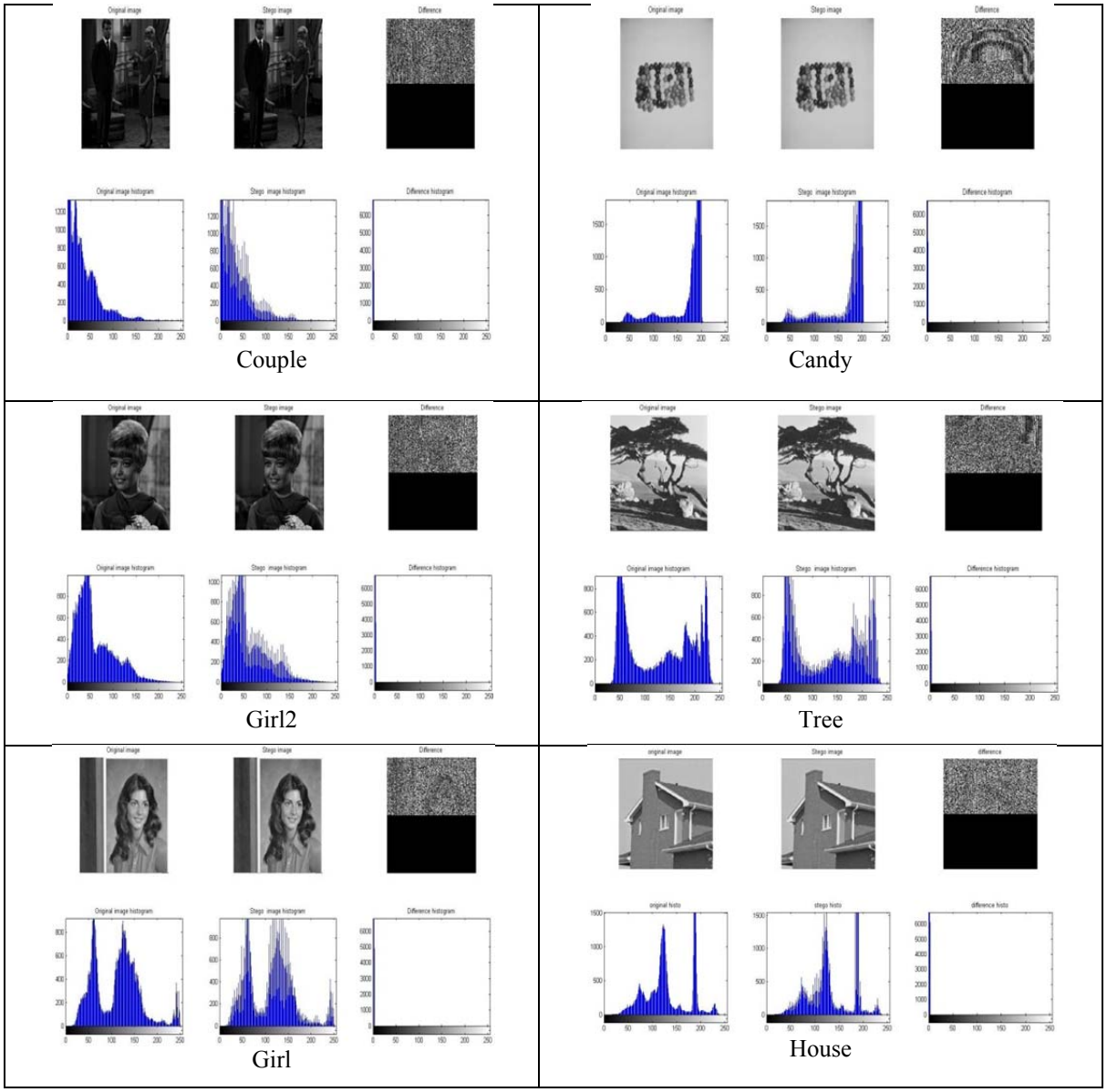


Fig. 4 Original images, its stego image, difference image and their histograms

Figure 4 shows the original image, stego image, difference between these image, and their respective histograms. Original image is image which we used for embedding secret message, stego image contains the original image with message is embedded. Histograms of both the image are also shown in this figure.

Table 3 contains the original and stego image's PSNR, MSE, MAXERR, L2RAT, Mean and standard deviation of both images [22].

