A High Capacity Highly Imperceptible Secret Information Hiding Approach for Colored Images

Simranjot Kaur[1] Jasdeep Singh[2] Sandeep Singh[3]
[1,2,3]Department of ECE Engineering
[1,2,3]BMSCE Sri Muktsar Sahib, and Sri Muktsar Sahib India

Abstract— Stenography is the branch of information security that hides the important and crucial information into an innocent media in such a way that no one except recipient can extract the information. The major goal of the is to enhance communication security by inserting secret message into the digital image, modifying the nonessential pixel of the image. The main objective of this research is to secure the data so that human eye cannot detect the data hidden inside the image. The data embedding and extraction algorithm will be designed so that large information can be hidden in image and the quality of the Stego image will be good. A steganography technique is proposed of data hiding using the concept of 2 bit identical matching technique and OPAP technique. To make the stego image imperceptible use the concept of hiding data on edges as on edges there is sharp change in color intensity and human eye will be unable to detect any hidden data. To use optimal pixel adjustment process for edge pixels to decrease the mean square error and to increase the peak signal to noise ratio and hence to make the stego image more imperceptible. And then use 2 bit identical match technique for non edge pixels. Then hide data in every layer of image to increase the capacity. The parameters PSNR, MSE, BER are measured and compared to the results with literature.

Key words: Data hiding, stego Image,OPAP,2-bit Identical Technique

I. Introduction

Steganography is the method for secret communication. The word "Steganography" derives from Greek and it means "cover writing". Secret information can be hiding in one of two ways, cryptography and steganography. The methods of cryptography attract the attention of attacker, whereas the methods of steganography hide the existence of information. From the methods of steganography, the most common method is to use images to hide the data. That is called image steganography. Stegnography is the technique that involves hiding a message in an suitable carrier e.g.,an image,an audio or video file.The carrier than send to a receiver without anyone else knowing that contain a hidden message[2]. Stenography is the branch of information security that hides the important and crucial information into an innocent media in such a way that no one except recipient can extract the information[4].The major goal of the is to enhance communication security by inserting secret message into the digital image,modifying the nonessential pixel of the image[6].

The image steganography embedding process can be understood from Figure 1.1 given below.

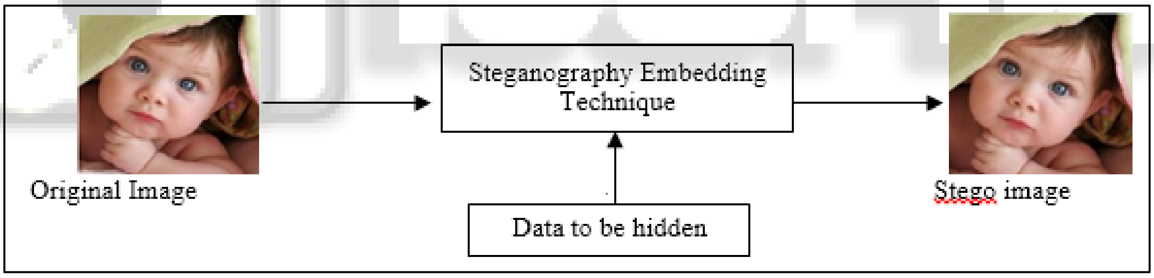


Fig. 1.1:- Block diagram of a simple Image Steganography Embedding Process

The image steganography extraction process can be understood from Figure 1.2 given ahead.

