ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 1, January 2016

# IMPLEMENTATION OF STEAGNOGRPHY IN TRUE COLOR IMAGE USING RANDOMIZATION TECHNIQUE

**Prateek Mishra**
Research Scholar
Jayoti VidhyaPeeth
Women's University, Jaipur

**Dr.Shachi Awasthi**
Faculty of engineering and
technology, jayoti vidhyapeeth
Women's University Jaipur

***Abstract:***Recently,many new algorithms have been proposed in the fields of steganography and visual cryptography with the aim of improving efficiency ,security, reliability, enhance data hiding capacity. Steganography detection is a technique to tell whether there are secret messages hidden in images. The performance of a steganalysis system is mainly obtained by the method of feature extraction and the architecture selection of the classifier. In this paper, we present a new method of data hiding and extract data from a color or a grayscale images. Because the human eye can recognize the hidden information in the image after using this detection. The experimental results show that the proposed method provides a better performance on testing images in comparison with the existing method in attacking Steghide.

**INTRODUCTION:**

Many efforts have been reported in literature for developinga data hiding technique. An early work on the image steganography is Least Significant Bit technique (LSB).These techniques are simple in both the embedding and de embedding(extracting messages) processes, but can be detected [1] [2]. Swanson [3] propose easiest way of hiding image into other image by changing LSB of host image.Data can be hidden in the text, by shifting words horizontally and by changing distance between words [4].Shirali [5] proposed another text based steganography by changing word spelling. Snehal[6] discuss effect of hiding data in various bits in image , this paper explains the LSB embedding technique and presents the evaluation results for 2, 4, 6 least significant bits. Park [7], has proposed an image Steganography method which is used to verify the secret information that is embedded in a spatial domain of the Cover image had been deleted, forged or changed by attackers. Abbas[8] uses multiple security by combining encryption with image steganograpy. Hsiang[9] propose concept for data hiding and security in black and white
image this paper uses a secret key and a weight matrix are to protect the hidden data. Another approach was proposed in [10] based on image histogram characteristics, zero and peak points are identified and manipulated to embed data in palette images. Gutub[11] presents a concept of storing variable number of bits in each channel (R, G or B) of pixel based on the actual color values of that pixel. Lower color component stores higher number of bits. Spiral-based Least Significant Bit (LSB) approach for hiding messages in images is presented in [12]. Ayed[13] propose more randomized approach to increase the security of the system and also capacity. Jamzad[14] propose block based steganographic technique to hide image in another cover image .As seen in various references [15], [16], [17], [18], [19] there are several different algorithms and methods to hide data in cover media.

**PROBLEM DEFINITION:**

True color image (24 bit depth) is represented by MxNx3array. Each pixel of the true color image contains three color channels i.e. R (red), G (green) and B (blue) each of the 8 bit. Proposed technique hides data in the image by selection of channel in the selected pixel of 24 bit image. In the selected pixel one of the three channels is used as indicator channel. Indicator Channel is selected randomly depends on the random number. Following Table shows the relation between random number and selected channel.

Table : Random number and indicator channel

| Random number | Indicator Channel |
|---|---|
| 0 | Pixel will not be selected |
| 1 | Red channel will act as indicator |
| 2 | Green channel will act as |
| 3 | Blue channel will act as indicator |

According to Table 1 if random key is 0 then corresponding pixel will not be involve in data hiding .If random key is 1 (one) then red channel of the selected pixel act as indicator channel. If random key is 2 (two) then green channel of the selected pixel act as indicator channel. If random key is 3 (three) then blue channel of the selected pixel act as indicator channel. There is no any clue to decide next indicator channel in sequence. If red of the pixel act as indicator two other Green and Blue channel hides data. If green channel selected as indicator channel then two other red and blue hide data. If blue channel is selected as indicator channel then red and green channel hide data. Following Table shows the relation between selected indicator channel and corresponding data channel that will contain data.