TABLE IV. Analysis of 8Kb Message in Image of 256 Resolution

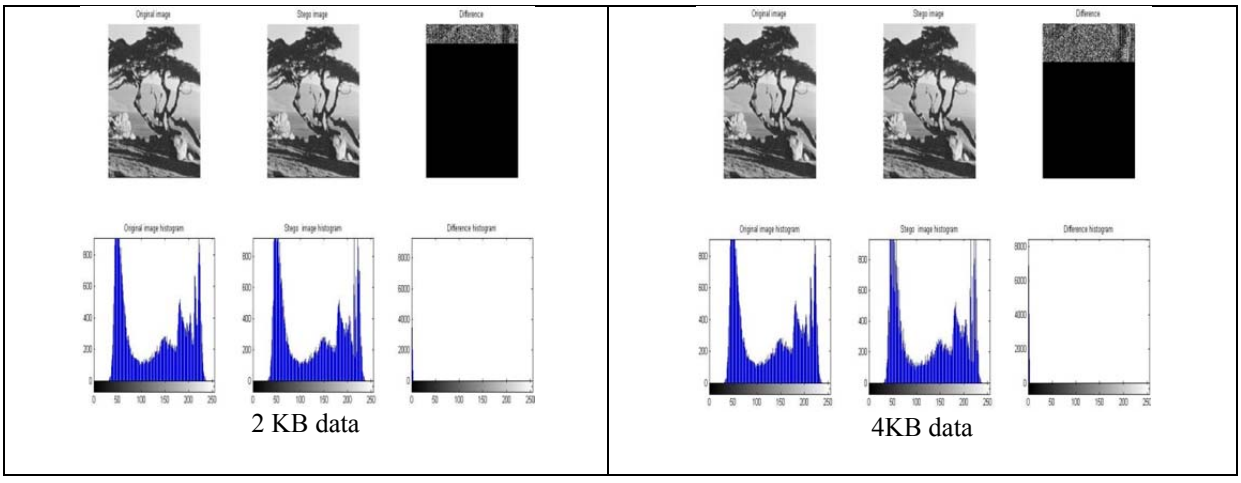
Image	PSNR	MSE	MAXERR	L2RAT	MEAN of Original Image	MEAN of Stego image	Standard Deviation of Original image	Standard Deviation of the stego image
Couple	47.7844	1.0830	3	1.0068	26.5820	26.2500	17.3316	17.1407
Candy	46.9721	1.3058	3	0.9976	178.2813	179.0391	9.3523	9.2997
Girl 2	47.2773	1.2172	3	1.0035	36.4805	36.2188	14.6611	14.6123
Tree	47.4958	1.1575	3	0.9980	149.8984	149.9102	54.7294	54.8994
Girl	46.8252	1.3507	3	0.9994	63.0273	62.7539	9.1216	9.2239
House	46.3676	1.5008	3	0.9978	179.2969	179.9453	24.4458	24.6894

Case 2 Different Images of 256×256 with different size data

Fig. 5. Original image having resolution 256

In this case same image is used for embedding variable size of data. Image used is Tree. Image having the 256*256 resolution. In this image, different data size like 2 KB, 4 KB, 6KB, 8KB etc. are embedded.

Figure 6 shows different images when variable size data is embedded. The below diagram shows original image and its histogram, stego image and its histogram and difference between two images and histogram of this difference. The difference image of original and stego image represent the portion of the stego image where the data is hidden.



