# ADAPTIVE DATA HIDING APPROACH FOR TRUE COLOR IMAGE USING RANDOMIZATION TECHNIQUE

**Prateek Mishra**
Research Scholar
Jayoti VidhyaPeeth
Women's University
Jaipur
rajeev441220@yahoo.com

Rajeev Shrivastava
Research Scholar
Jayoti VidhyaPeeth
Women's University
Jaipur
rajeev441220@rediffmail.com

**Dr.Rajkumar**
Faculty of Engg.& Tech.
Jayoti VidhyaPeeth
Women'sUniversity
ankita270481@yahoo.co.in

***Abstract*— In today's scenario of internet world, hiding data with security is the highly challenging and desirable task. There are large numbers of techniques available which are capable of hiding data in cover media. The purpose of this research work is to develop a novel, secure and high capacity data hiding technique in 24 bit true color image. This novel approach uses pixels of 24 bit true color image to hide secret message. The proposed approach is adaptive and according to size of data it decides best possible technique to hide data in true color image. The developed technique applies multiple security mechanisms using randomization and data hiding methods. The major focus in this proposed work is to hide more data with higher security in cover media. In this approach the pixels that are going to contain the data are selected randomly based on the random key. At the receiving end it is difficult to retrieve secret data without secret key. The main advantages of proposed approach are: First it is adaptive, i.e. depending upon the data size, it automatically decides the best technique for hiding. Second it is secure due to randomization in the pixel and channel selection. Third it provides high capacity for hiding data in cover image.**

Keywords- LSB, MSE, PSNR, Steganography.

## I. INTRODUCTION

Many efforts have been reported in literature for developing a 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. Remaining part of the paper are organized as follows: section (II) deals with our proposed algorithm ,section(III) deals with implementation and result, Finally section (IV) gives conclusion and future work .

## II. PROPOSED ALGORITHM

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 1 shows the relation between random number and selected channel.

Table 1: 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 indicator |
| 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 2 shows the relation between selected indicator channel and corresponding data channel that will contain data.

Table2: 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 3 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.

Table 3: 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 |

**Algorithm:**
Algorithm consists of the two processes
(i) Insertion process
(ii)Extraction process
**(i)Insertion process:** Insertion process hide data in cover image, to hide data, pixel channel is selected according to the value of randomly generated key. Insertion (Hiding) process consists of the following steps:
**Step 1:** Read RGB image.
**Step 2**: Read Secret data file.
**Step 3:** Generate matrix of random number as long as size of image such that each element is 0/1/2/3, to select pixel and the indicator channel, store this random number as secret key file.
**Step 4:** Generate another random number from 1 to 3 (i.e. 01, 10, and 11 in binary) to decide number of bit to hide in channel and calculate maximum possible data that can be hidden in image do the following:
**(i)** Calculate maximum possible data for 2 -bit technique.
**(ii)** Calculate maximum possible data for 3- bit technique.
**(iii)** Calculate maximum possible data for 4- bit technique.
**Step 5:** Calculate data length and write from 1 to 8$^{th}$ pixel.
**Step 6:** Compare maximum possible data with data length of the secrete message, do the following:
If (data length<=Maximum possible data for 2-bit technique)
Then write 00 in LSB of 9$^{th}$ pixel's red and green channel, hide data using 2 -bit technique
Else
If (data length<=Maximum possible data for 3 bit technique)
Then write 01 in LSB of 9$^{th}$ pixel's red and green channel, hide data using 3 bit technique
Else
If (data length<=Maximum possible data for 4 bit technique)
Then write 10 in LSB of 9$^{th}$ pixel's red and green channel, hide data using 4 bit technique.
**Step 7**: Exit
**(ii)Extraction:** Extraction process extract hidden data from stego image .pixel from which data to be extracted is selected according to the random key which is same as the key used in hiding process. Extraction process involve following steps.
**Step 1:** Read stego image.
**Step 2:** Read random key file.
**Step 3:** Calculate message length from 1$^{st}$ to 8$^{th}$ pixels.
**Step 4:** Read header from red and green channel of 9$^{th}$ pixel and do the following:
If header from 9$^{th}$ pixel is 00
Then extract data using 2 bit technique.
Else
If header from 9$^{th}$ pixel is 01
Then extract data using 3 bit technique.
Else
If header from 9$^{th}$ pixel is 10
Then extract data using 4 bit technique.
**Step 5**. Exit
Technique involve dynamic decision about best approach to hide data in image hence prior to hiding it calculate data size and possible data size which can be hidden in image, according to the estimated data it decides appropriate technique which can be used for data hiding. I have consider three different method to hide data, first one is to hide data 2 bit in each channel depending on the indicator key ,If 2 bit technique is not suitable then three bit data hiding technique is used and if data size is too large then 4 bit data hiding is used. If data size is too large for 4 bit technique then message will be declared that try with another larger image.