TableI: Indicator channel and corresponding data channel

| Selected indicator Channel | First data channel | Second data channel |
|---|---|---|
| Red | Green | Blue |
| Green | Red | Blue |
| Blue | Red | Green |

Value of the two least significant bit of the indicator channel decides data stored on other two channels. Following Table shows the relation between value of indicator bit and hidden data in the two other channels. If indicator bit are 01 second data channel hide 2/3/4 bit data, if it is 10 first data channel hide 2/3/4 bit of data, and if it is 11 both channel hide 2/3/4 bit each. We have consider only 01, 10 and 11 two the LSB's of the indicator channel.

TableII : Indicator channel and corresponding data

| Indicator channel(value of 2 LSBs ) | First data channel | Second data channel |
|---|---|---|
| 01 | No data | Hide 2/3/4 bit |
| 10 | Hide 2/3/4 bit | No data |
| 11 | Hide 2/3/4 bit | Hide 2/3/4 bit |

## METHODOLOGY

- Data Hiding & Extraction
- Implementing in MATLAB using Image processing toolbox

## SIMULATION MODEL AND PERFORMANCE METRICS

MATLAB has been accustomed method and judge the proposed system and has been found that made set of libraries in Matlab computer code are creating it easier for creating simulation. The proposed works are going to be evaluated using following metrics:

**Accuracy:** By comparing the text before encryption and data hiding and text after retrieving hidden data and decryption of the same.

**Performance:** It is calculated on the basis of the time taken during the processing of encryption and data hiding in milliseconds. It gives the performance of the system.