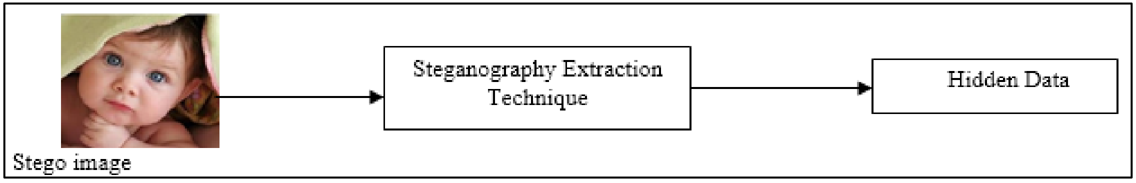


Fig. 1.2:- Block diagram of Steganography Extraction from a Stego image

In this method, the pixels of the images are altered to hide the secret data so as invisible to the others and the changes applied in the image are not tangible. The image used to encode the secret data is called the cover image while the cover image with the secret data encoded in it is called the stego image. Images are the most popular cover files used for steganography. There are two types of compression: lossy and lossless. Both methods save storage space, but the procedures are different. Lossy compression creates smaller files by discarding excess image data from the original image. It deletes details that are too small for the human eye to differentiate. As a result, close approximations of the original image are made, but not an exact duplicate. An example of an image format that uses this compression technique is Joint Photographic Experts Group (JPEG), whereas lossless method hides messages in more significant areas of the cover image, making it more robust. So the lossless image formats are most suitable for image steganography. Image files fulfill this requirement of redundancy so they are very commonly used as a medium for steganography. Audio files contain redundant information but not used as widely as image files. There are two techniques proposed to use images as cover objects. These techniques can be categorized in the following two ways: Spatial domain techniques and Transform domain techniques.

A. Problem Formulation

Till now from 480 BC there are many researches about the steganography but still there is problem of destroying the data by hacker performing the steganalysis by analyzing the quality of the stego image. Researchers gave many techniques but still there is problem of degradation in quality of the image with increase in amount of secret information to be hidden. The major gaps in our literature are quality of stego image, security of the data, and data payload of the system.

B. Research Objectives

The main objective of this dissertation is to secure the data so that human eye cannot detect the data hidden inside the image. Main objectives are to propose a steganography technique of data hiding using the concept of 2 bit identical matching technique and OPAP technique. To make the stego image imperceptible use the concept of hiding data on edges as on edges there is sharp change in color intensity and human eye will be unable to detect any hidden data. To use optimal pixel adjustment process for edge pixels to decrease the mean square error and to increase the peak signal to noise ratio and hence to make the stego image more imperceptible. To use 2 bit identical match technique for non-edge pixels. To hide data in every layer of image to increase the capacity. To measure the parameters PSNR, MSE, BER and compare the results with literature.

II. METHODOLOGY

A. Proposed Work

In the present work, a high capacity highly imperceptible steganography approach for colored images is proposed which hides the message bits at each layer of image using 2-2-2 bit approach of data hiding. The presented algorithm can be applied to the RGB images and does not hide the data to the gray scale images. 2-bit identical method and optimal pixel adjustment process (OPAP) is used to hide the secret information bits. At edge pixels data is hiding using OPAP and at non edge pixels data is hiding using 2 bit identical method. The user of the system is asked to select the original image, and secret data. After having these inputs from the user the secret data entered by the user is hidden into the image selected by the user with the proposed algorithm described in detail in section 2.1.1. The stego image is shared with the receiver party. And the receiver party uses this stego image to extract and access the secret message hidden into this stego image. The secret information is extracted using the proposed algorithm described in detail in section 2.1.3.

1) Hiding of Secret Information

In the proposed algorithm, to conserve the quality of stego image and to make the algorithm more imperceptible 2 techniques of data hiding are used. One of these is 2 bit identical matching technique which is very effective technique to preserve the quality of stego image and secondly optimal pixel adjustment (OPAP) technique is used to hide the data. It is preferred to hide data in the edges using OPAP because by doing so the visual quality of image is affected less as compared to other areas of image. And to make the algorithm high data capacity embedding system, 6 bits of data is hiding at every pixel by spreading 2 bits on each layer of RGB image. The block diagram showing the basic layout of present approach of message hiding is shown in figure 2.2.

