International Journal of Engineering & Technology, 7 (4) (2018) 4295-4299

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet. v7i4.19692
Research paper

Improved method using a two Exclusive-OR to binary image in RGB color image steganography

Hamid Mohammed Farhan [1] *, Zena Ahmed Alwan [1]

Electrical Engineering Technical College, Middle Technical University, Iraq
**Corresponding author E-mail: hamd_farhan@yahoo.com, zena782017@gmail.com*

Abstract

In this paper present adaptive technique algorithm to hide the secret Binary image inside color image to make information of binary image more save omit we used steganography technique was Least Significant Bit(LSB). We are applying Two Exclusive-OR operations between our secret Binary Image and 8-bit (Red, Green, and Blue) bands in color Image. We are hiding our secret encrypted Binary Image in the LSB of Blue bands. Each pixel will have applying Two XOR operations sequential to increases security to the Binary Image, and then store our encrypted pixel in 8-bit-LSB of Blue band, the stored data at this place is not the real data but it obtains by performing the Exclusive-OR operation. This method applied to different set of images. Furthermore, it observed that the projected method assure good result as the "Peak Signal to Noise Ratio (PSNR)" and "stands for Mean Square Error (MSE)" are good. When the method compared with other existing methods, it shows enhancement in the imperceptibility and message capacity. This method was easy to make, easy to understand and provide security against attack.

Keywords: *Image Security; Information Hiding; LSB; Steganography; Exclusive-OR Operation.*

1. Introduction

The action of concealing a hidden message that arrives with an ordinary message and sending it back to another destination is a Steganography [1-3]. Not anyone who sees the message can recognize the hidden message within. One of insertion is "LSB" methodology that is sort of easy and customary approach to present data during a type of an image [4]. Itis limited approach to every slight image manipulation other techniques such as LSB is useful image in this process of LSB method [5]. That holds encrypted data. LSB addition could be a very easy and usual technique to inserting data in an image in special domain. The limitation of this method is weak to every slight image manipulation.
Steganography needs two requires files: cover media, and the hidden data [6]. The combined cover image and the hide image will make a stego image, which is known as stego-image image [7]. LSB is one popular method, where the least significant bit of each pixel is changed by bits of the secret image until secret pixels finishes [8-11]. The danger of information being uncovered [7], therefore we use two Exclusive-OR technique makes an attempt at predomination this problem, wherever pixels, which is able to be accustomed hide information [12-14].
Picture based steganography mechanics need a picture to shroud the information in this picture is known as a cover media. Advanced pictures are put away in PC frameworks as a variety of focuses (pixels) where every pixel has three shading parts: Red part, Green part, and Blue part. Every pixel is spoken to with three bytes to show the force of these three hues (RGB) [5]. The shading channel, where the mystery information will be undetectable in, is cycling a great deal for all bits as per a particular example [13]. For instance, first piece of the mystery information is put away in the LSB of red channel, the second piece in the green channel, the third piece in the blue channel et cetera. This technique is additional secure than the LSB but still it is bear discover the cycling pattern that will detect the secret data. In addition, it has low space than the LSB steganography is also an altered method that uses the color image. Anyway in this technique, some pixels of the cover image was selected a passing number generator (PRNG) but, the secret will be hided in the blue channel of the choose pixels. Repeated this technique has editor the key and rut of ability since it employ just the Blue channel out of the three channels of their ready channels [11].

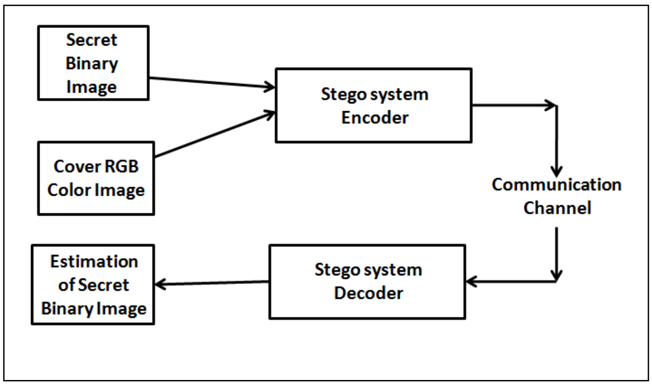


Fig. 1: Basic Structure of Steganography Technique.