## RESULTS & DISCUSSION


Figure 1: Screen Shot Showing GUI for MATLAB Histogram

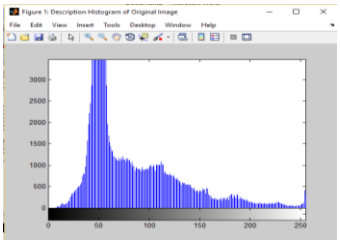

Figure 2: Original Image Histogram

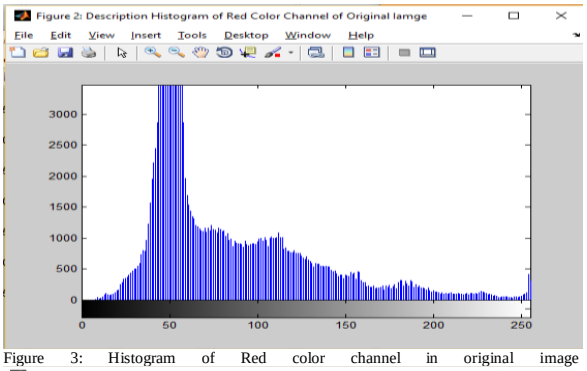


Figure 3: Histogram of Red color channel in original image

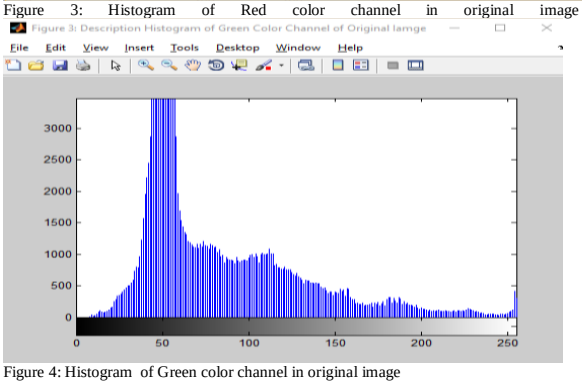


Figure 4: Histogram of Green color channel in original image

ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 1, January 2016

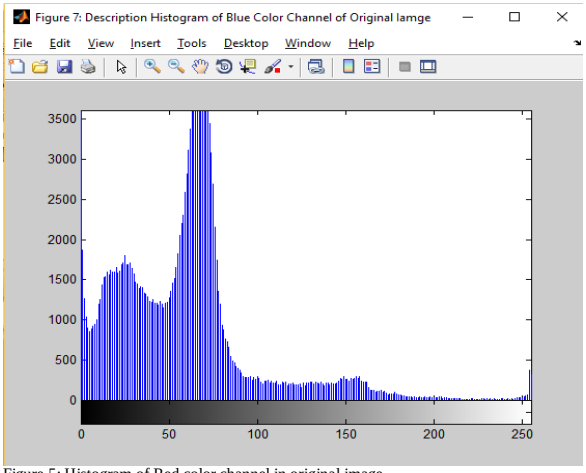


Figure 5: Histogram of Red color channel in original image

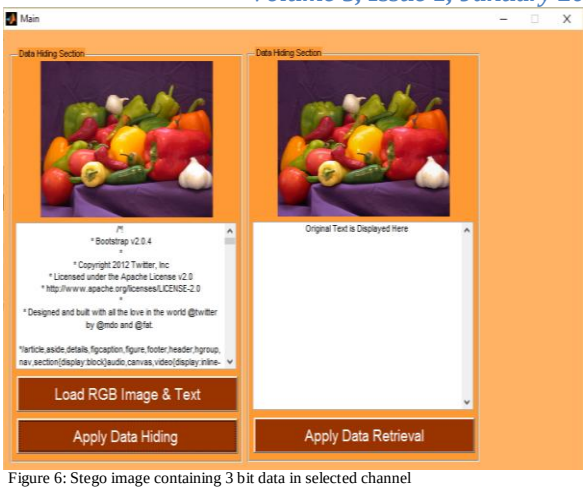


Figure 6: Stego image containing 3 bit data in selected channel

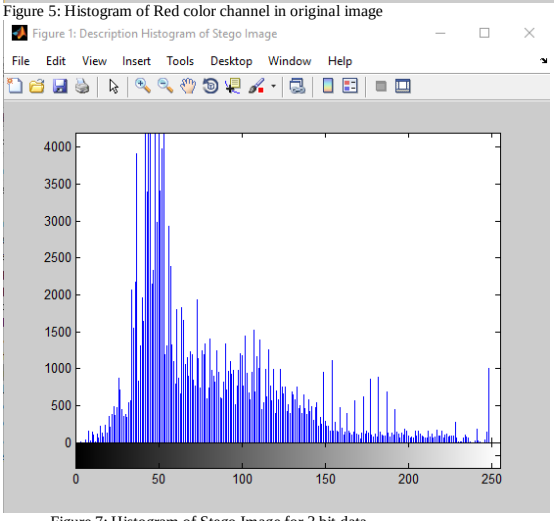


Figure 7: Histogram of Stego Image for 3 bit data

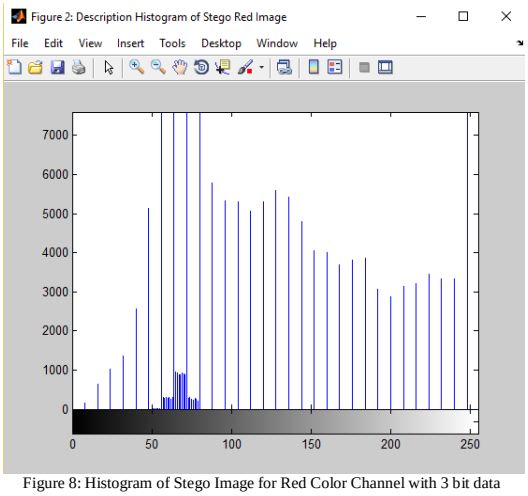


Figure 8: Histogram of Stego Image for Red Color Channel with 3 bit data

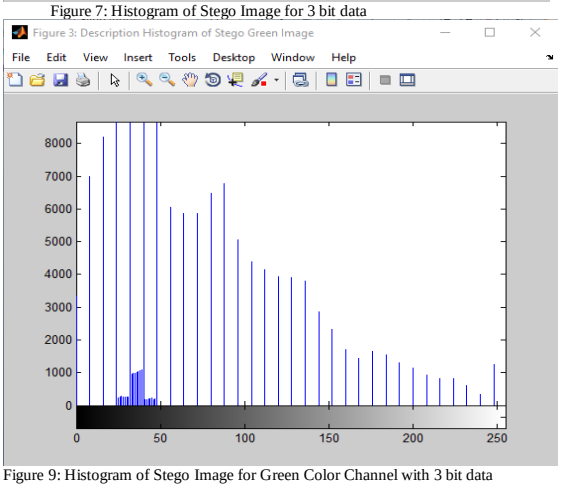


Figure 9: Histogram of Stego Image for Green Color Channel with 3 bit data

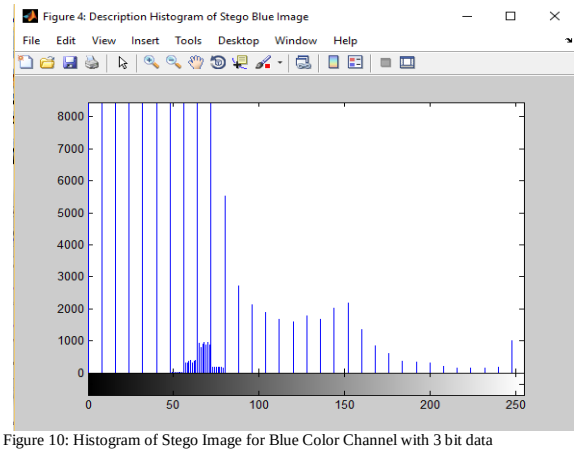