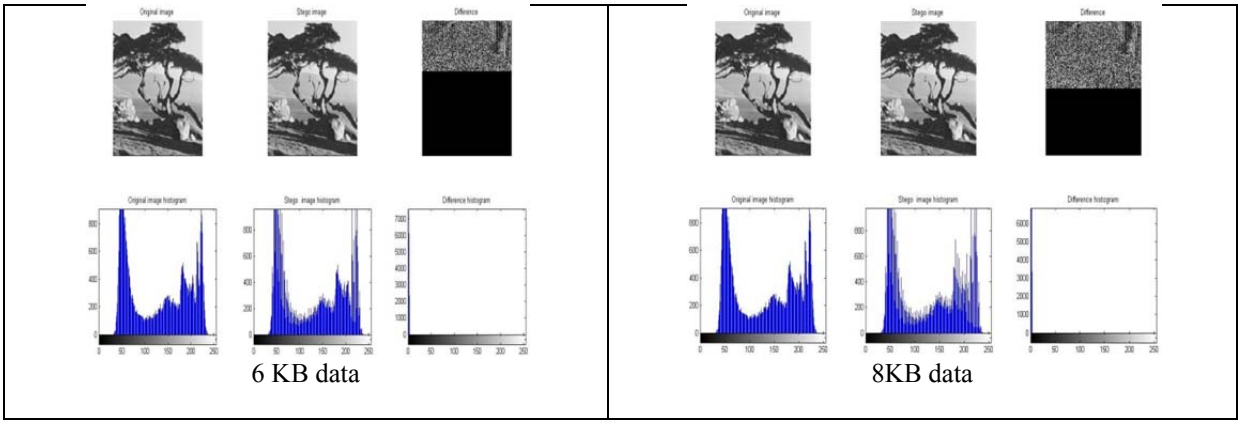


Fig. 6. Embedding of variable size data

In this case we have embedded different size data in the same image. Figure 6 shows different data size inserted in same image with their histograms. The original image, the stego image and difference is shown and also their histograms are shown.

TABLE V. Analysis for Different Size Data in Same Image

Image	PSNR	MSE	MAXERR	L2RAT	MEAN of Original Image	MEAN of Stego image	Standard Deviation of Original image	Standard Deviation of the stego image
2KB	53.8605	0.2673	3	0.9992	149.8984	149.8294	54.7294	54.6560
4KB	50.8059	0.5401	3	0.9990	149.8984	149.9102	54.7294	54.7242
6KB	48.8605	0.8453	3	0.8453	149.8984	149.8438	54.7294	54.8402
8KB	47.4958	1.1575	3	0.9980	149.8984	149.9102	54.7294	54.8994

Case 3 Different Image Size with 8 Kb Data Embedded.

Fig.7. Original image of different resolution

We use some of the images with different resolution. In this case we embed equal amount of data in three different image of different resolution. Embedding data size is of 8 KB and image resolutions are different. Figure 8 also shows original and stego image and their respective histograms.