A steganography method is presents in this paper, which binary image data are hidden in a 24-bit color RGB format image. Each pixel will have applying Two Exclusive-OR operations sequential to increases security to the Binary Image, and then store our encrypted pixel in 8-bit-LSB of Blue band, the stored data at this place is not the real data but it obtains by performing the Exclusive-OR operation.

2. Steganography

Steganography techniques require two files: cover media, and the data to be hidden [6]. To make a stego file we need to mix the cover image and the embedded message, this techniques in our work for image steganography known as stego-image image [7]. The LSB is One of the commonly techniques was used, its work by they pixel is replaced by bits of the secret till secret message finishes [5, 8]. The risk of information being uncovered with this method as is susceptible to all sequential scanning based techniques [7], which is threatening its security.

The main goal of steganography method is to raise level of encryption and secure communication by embedding messages into image bits and increasing pixel of image. Generally, digital image is stored as an array, which is comprised of fixed number of elements, where each of them has its own specify position and value. In case of 24-bit colure image; three component of column pixel are red, green and blue so three bytes (24-bits) reefers to each pixel intensity of image colors.

3. LSB coding

The LSB algorithm was one of the most very popular methodologies; this technique is simplest and most famous method, which hides the secret message directly through concerning the LSB of each pixel in an image. A series of bytes holding the secret data was replaced in the least weighty bit in some bytes of the cover file in order to hide them. The LSB method generally is a great way in cases where the "LSB" exchange doesn't cause significant quality degradation, such as in 24-bit bitmaps.

In calculating, the unit's value of any number was determined by the LSB it known as the bit position in a binary, that is, deciding if the number is even or odd. The LSB was also known as the right-most piece, because of the tradition in positional documentation of composing less critical digit further to one side. It is practically equivalent to the minimum huge digit of a decimal whole number, which is the digit in the ones (right-most) position.

1	0	0	0	0	1	0	0

Fig. 2: Binary Representation of Decimal 130.

The binary portrayal of decimal 130, with the LSB featured. The MSB in an 8-bit parallel number speaks to an estimation of 128 decimal. The LSB represent to an estimation of 1. For instance, to shroud the letter "M" (ASCII code 77, which is 01001101) inside eight bytes of a cover, the LSB of every byte can set like this:

10010011
01010010
10011011
11010011
10001010
00000010
01110011
00101010

The application disentangling the cover peruses the eight LSB of those bytes to reproduce the concealed byte—that is 0110001—the letter "M" As you may understand, utilizing this procedure let you shroud a byte each eight bytes of the cover. Note that there's a 50% possibility that the bit you're supplanting is the same as its substitution, as such, a fraction of the time, the bit doesn't change, which limits quality corruption.

4. 24-Bit imaging

A 24-bits color image is considered the best in definition of RGB color model where each color shows as in its primary spectral component of RGB this model based on Cartesian Coordinated System, where primary value are laid in three coursers, where secondary color known as cyan, magenta, and yellow where, they are contend of three other corners, black color is at the origin and the white is at the farthest corner from origin. Equal value include RGB are considered the line that links two corners. So the shade produce Gray color, which is called the gray line, so each of these pixels in RGB color require 8-bit for its representation where each pixel significant by 24-bit in total so the sum of possible color with 24-bit RGB reaches' (28)3= 16,777,216[15].