Figure 10: Histogram of Stego Image for Blue Color Channel with 3 bit data

ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 1, January 2016

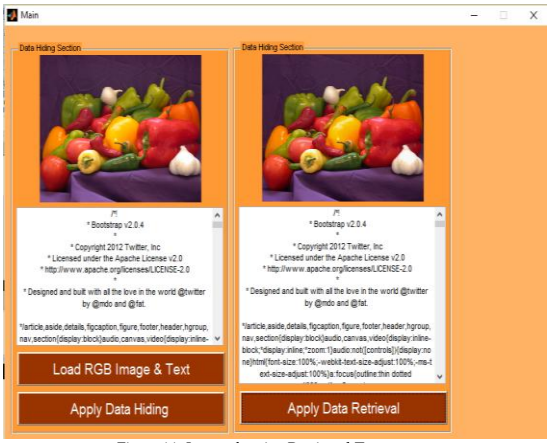


Figure 11: Image showing Retrieved Text

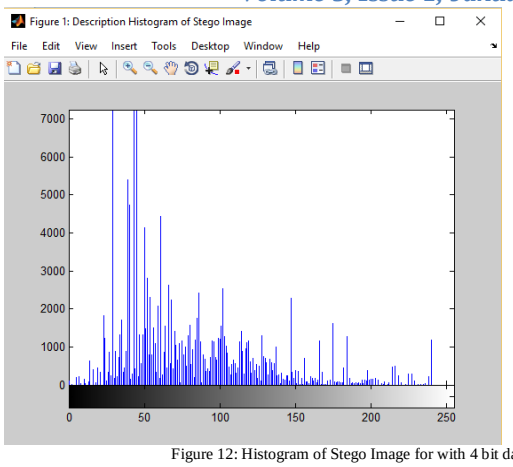


Figure 12: Histogram of Stego Image for with 4 bit data

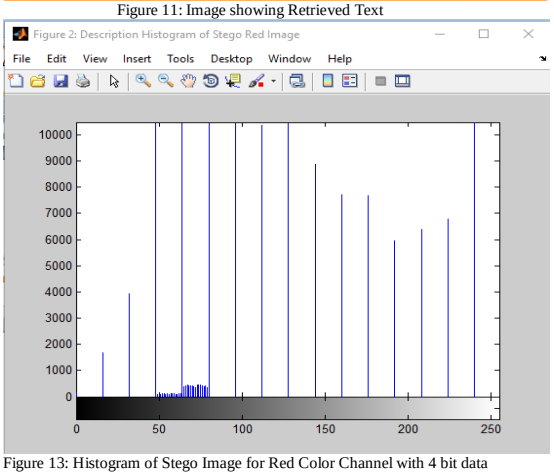


Figure 13: Histogram of Stego Image for Red Color Channel with 4 bit data

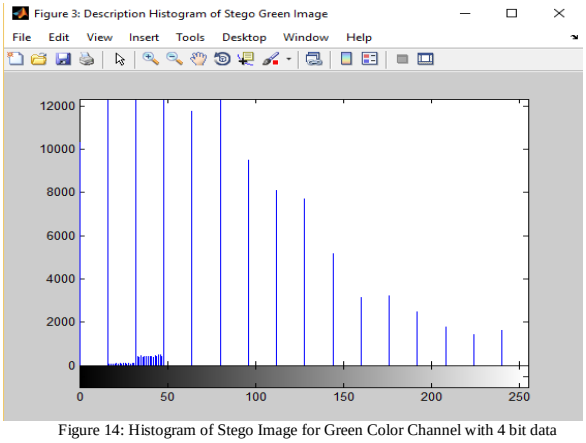


Figure 14: Histogram of Stego Image for Green Color Channel with 4 bit data

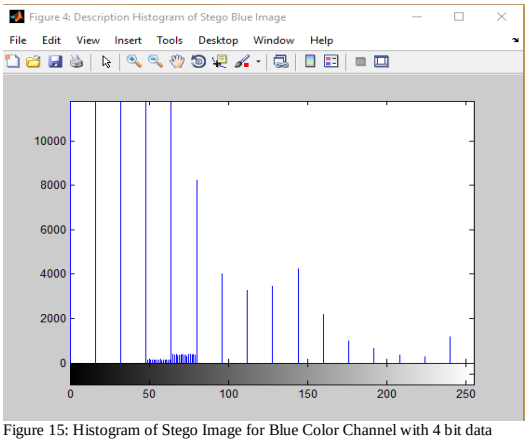


Figure 15: Histogram of Stego Image for Blue Color Channel with 4 bit data

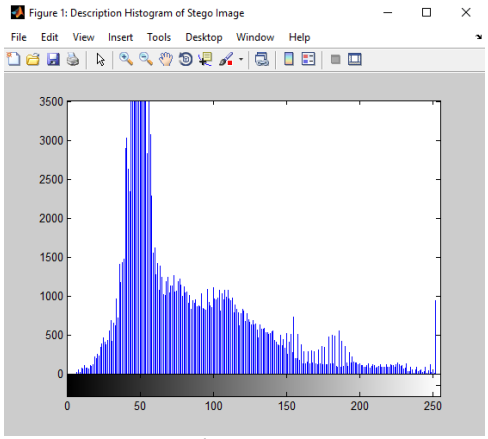


Figure 16: Histogram of Stego Image with 2 bit data

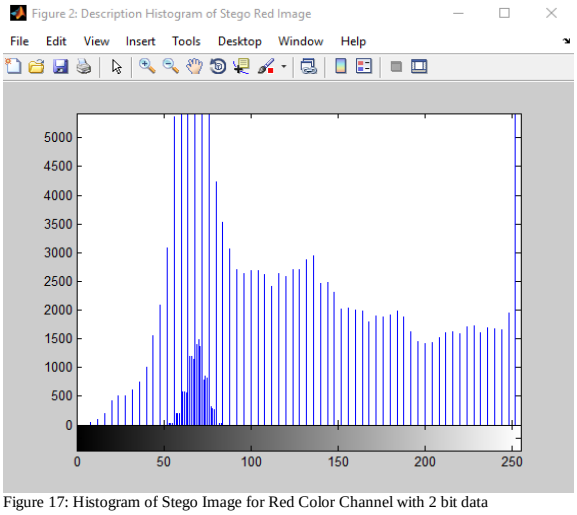


Figure 17: Histogram of Stego Image for Red Color Channel with 2 bit data

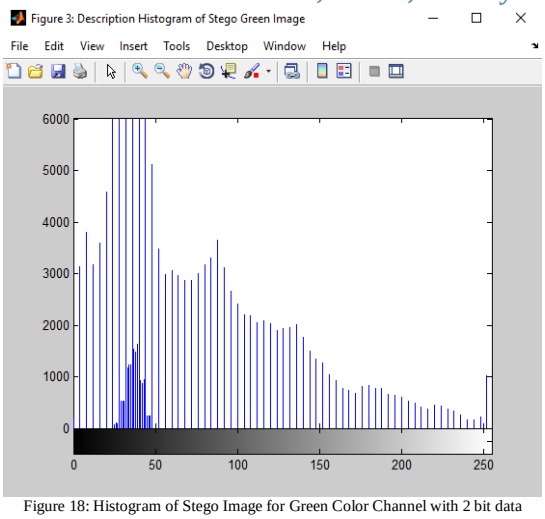


Figure 18: Histogram of Stego Image for Green Color Channel with 2 bit data

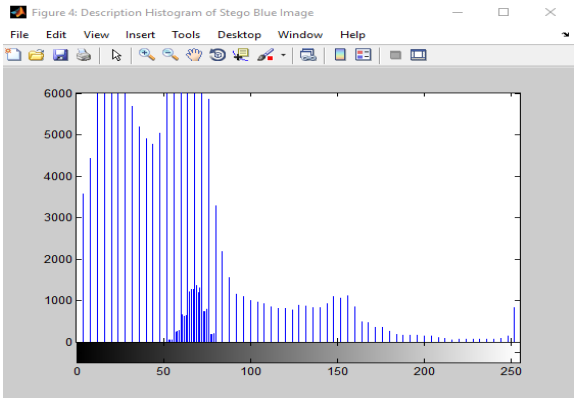