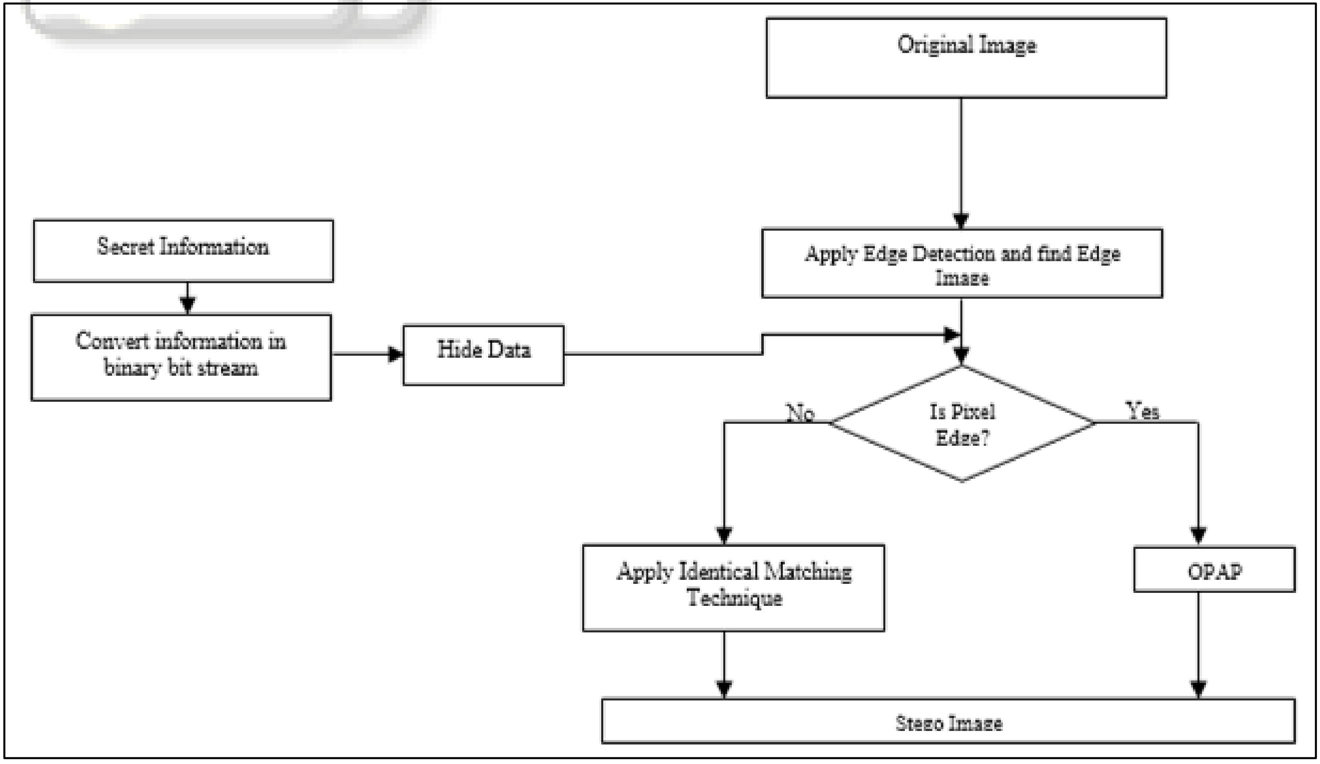

Original Image
Apply Edge Detection and find Edge Image
Secret Information
Convert information in binary bit stream
Hide Data
Is Pixel Edge?
No
Yes
Apply Identical Matching Technique
OPAP
Stego Image

Fig. 2.2: Flow diagram of proposed embedding algorithm

2) *Message Hiding Algorithm Steps*

Input: RGB Image, Secret Information
Output: Stego Image

- Step 1: Read RGB image file.
- Step 2: Get all three red, green, and blue layers of image.
- Step 3: Extract the edge pixels of image from all layers.
- Step 4: Convert the secret information into binary form.
- Step 5: Start hiding data, if pixel is edge hide 2 bits in each layer using OPAP technique and if pixel is non-edge hide 2 bits of data in each layer using 2 bit identical approach. Save the bit positions in each pixel where data bits are hidden.
- Step 6: Combine all layers after hiding full information and get stego image.