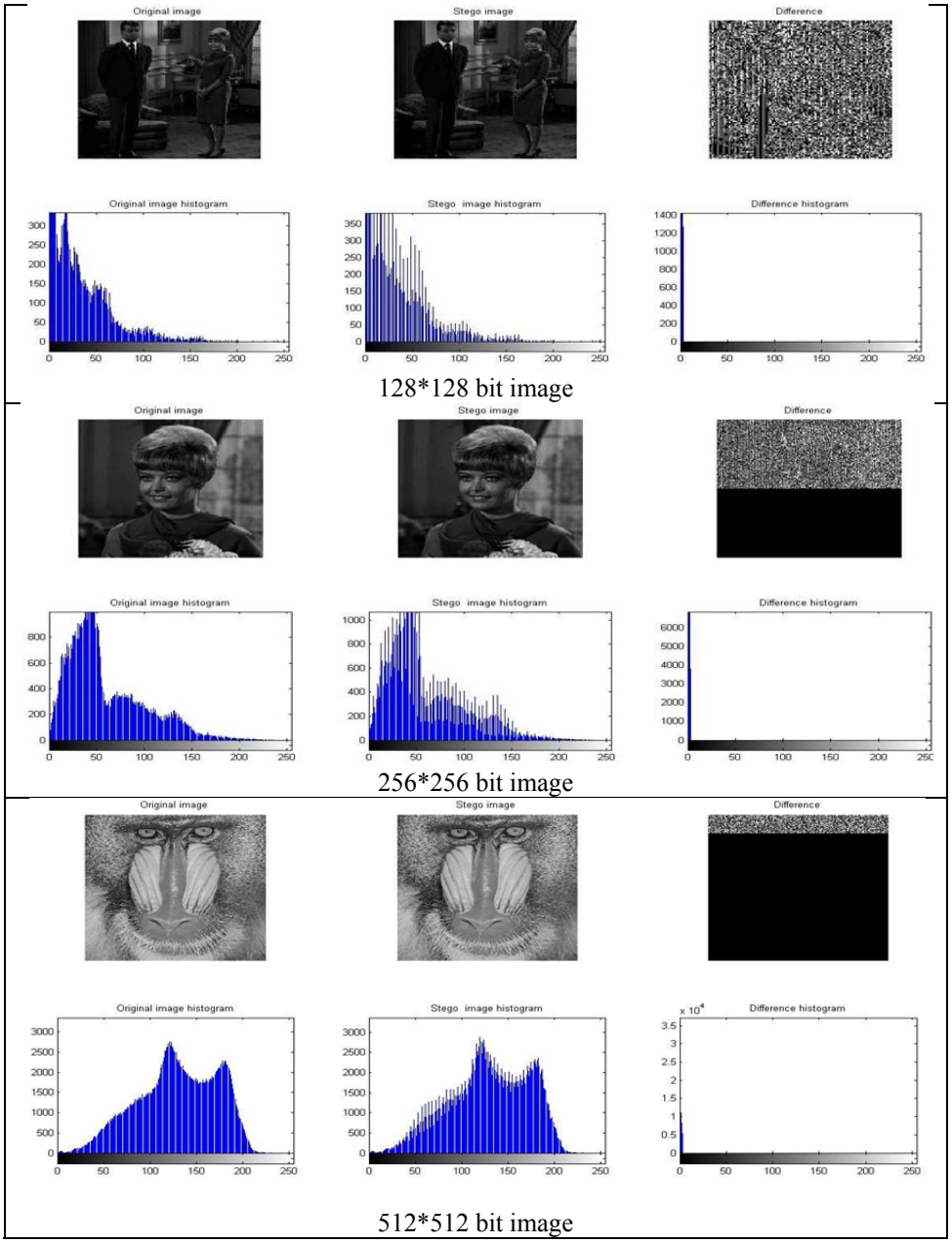


Fig. 8. Histogram of different Size Image with same amount of data

TABLE V. Analysis for same size data in Different Size Image

Image	PSNR	MSE	MAXERR	L2RAT	MEAN of Original Image	MEAN of Stego image	Standard Deviation of Original image	Standard Deviation of the stego image
128 bit (Couple)	44.9681	2.0714	3	1.0112	23.2109	22.5234	13.6091	13.6064
256 bit (Girl2)	47.2773	1.2172	3	1.0035	36.4805	36.2188	14.6611	14.6123
512 bit (Baboon)	52.7030	0.3490	3	0.9999	131.2734	131.2070	43.7456	43.8849

This table contains data with different image of different size and 8 KB data is embedded. As the image size increase there is improvement in image quality.

V. COMPARISON

We are using different method for comparison to be done with the proposed method. There we are using PIT method, SCC method, FMM method, CST method and classic LSB method. Around 50 images for comparison were taken. This comparison shows that the proposed method is better from other method except the classic LSB method.

TABLE VI. Comparison of proposed method with different method

Image Name	Classic LSB Method	SCC Method [19]	PIT[9]	FMM[20]	CST[21]	Proposed Method
House	52.04	52.89	51.07	67.55	51.17	46.37
Couple	48.40	47.91	46.58	46.25	55.91	47.78
Girl	52.04	52.89	51.07	67.55	51.17	46.83
Candy	48.40	47.91	46.58	46.25	55.91	46.97
Tree	56.27	49.76	48.60	46.12	38.54	45.50
Girl 2	56.02	47.26	46.39	45.82	47.49	47.28
Average of 150 Images	45.28	41.83	41.22	41.97	37.38	45.30

VI. CONCLUSION

In this paper, we proposed a novel image steganography technique which increases security. Here we are using the image (gray scale image) which is 2 dimensional, which reduces the processing time and enhance the security of hidden data. In this proposed method, large amount of data can be hidden because we are hiding 2 bit of data in one pixel. The stored data at this position is not the actual data but it is obtained by performing the XOR operation. We are performing the XOR operation using 8th bit, first bit of data and 7th bit, 2nd bit of data. The result produces two bits which are not the actual data and we are storing this obtained bit at the LSB position. If an attacker able to detect the LSB bit then we have no need of getting worried because this is not the actual data at this position. The proposed method is feasible in the sense that this method is easy to implement, easy to understand and also provide security against attack. This proposed method also makes the stego image of better quality. After seeing the stego image, no one could imagine the presence of message is in the image. After implementation and analysis we get the good imperceptibility and capacity.