Figure 19: Histogram of Stego Image for Blue Color Channel with 2 bit data

Table III: Maximum data hidden in three different methods

| SNO | Data Size | Compressed Size of Data | Technique Used 2/3/4 bit | Percentage of Pixel Utilized | MSE | PSNR (DB) |
|---|---|---|---|---|---|---|
| 1 | 8 K | 0.6 K | 2 | 0. 45437 % | 0. 92853 | 48. 48686 |
| 2 | 8 K | 0.6 K | 3 | 0. 30292 % | 0. 99046 | 48. 20641 |
| 3 | 8 K | 0.6 K | 4 | 0. 22719 % | 0. 99820 | 48. 17263 |
| 4 | 43 K | 1 K | 2 | 0. 62120 % | 0. 92849 | 48. 48702 |
| 5 | 43 K | 1 K | 3 | 0. 41413 % | 0. 99043 | 48. 20656 |
| 6 | 43 K | 1 K | 4 | 0. 31060 | 0. 99819 | 48. 17268 |
| 7 | 82 K | 13.827 K | 2 | 9.37703% | 0.92476 | 48.50451 |
| 8 | 82 K | 13.827 K | 3 | 6.25136 | 0.98985 | 48.20911 |
| 9 | 82 K | 13.827 K | 4 | 4.68852 | 0.99829 | 48.17224 |

Results from various image and data are taken, above Table 4 shows the various results for the image peppers.png (512X384). Figure is the comparison between original and stego image created during hiding process. Above Figure is the histogram of original image. Figure is the histogram generated during 2-bit data hiding technique, Figure is the histogram generated during 3- bit data hiding technique, Figure is the histogram generated during 4-bit data hiding technique.

## Conclusion

The proposed system has been implemented using the MATLAB tool with the motive of hiding large amount of text in the images using different techniques. The different – different bits have been used with the different size of input text. The different bits are automatically selected depending on the text size and retrieve when the decryption is required to be done. The results obtained from the proposed implementation are also very encouraging and found to be accurate. Alongwith the accuracy of the system is found to be 100%, the performance of the system is also very good and as per the

expectation. The capacity ration is also increased due to compression of the data before hiding in the images. MATLAB is also having good library for support and implementation of the image processing and measurements of the results.