3) *Extraction of Secret Information*

In order to retrieve the hidden secret information from the stego image; 2 bits from each layer of every pixel are extracted from the respective bit position and rearranged it.

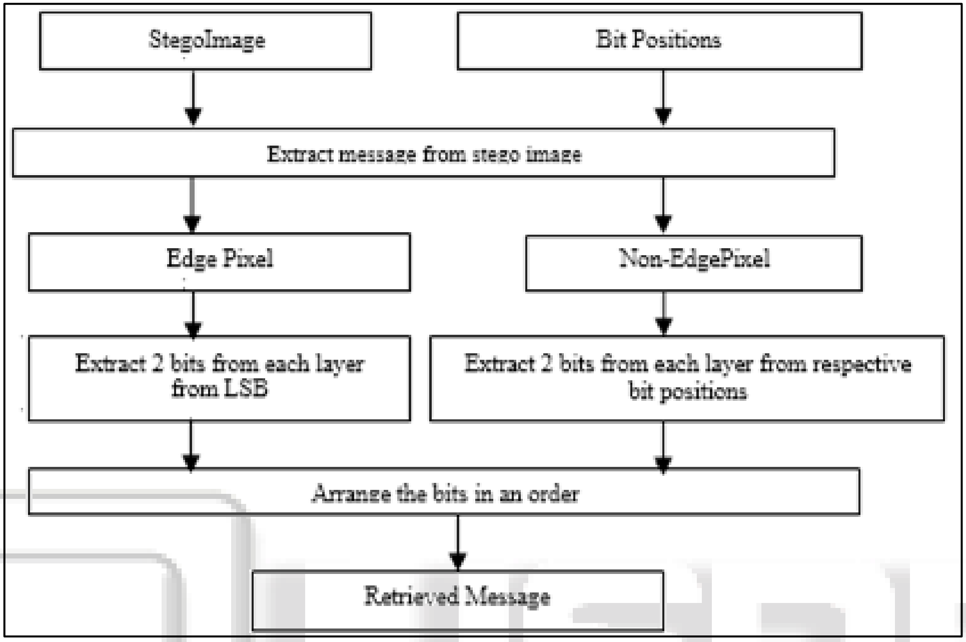

StegoImage
Bit Positions
Extract message from stego image
Edge Pixel
Non-EdgePixel
Extract 2 bits from each layer from LSB
Extract 2 bits from each layer from respective bit positions
Arrange the bits in an order
Retrieved Message

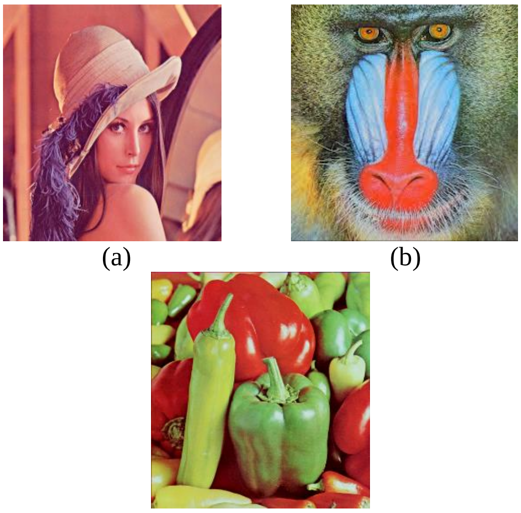
Fig. 2.3 Message Retrieval Process

4) *Message Retrieval Algorithm Steps*

Input: Stego Image, Bit Positions
Output: Secret Message

- Step 1: Read the Stego-image file.
- Step 2: Start retrieving hidden bits.
- Step 3: Extract 2 bits from each layer of every pixel from the respective bit positions.
- Step 4: Rearrange the bits in order
- Step 5: Get secret information

B. *Test Images*


(a) (b)

(c)