For example, a grid for 3 pixels of a 24-bit image can be as follows:

(01100101 00110011 11010110)
(11000001 10010110 00011110)
(10110010 10110100 01101101)

At the point when the number 207, which binary portrayal is 11001111, is implanted into the slightest noteworthy bits of this piece of the picture, the results lattice is as per the following:

(01100101 00110011 11010110)
(11000000 10010111 00011111)
(10110011 10110101 01101101)

In spite of the fact that the number was implanted into the initial 8 bytes of the framework, just the 3 underlined bits should have been changed by the inserted message. By and large, just 50% of the bits in a picture should be changed to conceal a mystery message utilizing the most extreme cover measure. Since there are 256 conceivable forces of every essential shading, changing the LSB of a pixel brings about little changes in the power of the hues. These progressions can't be seen by the human eye - in this way the message is effectively covered up. With a well-picked picture, one can even conceal the message at all and additionally second to minimum noteworthy piece and still not see the distinction. In the above illustration, back to back bytes of the picture information – from the primary byte to the finish of the message – are utilized to implant the information [5].

5. Relate work

In [8], the authors examined a method of improving the LSB method for textual message embedding. They embedded the code using all three-color channel spaces and subsequently manipulated only the least significant Bit of the pixel. The findings revealed that this approach was at risk of attacks and, on this basis, it was concluded that it was not safe. The test was performed by employing three code word lengths: 10, 20, and 30. The text to hide is very short, the PSNR was 81.141 at message length = 30.

The authors in [9] were represented a combining between LSB steganography and Rivest-Shamir-Adleman (RSA) cryptology. if we compared with the traditional LSB the PSNR value of that method is more than 3dB, which is greatly improved.

N. Akhtar, S. Khan, P. Johri were introduced two different LSB methods based on bit inversion were proposed [10]. In the study, 6 different messages were embedded in 3 different images. As a result, the experiments carried out, the PSNR value was improved by 5.92% in first proposed method, by 15.8% in second proposed method.

A new LSB steganography algorithm [11] based on changing the embedding direction of message bits was proposed. The proposed method has been tested on 10 different images and a 1.32% improvement in PSNR value compared to the classical LSB method has been achieved. Again, a new LSB steganography method [12] was proposed for color images. According to this method, 2-2-4 message bits are embedded in the R-G-B channels, respectively. The new method was experimented on two different images and PSNR value were improved by 36.44% and 64.54%, respectively and, 1-2-4 LSB method was applied to embed data in grayscale and color images [13]. The message is encrypted with the RSA algorithm to increase resistance against the attacks. The proposed method was tested on 4 different images and improved PSNR value up to 41.48% was obtained.

In the last, a new steganography method that combines LSB steganography with 8-Neighboring PVD (8nPVD) was proposed in [14]. The new work was tested on 5 different pictures. The obtained method was compared in terms of capacity and PSNR value. The increase in PSNR was 2.38%.

6. The proposed method

This work produce an adaptive steganography image technique by applying XOR operation on (LSB) pixels, in our method takes advantage of three different bands and the dependency of a pixel. A 24-bit color image is content three different arrays (red_array, green_array, and blue_array). The Pixel data of Binary Secret Image was hidden on LSB of Blue band, Two Exclusive-OR operation used before saving data to protect data information.

The New method builds on two main processes. The procedure steps state as follows (6.1) First one deals with the hiding data which passes some controls to Matlab GUI for implementation of LSB hiding algorithm, The other process as follows(6.2) returns back the reverse information in the cover RGB color image. We have implemented steganographic routines in Matlab using the GUI toolbox. Table (1) and Table (2) was shows the import of indicator values. The proposed algorithm was implemented in Matlab R2013a (8.1.0.604).