Proposed data hiding technique is introduced as a new method for hiding secret data inside the true color image.The algorithm adds more randomization by using two different selection one for pixel selection and second for channel selection within selected pixel. This randomization adds more security for data. Developed system has following advantages:

(i) Improved hidden data capacity per pixel.
(ii) Automatic decision making of best possible technique tohide data if data size becomes larger.
(iii) Higher security because no one can extract data with help of image and algorithm, without knowledge of secret key.By comparing the histograms of original and stego-Image, it can be concluded that proposed technique is a solution for the acceptable data hiding approach. PSNR (Peak Signal to Noise Ratio) value obtained from the result is acceptable. We can again improve total data capacity to be hidden by using compression of data before hiding. Further it can be extended to incorporate other text and image file formats.

## Future Work

The system can be further tested on the real time environment for accuracy, performance and capacity ratio in future. The system can further be improved and tested for the security of the hidden text by adding different encryption and compression of the techniques. The other steganography techniques can also be applied in future alongwith the proposed technique to test the improvements over the current work.

## REFERENCES:

[1] Fridrich, J. Long, "Steganalysis of LSB encoding in colorimages", IEEE 2000.
[2] N. F. Johnson, Sushil Jajodia,"Exploring Steganography:Seeing the Unseen", Computer vol. 31, no. 2, 1998.
[3] D. Swanson, B. Zhu and A. H. Tewfik, Robust Data Hiding for Images", MIEEE Digital Signal Processing Workshop, September 1996.
[4] Y.Kim , K.Moon and I.Oh , "A Text Watermarking algoprithm based on word Classification and Inter word Space Statitistis,
Procceding of the Seventh international Conference on Document Analysis and Recognition (ICDAR, 03),2003.
[5] M.Hassan Shirali Shareza,Mohammad Shirali Shahreza, "A New Synonym Text Steganography", IEEE 2008.
[6] Neeta Deshpande, Kamalapur Snehal, "Implementation of LSB Steganography and Its Evaluation for Various Bits", IEEE 2006.
[7] K. Y. Youngran Park, Hyunho Kang and K. Kobayashi, "Integrity verification of secret information in image steganography", The 20th Symposium on Information Theory and its Application Nov 2006.
[8] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt "Securing Info rmation Content using New Encryption Method and Steganography", IEEE 2008.
[9] Hsiang-Kuang Pan, Yu-Yuan Chen, and Yu-Chee Tseng, "A Secure Data Hiding Scheme for Two-Color Images", IEEE 2000.
[10] Noura A. Saleh, Hoda N. Boghdady, Samir I. Shaheen2 and Ahmed M. Darwish , "An Efficient Lossless Data Hiding Technique for Palette-Based Images with Capacity Optimization",IEEE 2008.
[11] Mohammad Tanvir Parvez and Adnan Abdul-Aziz Gutub ,"RGB Intensity Based Variable-Bits Image Steganography", IEEE 2008.
[12] Hassan Mathkour , Ghazy M.R. Assassa ,Abdulaziz Al Muharib, Ibrahim Kiady, "A Novel Approach for Hiding Messages in Images", IEEE 2009.
[13] Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabak, "Triple-A: Secure RGB Image Steganography Based on Randomization", IEEE 2009.
[14] Z.kermani ,M.Jamzad , "A Robust Steganography Algorithm Based On Texture Similarity Using Gabor Filter", IEEE Int.Symp on signal processing and Info .Technology , IEEE 2005.
[15] Hedies Sajedi,Mansour Jamzad,"Cover Selection Steganography Method Based on Similarity of Image Blocks", IEEE 8th International conference on Computer and Information Technology Workshops ,IEEE2008.
[16] Hassan Mathkour, Batool Al-Sadoon, Ameur Touir, "A New Image Steganography Technique", IEEE 2008.
[17] Se-Min Kim, Ziqiang Cheng, Kee-Young Yoo, "A New Steganography Scheme based on an Index-color Image", 2009 Sixth International Conference on Information Technology: New Generations ,IEEE 2009.
[18] Omer KURTULDU, Nafiz ARICA, "A New Steganography Method Using Image Layers", IEEE 2008.
[19] Mohammad Shiralii-Shahrreza "Text Steganography by changing word spelling"