Fig. 2.4 Test color images (a) Lena (b) Baboon (c) Peppers

C. *Image Edge Detection*

Basically edge detection is the way of localizing pixel intensity variations. The edge detection techniques have been employed in several areas such as segmentation, item recognition and in tracking etc. Hence, the edge detection is most important part in image processing and there exists several edge detection approaches like (Sobel, Prewitt, Roberts and Canny). These methods have been employed for identifying changes in the images. Hence, the derivative operation based approaches can be characterized in two sets first and second order derivative. The first order derivative method depends on calculating the gradient of directions and merging the result of each gradient. The value of gradient magnitude and orientation is estimated using two differentiation masks. The Canny method applies two thresholds to the gradient: a high threshold for low edge sensitivity and a low threshold for high edge sensitivity. Edge starts with the low sensitivity result and then grows it to include connected edge pixels from the high sensitivity result. This helps fill in gaps in the detected edges. The Canny method finds edges by looking for local maxima of the gradient of Image. The gradient is calculated using the derivative of a Gaussian filter. The method uses two thresholds, to detect strong and weak edges, and includes the weak edges in the output only if they are connected to strong edges. This method is therefore less likely than the others to be fooled by noise, and more likely to detect true weak edges.

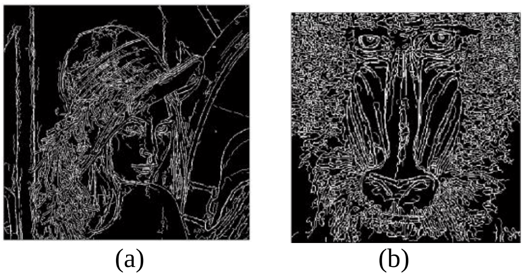


Fig. 2.5: Edge Images of Test images (a) Lena (b) Baboon

III. Results and Discussion

A. Simulation Results for Imperceptibility Analysis

We consider RGB images as cover image and data message to hide in the cover image. The simulations are performed on standard RGB images of size 512 X 512..The quality of the stego images has been evaluated and the results are presented. The size of the confidential message is considered for the experiment is 8 KB and 16 KB. Figures 3.1 to 3.2shows the cover image and corresponding stego image of Lena after hiding a data of 8192 and 16,384 bytes respectively and calculated values of MSE, PSNR and BER are tabulated in table 3.1.

Table 3.1 represents that the PSNR value achieved is 74.0960 for Lena image for message length of 8192 bytes and 70.4213 for the data length of 16,384 Bytes. These PSNR values are higher than the PSNR obtained in [17] and [18]. Because we find the identical values between data bits and pixel bits, so chances of occurrence of error are very less

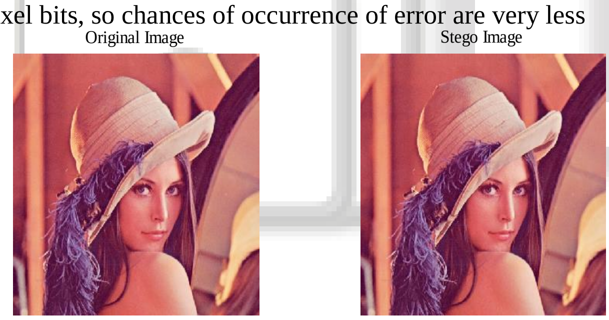


Fig. 3.1: Simulation Results of Lena Image with 8192 Bytes Original Image (b) Stego Image

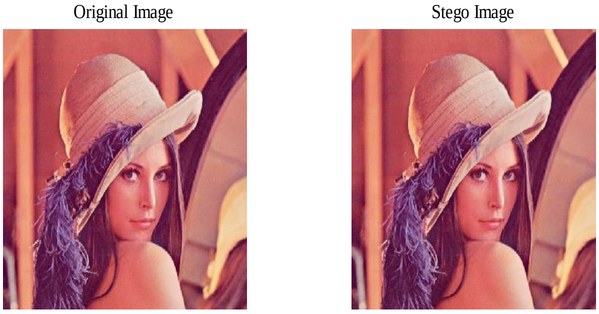


Fig. 3.2: Simulation Results of Lena Image with 16,384 Bytes (a) Original Image (b) Stego Image