6.1. Embedding algorithm

```
Steps for Binary Image Hiding process:
Start
Input images: Color Image (Img_c) and Binary Image (Img_S)
Output images: Stego Cover Image
Step1: open Color image (Img_c) and the Binary Image (Img_s) to be hided
Step2: Split color image into RGB parts (R part, G part, B part)
Step3: Convert Img_c and Img_s to binary bits form.
Step4: Repeat step5 for all row and column of cover image
Step5: Read each pixel in Img_s and pixel of R part to Img_c
If XOR (LSB of Img_s, LSB of R part of Img_c) =00 or 11 then
 XOR (1, LSB of G part of Img_c) then if LSB of G part=1
Then put 1 in the LSB of B part of Img_c
Else put 0 in the LSB of B part of Img_c
Else
 XOR (LSB of Img_s, LSB of R part of Img_c) =01 or 10 then
 XOR (0, LSB of G part of Img_c) then if LSB of G part=1
Then put 0 in the LSB of B part of Img_c
Else put 1 in the LSB of B part of Img_c
Step6: Save the secret Image (Img_s)
End
```

6.2. Reconstructed algorithm

```
Steps for Binary Image recovery process:
Start
Input_images: Stego color Image (Img_sc)
Output_images: Binary Image (Img_s)
Step1: open color image (Img_sc) and divide to RGB parts
Step2: Split the cover to RGB parts
Step3: Convert Img_sc to binary bits form.
Step4: Repeat step5 for all row and column of Img_sc
Step5: Read each pixel in Img_sc
If XOR (LSB of B part Img_sc , LSB of G part of Img_sc )=00 or 11 then
If XOR (1, LSB of R part of Img_sc )=00 or11
Then put 1 in the LSB of Img_s
Else
XOR (LSB of B part Img_sc , LSB of G part of Img_sc )=01 or 10 then
If XOR (0, LSB of R part of Img_sc )=01 or 0
Then put 0 in the LSB of Img_s
Step6: Display Secret Image (Img_s)
End
```

7. Experimental results

The experimental results of the project method show the following sections:

Three Images used to test the proposed method;

These images have different size including “Lena”, “Penguins”, and “Tulips”. We use two checkers were PSNR and MSE, this measure percentage of pixels that will be change when the projected method appalled on this tests images. Three different Binary Image size says 16.9KB, 24.0KB and 28.1KB.