Following table 3 shows all three techniques which are used and the channel involve in data hiding.

## III. IMPLEMENTATION AND RESULTS

Proposed technique is implemented in MATLAB R2007a. Two of the error metrics used to compare the host image and stego-image are Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a stego image. The higher PSNR, the better the quality of the image. To compute the PSNR, the block first calculates the mean-squared error using the following equation.

$$MSE = \frac{\sum_{M,N}(H(m,n) - H'(m,n))^2}{M * N} \quad \ldots\ldots\ldots 1$$

$$PSNR = 10 * \log_{10}\left(\frac{255^2}{MSE}\right) \quad \ldots\ldots\ldots 2$$

Where MXN are the size of image
H (m, n) is color intensity of image
H (m, n)'color intensity of stego image
Experiment is performed on different true color image. Following Table 3 shows results of hiding data of different size in peppers.png (512X384) .
Table 4 : Maximum data hidden in three different methods

| S. No. | Data Size (KB) | Technique Used 2/3/4 bit | Percentage of pixel utilized | MSE | PSNR (DB) |
|---|---|---|---|---|---|
| 1 | 9.48 | 2 | 14.8092 | 0.128435 | 57.044 |
| 2 | 20.3 | 2 | 31.7566 | 0.314463 | 53.1551 |
| 3 | 29.5 | 2 | 46.1049 | 0.36459 | 52.5128 |
| 4 | 36.2 | 2 | 56.6467 | 0.602514 | 50.3311 |
| 5 | 51.8 | 3 | 53.9154 | 2.25149 | 44.6061 |
| 6 | 72.2 | 4 | 56.3655 | 5.84583 | 40.4623 |