Image	Data Length (in KB)	MSE	PSNR	BER
Lena (512 X 512 X 3)	8KB	0.0025	74.0960	0.0135
	16KBs	0.0059	70.4213	0.0142

Table 3.1 :MSE, PSNR, and BER for Lena Image with Different Amount of Data

Figures 3.3 and 3.4 shows the cover images and corresponding stego images of Peppers after hiding a data of 8192 and 16,384 bytes respectively and calculated values of MSE, PSNR and BER are tabulated in table 5.2.

Image	Data Length (in KB)	MSE	PSNR	BER
Peppers (512 X 512 X 3)	8KB	0.0068	69.8106	0.0143
	16KBs	0.0143	66.5892	0.0150

Table 3.2: MSE, PSNR, and BER for Peppers Image with Different Amount of Data

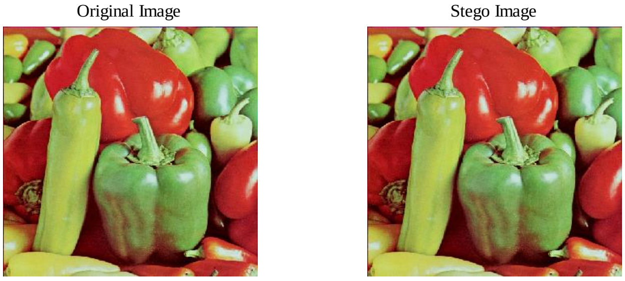


Fig. 3.3 Simulation Results of Peppers Image with 8192 Bytes (a) Original Image (b) Stego Image

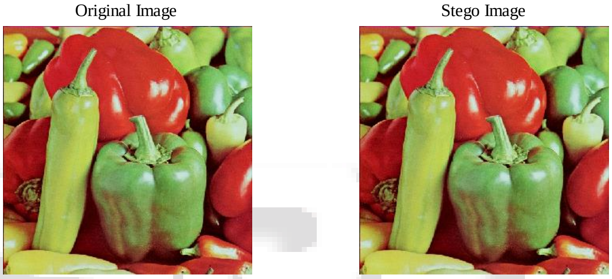


Fig. 3.4 Simulation Results of Peppers Image with 16,384 Bytes (a) Original Image (b) Stego Image

Image	Previous Work [61]		Proposed method	
	Data	PSNR	Data	PSNR
Lena	12,767 Bytes	43.7429	16,384 Bytes	70.4213

Table 3.4 Comparisons between Proposed Work and Previous Work for PSNR

Image	Data Length (in KB)	Previous Work [60]		Proposed method	
		MSE	PSNR	MSE	PSNR
Lena	8 KB	0.0134	66.8678	0.0025	74.0960
	16 KB	0.0321	63.1004	0.0059	70.4213
Pepper	8 KB	0.0325	63.0163	0.0068	69.8106
	16 KB	0.0580	60.4989	0.0143	66.5892
Baboon	8 KB	0.0179	65.6137	0.0100	68.1339
	16 KB	0.0359	62.5739	0.0197	65.1926

Table 3.5 Comparisons between Proposed Work and Previous Work for MSE and PSNR

Also the presented work has high data payload as compared to both of the techniques of literature [17] and [18].

Table 3.5 provides the comparative analysis for the data payload.