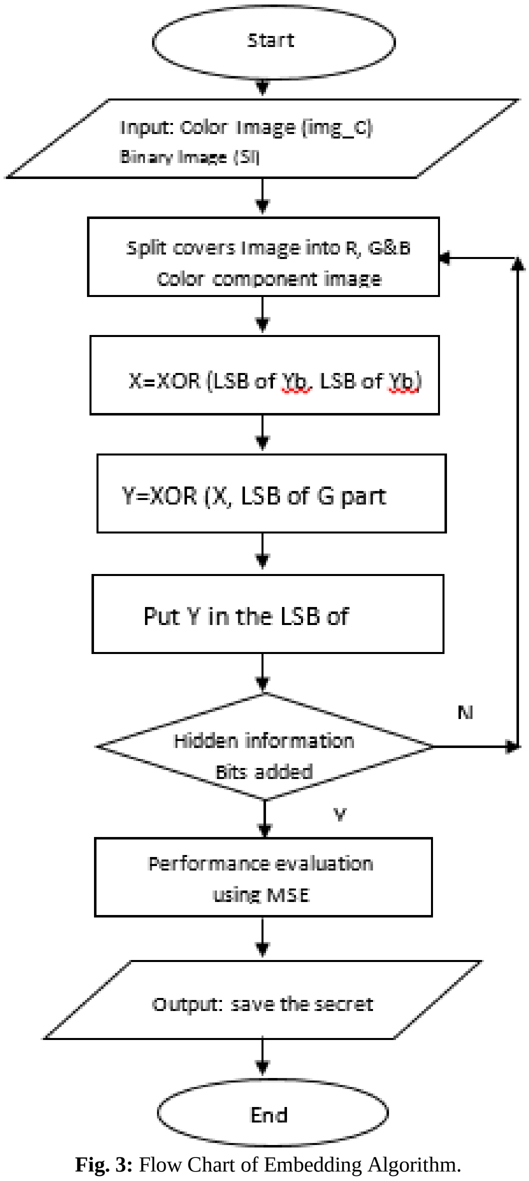


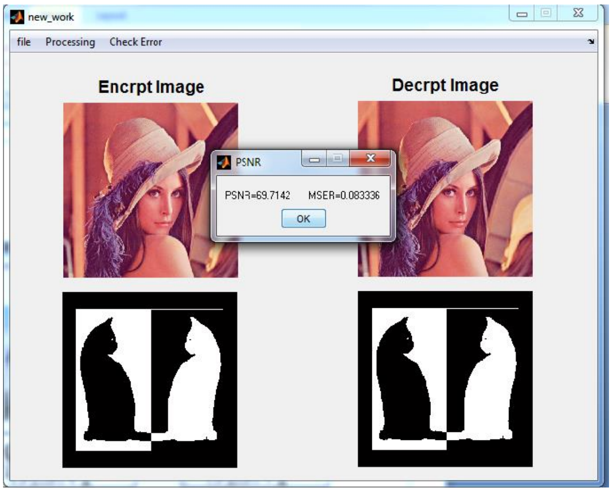
Fig. 3: Flow Chart of Embedding Algorithm.

Table 1: Size of Cover Color Image and the Secrete Binary Image of Three Experiments

Cover Image	Dimensions of Cover Image	Size of Cover Image	Dimensions of Secrete Binary Image	Size of Secrete Binary Image
Lena	512x512	463KB	400x333	16.9KB
Penguins	1024x768	759KB	540x362	24.0KB
Tulips	1024x768	606KB	640x360	28.1KB

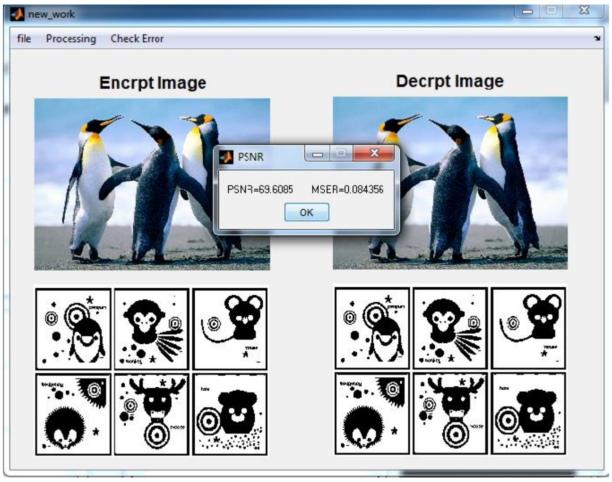
Table 2: Value of (PSNR, MSE) Using RGB Channel for Different Color Images (for Bit per Pixel=8/3)

Cover image	PSNR	MSE
Lena	69.7142	0.0833
Penguins	69.6085	0.0844
Tulips	71.4183	0.0685



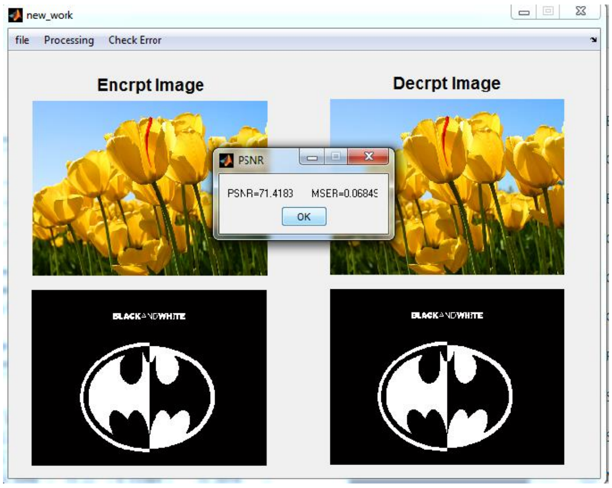
PSNR=69.7142 MSER=0.083336

Fig. 4: 'Lena' Covers Images and the Binary Image of Experiment 1.



PSNR=69.6085 MSER=0.084356

Fig. 5: 'Penguins ' Cover Images and the Binary Image of Experiment 2.