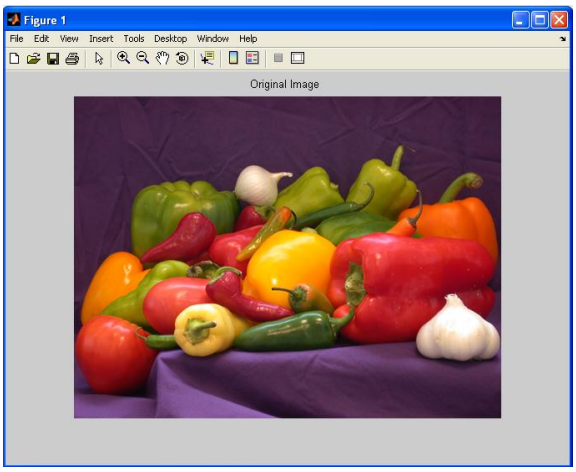



Figure 3(a) Original Image

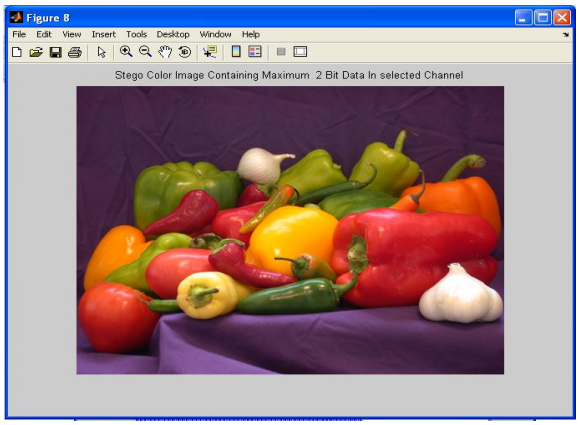



Figure 3(b) stego image containing 2 bit data in selected channel

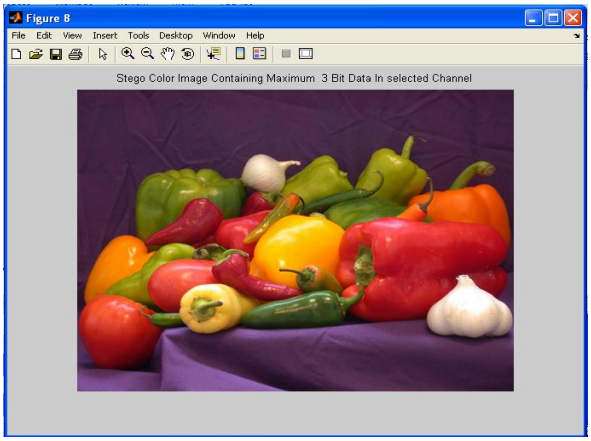



Fig3(c) stego image containing 3 bit data in selected channel

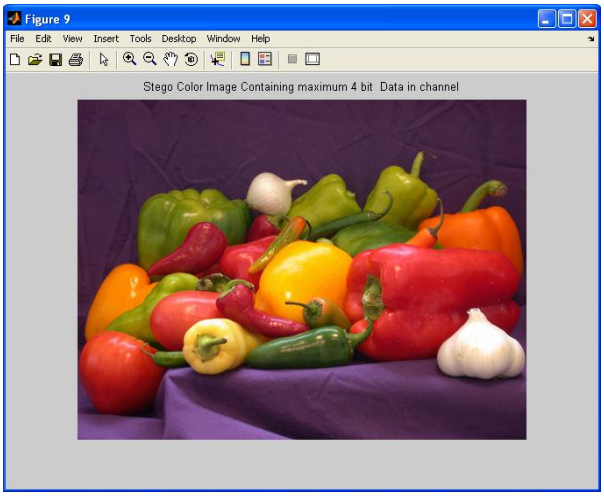
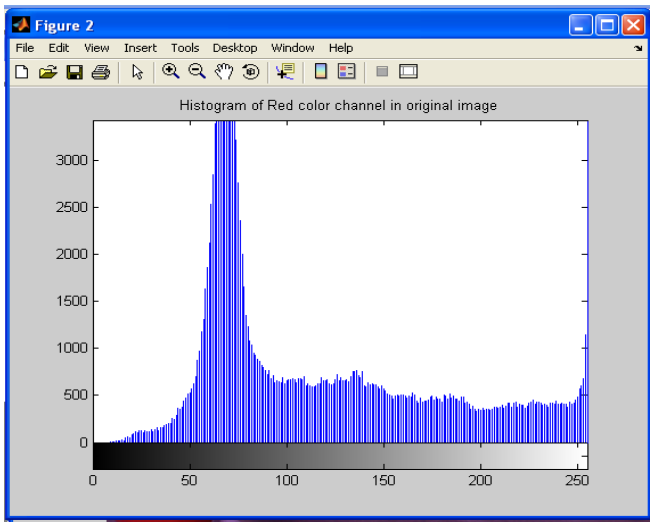
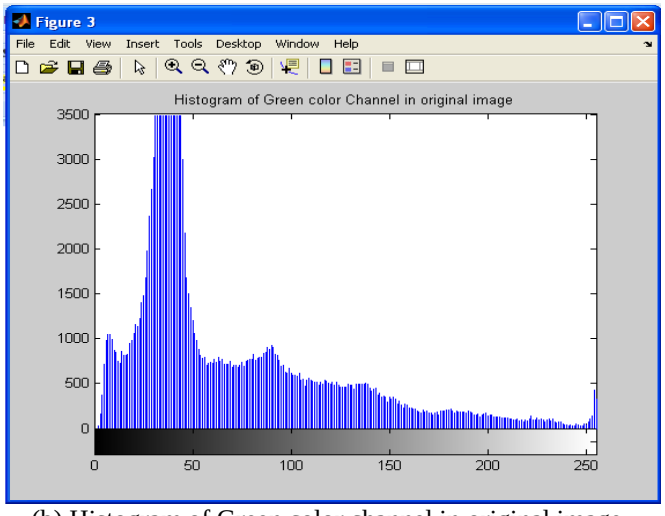