IV. Conclusion

In the proposed method, an image steganography technique based on OPAP and 2-bit identical technique is proposed, which results in good visual chracteristics of the stego image. Because we find the identical values between data bits and pixel bits, so chances of occurrence of error are very less.And OPAP is used to hide bits at edge pixels and at edges pixel intemsity is sharply changes due to which data presence at edges cannot be seen easily. Due to these facts the algorithm is robust to attcaks also. And also from the experiments and comparative analysis it has been shown that the proposed algorithm outperforms in terms of perceptiility and data payload. During the course of this work, some potential directions of future research were identified. Firstly, it was observed that most of the steganographic research till date has been towards designing algorithm which generate stego images which are as close to the cover as possible. All the algorithms study the behaviour of the cover image while ignoring the message bit stream. It may be possible to design some encoding functions, which given a cover image and an embedding algorithm can modify the message stream such that it becomes more suitable for embedding than the original bit stream. Secondly, although embedding algorithm is acknowledged by the attacker, the exact message sequence cannot be reconstructed unless the attacker has the knowledge of the encoding function. Furthermore, image quality can be enhanced by increasing number of blocks and data capacity can be increased by using applying some compression technique.

References

[1] Simrat Pal Kaur and Sarbjeet Singh, “A New Image Steganography Based on 2k Correction Method and Canny Edge Detection”, International Journal of Computing & Business Research, ISSN 2229-6166, 2011.

[2] Saurabh Singh, and GauravAgarwal, “Use of image to secure text message with the help of LSB replacement”, International journal of applied engineering research, Vol. 1, 2010.

[3] Nitin Jain, SachinMeshram, and ShikhaDubey, “Image Steganography Using LSB and Edge – Detection Technique”, International Journal of Soft Computing and Engineering (IJSCE), ISSN 2231-2307, Vol. 2, Issue 3, July 2012.

[4] W.J. Chen, C.C. Chang, T.H.N. Le, “High payload steganography mechanism using hybrid edge detector,” Expert Systems with Applications 37, pp.3292–3301, 2010.

[5] Sharma, S. Kumar, “A New Approach to Hide Text in Images Using Steganography”, IJARCSSE, Volume3, Issue 4, ISSN: 2277 128X, April 2013.

[6] Ross J. Anderson, Fabien A.P. Petitcolas, “On the Limits of Steganography”, IEEE Journal of Selected Areas in Communications, 16 (4):474-481, ISSN 0733-8716, May 1998.

[7] S.F. Mare, M. Vladutiu, L. Prodan, “Decreasing change impact using smart LSB pixel mapping and data rearrangement”, IEEE, 2011.

[8] Tanana Morkel, "Image Steganography Applications for Secure Communication", Universities van Pretoria, May 2012.

[9] N. Provos, P. Honeyman, “Hide and seek: an introduction to steganography”, IEEE Security and Privacy Magazine 1, 2003.

[10] Wen-Jan Chen, Chin-Chen Chang, T-Hoang Ngan Le, “High payload steganography mechanism using hybrid edge detector”, Expert Systems with Applications, Elsevier, ISSN 3292–3301, 2010.

[11] RonakDoshi, Pratik Jain, Lalit Gupta," Steganography and Its Applications in Security ", International Journal of Modern Engineering Research, ISSN 2249-6645, Vol.2, Issue 6, 2012.

[12] ShashikalaChannalli, Ajay Jadhav,"Steganography: An Art of Hiding Data," International Journal on Computer Science and Engineering, Vol. 1, Issue 3, pp. 137-141, 2009.

[13] Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, 2012.

[14] N. F. Johnson, and S. Jajodia, “Steganography: Seeing the Unseen”, IEEE Computer Society, pp. 26-34, Feb. 1998.

[15] Niles Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Computer Society, 2003.

[16] Khan Muhammad, Jamil Ahmad, Haleem Farman, Zahoor Jan, Muhammad Sajjad and Sung WookBaik, “A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption”, KSII Transactions on internet and information systems, vol. 9, no. 5, May 2015.

[17] SwarnjeetKaur and NavdeepGoel, “Segmentation and Block Based ImageSteganography using Optimal Pixel Adjustment Process and Identical Approach”, IEEE International conference on Recent Advances in Engineering & Computational Science (RAECS) December 2015

[18] DilpreetKaur, Harsh Kumar Verma, and Ravindra Kumar Singh, “A Hybrid Approach of Image Steganography” IEEE International conference on Computing, Communication, and Automation (ICCCA), 2016.