PSNR=71.4183 MSER=0.06849

Fig. 6: 'Tulips ' Cover Images and the Binary Image of Experiment 3.

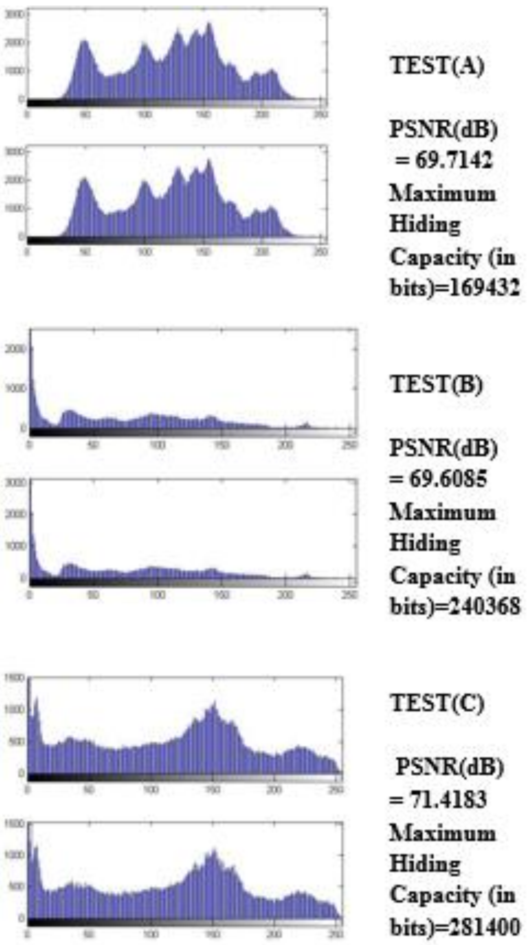


Fig. 7: The First Histogram to Original Image and the Histogram to Embedded Image.

PSNR gives the match between two images. Therefore, the PSNR must be high for a good method [16-22]:

$$PSNR = 10\,log_{10}\left[\frac{R^2}{MSE}\right] \qquad (1)$$

Where:
R: is the maximum value range that a pixel can take, for 8-bit images: R=255
MSE error calculated using the equation given:

$$MSE = \frac{1}{nxm}\sum_{k=1}^{n}\sum_{I=1}^{m}\left(img_{kI} - img_{sc_{kI}}\right)^2 \qquad (2)$$

Where:
N: is row size of the image.
M: is column size of the image.
img_{kI} : is cover image
$img_{sc_{kI}}$: is stego image.
If MSR is low value that will means the quality of image was good.

8. Conclusion

In this paper, the performance of the algorithm in terms of ("MSE", "PSNR") is show the experimental results tables and show that the projected structure is an effective way to integrate hidden information treatment and it is very not easy for illegal users to recognize the changes in stego image. Because the data that the save in LSB was not the original data pixel, we replaced the result of encrypted data pixel tat performed two Exclusive-OR. This technique process gives a way to more information saved by an illegal user. In addition, this process provides a novel size for image steganography.

Our experimental results was shown that the proposed method provides an efficient way for embedding large data into cover images without making visible distortions. Moreover, the proposed methods were more security.

References

[1] Z. Ahmed, H. Mohammed, "Secure Watermark Image Steganography by Pixel Indicator Based on Randomization", Vol. 4, No. 2, 2012, Journal OF Madent Alelem College.

[2] Ö. ÇATALTAŞ, K. TÜTÜNCÜ," Improvement of LSB Based Image Steganography ", Proceedings of Research World International Conference, Rome, Italy, 20th-21st July 2017.

[3] K. Joshi, P. Dhankhar, R. Yadav," A New Image Steganography Method in Spatial Domain Using XOR", 978-1-4s673-6540-6/15, 2015 IEEE.

[4] K. Joshi, R. Yadav, "New Approach toward Data Hiding Using XOR for Image Steganography", 978-1-5090-3251-8/16, 2016 IEEE.