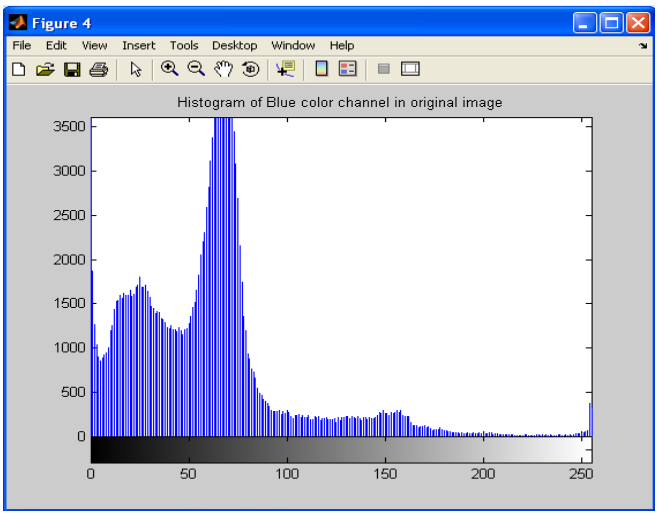

Figure 3(d) stego image containing 4 bit data in selected channel




(a) Histogram of Red color channel in original image

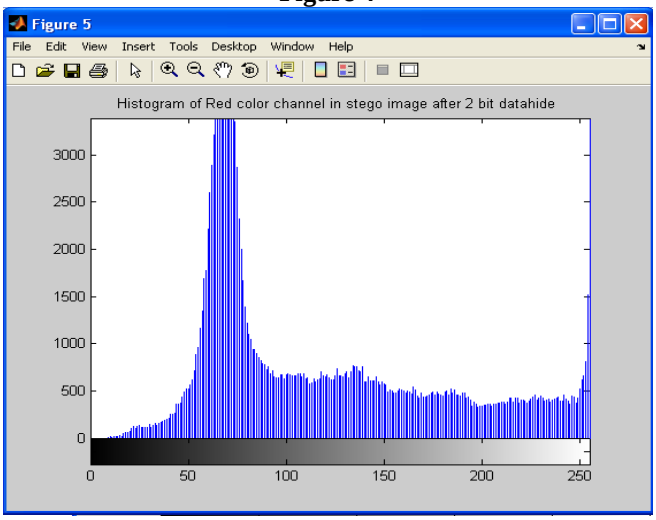



(b) Histogram of Green color channel in original image

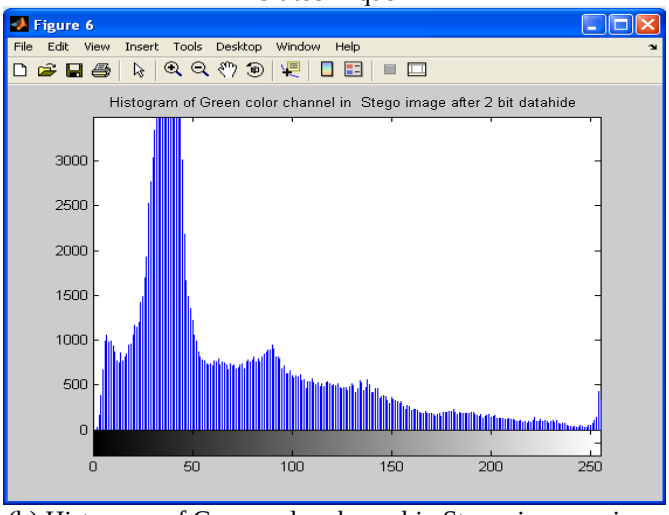



( c) Histogram of Blue color channel in original image

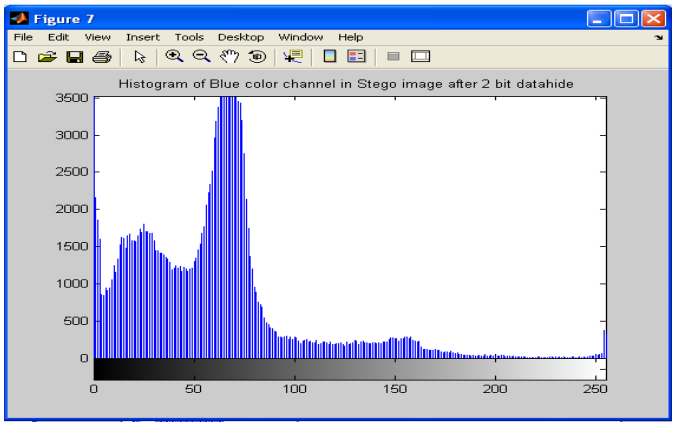
**Figure 4**




(a) Histogram of Red color channel in Stego image using 2 bit technique

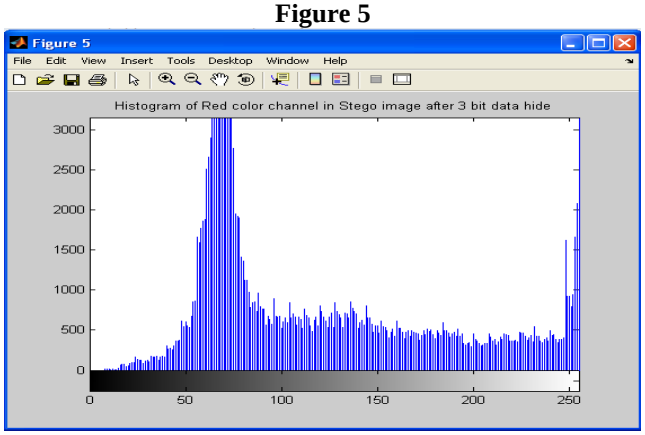



(b) Histogram of Green color channel in Stego image using 2 bit technique

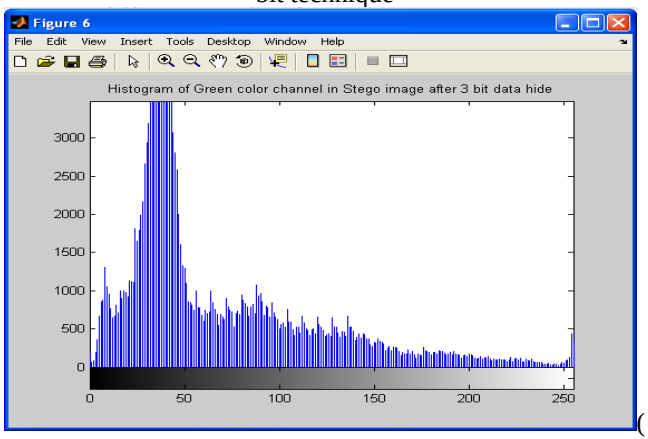



( c) Histogram of Blue color channel in Stego image using 2 bit technique

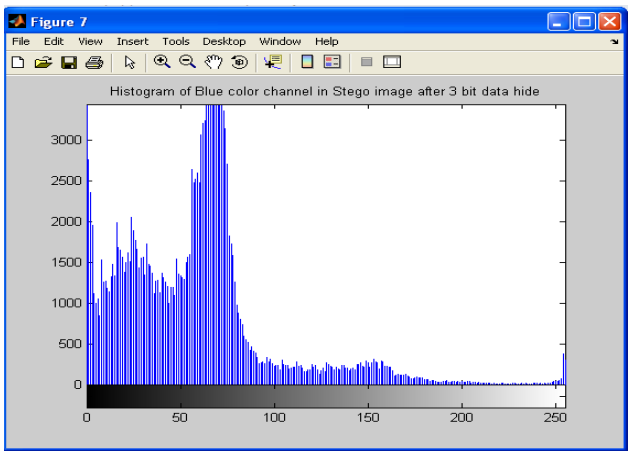