REFERENCES

[1] Cheddad A, Condell J, Curran K, Kevitt P (2010) Digital image steganography:survey and analysis of current methods. Signal Process 90:727-752.
[2] Anderson RJ, Petitcolas FAP (1998) On the Limits of Steganography , IEEE Journal on Selected Areas in Communications, 16:474-481.
[3] Johnson NF, Jajodia S(1998) Exploring steganography: Seeing the unseen, IEEE Computer Journal, 31:26–34.
[4] Mielikainen J (2006) LSB matching revisited, Signal Proc Lett IEEE 13:285-287.
[5] Yang C-H, Weng C-Y, Wang S-J, Sun H-M (2008) Adaptive data hiding in edge areas of images with spatial LSB domain systems, Inform Forensic Secur IEEE Trans 3:488-497.
[6] Al-Taani AT, Al-Issa AM (2009) A novel steganographic method for gray-level images. World Academy of Science, Engineering and Technology3:613-618.
[7] Wang C-M, Wu N-I, Tsai C-S, Hwng M-S (2008) A high quality steganographic method with pixel-value differencing and modulus function J Syst Softw, 81:150-158.
[8] Wu D-C, Tsai W-H (2003) A steganographic method for images by pixel-value differencing. Pattern Recogn Lett 24:1613-1626.
[9] Gutub AAA (2010) Pixel indicator technique for RGB image steganography. J Emerg Technol Web Intell 2:56-64.
[10] Gurub A, Ankeer M, Abu-Ghalioun M, Shaheen A, Alvi A (2008) Pixel indicator high capacity technique for RGB image based steganography. In WoSPA 2008-5th IEEE International Workshop on Signal processing and its Applications 1-3.
[11] Raftari N, Masoud A, Moghadam E (2012) Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT, IEEE Fourth International Conference on Computational Intelligence, Comm. Systems and Networks.
[12] Qazanfari K, Safabakhsh R (2013) High Capacity method for hiding data in the discrete cosine transform domain. J Electron Imaging 22:043009.
[13] Narasimmalou T., Joseph Allen R (2012) Optimized Discrete Wavelet Transform based Steganography IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), 88-91
[14] Chen W-Y (2008) Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques. Appl Math Comput 196:40-54.
[15] Khan M, Muhammad S, Mehmood I, Rho S, Baik S (2015) A novel magic LSB substitution method using multi-level encryption and achromatic component of an image, Springer Science+Business media, 1-27.
[16] Jung KH, Yoo KY (2014) Steganographic method based on interpolation and LSB substitution of digital images, Springer Science+Business Media, 74:2143–2155
[17] Abduallah WM, Rahma Abdul Mohem S. and Pathan Al-Sakib Khan (2013) Reversible Data hiding scheme based on 3-Least Significant Bits and Mix Column Transform", Institute for computer Sciences, Social Informatics and Telecommunications Engineering, 405-417.

[18] Abdul A, Gutub A (2010) Pixel indicator technique for RGB Image Steganography, Journal of Emerging tevhnologies in web intelligence, 2.(1):56-64.
[19] Bailey K, Curran K (2006) An evaluation of image based steganography methods. Multimedia Tools Appl. 30:55-88.
[20] Jassim FA (2013) A novel steganography algorithm for hiding text in image using five modulus method. arXiv preprint arXiv:1307.0642.
[21] Muhammad K, Ahmad J, Rehman NU, Jan Z, Qereshi RJ (2014) A secure cyclic steganographic technique for color images using randomization. Tech J Univ Eng Technol Taxila Pakistan 19:57-64.
[22] Joshi K, Yadav R, Allwadhi S, PSNR and MSE based investigation of LSB, IEEE Proceding on International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 280 - 285, 2016.

AUTHOR PROFILE

Kamaldeep Joshi received his M.Tech degree in Computer Science and Engineering from Maharishi Dayanand University, Rohtak, Haryana (INDIA). He is currently working as an assistant professor in Computer Science and Engineering Department at University Institute of Engineering & Technology (Maharshi Dayanand University Rohtak, Haryana) India. His research interest includes Steganography, Watermarking, Biometrics and Neural Network.

Rajkumar Yadav received the Ph.D. degree in Computer Science and Engineering from Maharshi Dayanand University, Rohtak, Haryana(INDIA) in 2011.He is currently working as an assistant professor in Computer Science and Engineering Department at University Institute of Engineering & Technology (M.D. University Rohtak, Haryana) India. His research interest includes Information Hiding Techniques, Network Security and Biometrics.

Gaurav Chawla received his M.Tech degree in Software Engineering from Maharishi Dayanand University, Rohtak, Haryana (INDIA). He is currently working as an assistant professor in Department of Computer Science and Engineering, Faculty of Engineering and Technology, Jamia Hamdard University, New Delhi, India. His research interest includes Steganography, Watermarking, and Biometrics.