[5] K. Farhan Rafat, M. Junaid Hussain, "Secure Steganography for Digital Images Meandering in the Dark", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, 2016.

[6] M. Abdur Razzaq, M. Adnan Baig, R. Ahmed Shaikh, A. Ahmed Memon, "Digital Image Security: Fusion of Encryption, Steganography and Watermarking ", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 5, 2017.

[7] K. Joshi, R. Yadav , G. Chawla, "An Enhanced Method for Data Hiding using 2-Bit XOR in Image Steganography", Kamal deep Joshi et al. / International Journal of Engineering and Technology (IJET), Vol. 8, No. 6 ,Dec 2016-Jan 2017.

[8] P. Jain, N. Kanwal, " Image Steganography in RGB Color Components using Improved LSB Technique Image Pattern Compression using Weighted Principal Components Algorithm ", Indian Journal of Science and Technology, 9(45), PP(1-4),2016.

[9] X. Zhou, W. Gong, W. Fu, L. Jin, “An Improved Method for LSB Based Color Image steganography Combined with Cryptography”, Okayama, Japan, IEEE, ICIS 2016, June 26-29, 2016.

[10] N. Akhtar, S. Khan, P. Johri, “An Improved Inverted LSB Image Steganography”, International Conference on Issues and Challenges in Intelligent Computing Techniques, IEEE (ICICT), 2014.

[11] S. Sugathan, “An Improved LSB Embedding Technique for Image Steganography”, second International Conference on Applied and Theoretical Computing and Communication Technology, IEEE (iCATccT), 2016. https://doi.org/10.1109/ICATCCT.2016.7912072.

[12] A. Singh, H. Singh, “An Improved LSB based Image Steganography Technique for RGB Images”, International Conference on Electrical, Computer and Communication Technologies, IEEE (ICECCT), 2015.

[13] S. Goyal, M. Ramaiya, D. Dubey, “Improved Detection of 1-2-4 LSB Steganography and RSA Cryptography in Color and Grayscale Images”, International Conference on Computational Intelligence and Communication Networks, IEEE, 2015. https://doi.org/10.1109/CICN.2015.220.

[14] M. Kalita, T. Tuithung, “A Novel Steganographic Method Using 8-Neighboring PVD (8nPVD) and LSB Substitution”, The 23rd International Conference on Systems, Signals and Image Processing, Slovakia, IEEE, 23-25 May 2016.

[15] Chan C-K and L-M Chng, "Hiding data in image by simple LSB substitution" pattern recognition, International Journal of Security and Its Applications, Page (469-474), Vol. 37, No. 3, 2004.

[16] Juneja M. and Sandhu P. S., “An improved LSB based steganography technique for RGB color images,” International Journal of Computer and Communication Engineering, Vol. 2, No. 4, 2013.

[17] Kaur M, Gupta S., Sandhu P. S. and Kaur J., “A dynamic RGB intensity based steganography scheme,” World Academy of Science, Engineering and Technology, vol. 67, pp. 833-838, 2010.

[18] Emad T. Khalaf, N. Sulaiman,”Segmenting and hiding data randomly based on index channel,” International Journal of Computer Science Issues, Vol. 8, No. 1, issue 3, May 2011.

[19] Anupam K. Bairagi, Saikat Mondal and R. Debnath, "A robust RGB channel based image steganography technique using a secret key," Proceedings of the 16th International Conference on Computer and Information Technology, pp. 81-87, Khulna, Bangladesh, 2014.

[20] N. Jain, S. Meshram, S. Dubey,” Image Steganography Using LSB and Edge – Detection Technique”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Vol.2, No.3, July 2012.

[21] K. Vyas, B.L.Pal “A Proposed Method In Image Steganography To Improve Image Quality With LSB Technique” International Journal of Advanced Research in Computer and Communication Engineering Vol.3, No.1, 2014.

[22] R. Chandekar, “Data Hiding for Binary Image by Connectivity-Preserving”, International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), ISSN 2249-6831, Vol.3, 105-112, 2013.