**Figure 5**




(a) Histogram of Red color channel in Stego image using 3 bit technique

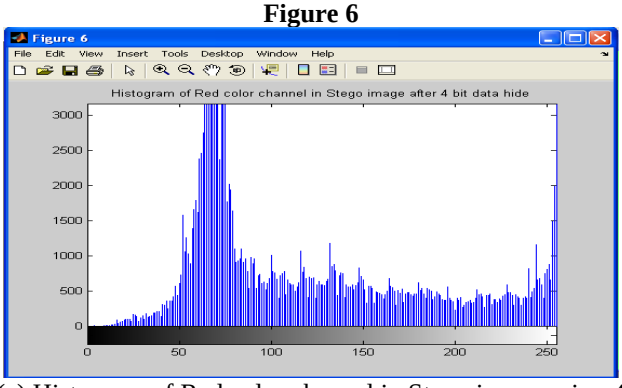



b) Histogram of Green color channel in Stego image using 3 bit technique

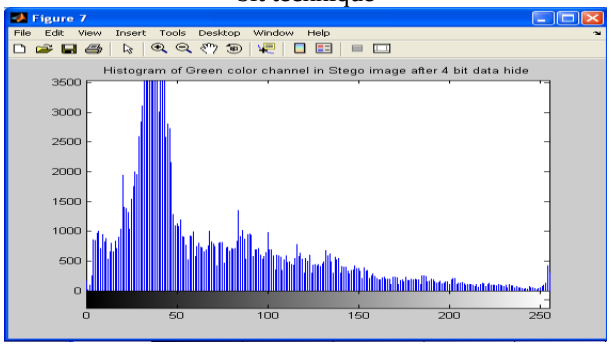



(c) Histogram of Blue color channel in Stego image using 3 bit technique

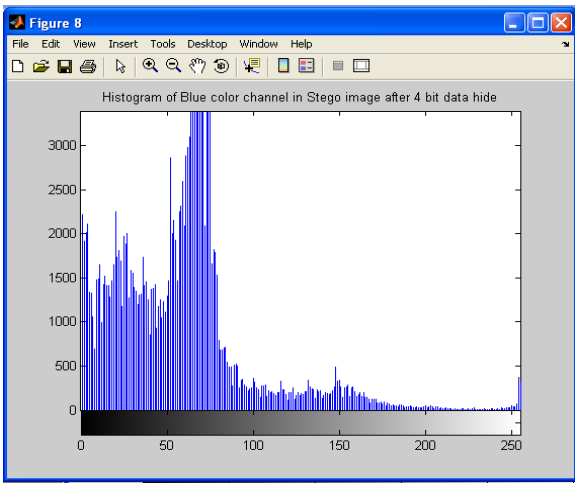
**Figure 6**




(a) Histogram of Red color channel in Stego image using 4 bit technique




(b)Histogram of Green color channel in Stego image using 4 bit technique




( c) Histogram of Blue color channel in Stego image using 4 bit technique

**Figure 7**

Results from various image and data are taken, above Table 4 shows the various results for the image peppers.png (512X384). Figure 3(a) to 3(d) is the comparison between original and stego image created during hiding process. Above Figure 4 is the histogram of original image. Figure 5 is the histogram generated during 2-bit data hiding technique(i.e 9.48 KB data hiding), Figure 6 is the histogram generated during 3- bit data hiding technique (i.e.51.8 KB data hiding), Figure 7 is the histogram generated during 4-bit data hiding technique(i.e. 71.2 KB data hiding).

## IV CONCLUSION AND FUTURE WORK

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 to hide 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.

## REFERENCES

[1] Fridrich, J. Long, "Steganalysis of LSB encoding in color images", 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", ICACT 2008.