

A New Pair Wise Bit Based Data Hiding Approach on 24 Bit Color Image using Steganographic Technique

Sudipta Kr Ghosal

Greater Kolkata College of Engineering & Management
Kolkata, India
sudipta.ghosal@gmail.com

Abstract— This paper proposes a novel steganographic method to hide information within the spatial domain of the 24-bit color image. The proposed steganographic method works by considering the three channels (viz. red, green and blue) of each pixel of the cover image one by one up to the (maximum, if desire) last pixel and calculating the number of ones and zeroes in the red channel. Then, we calculate the absolute difference value of the number of zeroes and number of ones which is again divided by the total embedding channel numbers viz. green and blue which is 2 for a 24 bit color image. The resultant number of bits of the hidden data is embedded on the LSB part (in bit range of 0-3) of the green and blue bytes (channels) of each pixel of the cover image respectively. In the reverse way, we can extract the hidden data from the green and blue channels by checking the red channel of each pixel of the stego-image. Experimental results show that the proposed technique has improvised the hiding capacity of data (text as well as image) and at the same time retains good visual clarity of the stego-image.

Keywords- Cover, 24 Bit Color Image, LSB, Hiding Capacity and Stego-image.

I. INTRODUCTION

Steganographic techniques allow communication between two authorized parties without an observer being aware that the communication is actually taking place. These techniques have many Army applications in the defensive information warfare arena, such as hidden communication, in-band captioning, and tamper proofing. A useful steganographic system must provide a method to embed data in an imperceptible manner, allow the data to be readily extracted, promote a high information rate or payload capacity, and incorporate a certain amount of robustness to removal [1], [2]. Digital steganography, or information-hiding schemes, can be characterized utilizing the theories of communication [3]. The parameters of information hiding such as the amount of data bits that can be hidden, the perceptibility of the message, and its robustness to removal can be related to the characteristics of communication systems: capacity, signal-to-noise ratio (SNR), and jamming margin. The notion of payload capacity in data hiding indicates the total number of bits hidden and successfully recovered by the stego

system. The signal-to-noise ratio serves as a measure of detectability.

The most popular one is embedding a message into a colored image using LSB [4]. In this method the data is being hidden in the least significant bit of each pixel in the cover image. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. If we are using 24-bit color image, the amount of change will be minimal and indiscernible to the human eye. But this techniques hiding capacity is not so good and the attacker can easily destroy the hidden data by changing the least significant bit with less degradation of image quality. Therefore, Wang et al. [5] proposed a method using the genetic algorithm to embed secret data into each host pixel and the transformed value is closer to the original host pixel. However, using the genetic algorithm consumes huge computational time and the solution of a mapping function is not optimal. In 2002, Chang et al. [6] offered their dynamic programming strategy to pick out the best solution from all of possible conditions that can significantly reduce the computation time. Also, Chan and Cheng [7] proposed to hide data by simple LSB substitution with an optimal pixel adjustment process (OPAP). Using the OPAP algorithm can prove that the obtained worst-mean-square-error (WMSE) between the cover image and the stego-image is less than 1/2 of that obtained by the normal LSB. Those steganographic schemes aim to improve the stego-image quality. On the other hand, an adaptive method based on using variable amount of bits instead of fixed length is proposed [8] for adjusting the hiding capacity. Ahmad A. Al-Taani and Abdullah M.L.Issa have proposed a new efficient steganographic approach for hiding information within a gray scale image. They compared the new method with two well-known methods, PVD and GLM methods. The results show the effectiveness of the proposed method compared with the other methods [9].

Also, when we talks about steganography, at that time another term comes in our mind that is watermarking. Invisible watermarking is treated as a subset of steganography [10]. The difference is that steganography conceals a message so that this hidden message is the object of the communication where in

watermarking; the hidden message provides important information about the cover media, such as authentication or copyright.

II. STEGANOGRAPHIC AND DATA HIDING METHODS

Steganography hides secret messages under the cover of a carrier signal so it cannot be seen or detected. Steganography technique should generally possess two important properties: good visual/statistical imperceptibility and a sufficient payload. The first is essential for the security of hidden communication and the second ensures that a large quantity of data can be conveyed. Two levels of protection can be done if the message is encrypted before hiding it, so it must be decrypted before reading it.

Steganography can be described by the following formulae:

$$\text{Cover media} + \text{embedded message} + \text{stegokey} = \text{Stegomedia}$$

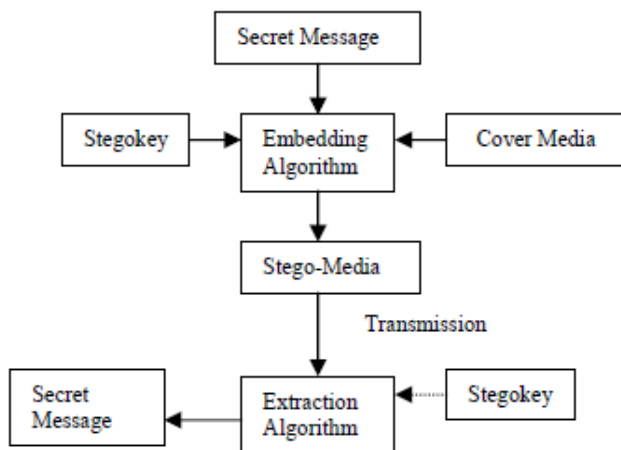


Fig. 1: Steganography Technique.

Here, we have briefly discussed about some popular steganographic methods.

A. An Introduction to LSB Technique

LSB is a simple approach to embed -ding information in an image. Applying LSB technique to each byte of a 24-bit image, three bits can be encoded into each pixel, as each pixel is represented by three bytes. Applying LSB technique to each byte of an 8-bit image, only one bit can be encoded into each pixel, as each pixel is represented by one byte. For example, if we use 8-bit image to hide the letter A (has the binary value 01000001), we need eight pixels. Suppose the original eight pixels are:

(00100111) (11101001) (11001000) (00100111) (11001000)
(11101001) (11001000) (00100111)

Inserting the letter A (as a binary value) into these eight pixels will give the following (starting from left side):

(0010011**0**) (11101001) (11001000) (0010011**0**) (11001000)
(11101000) (11001000) (00100111)

Only the emphasized bits are changed. Care needs to be taken in the selection of the cover image, so that changes to the data will not be visible in the stego-image. Common images, like the Mona Lisa painting, should be avoided.

B. An Introduction to PVD Technique

This method [11] is mainly based on the principle of that human eyes are most sensitive to smooth area and least sensitive to the edge areas of an image i.e. the degree of distortion tolerance of an edge area is naturally higher than that of a smooth area. On the basis of this principle, more data bits are embedded in the smooth areas of an image. Actually, the determination of edge or smooth areas is dependent on the difference between two consecutive pixel values. In case of smooth areas, the values of the pixels are very close to each other. On the other hand, the pixels in the edge areas differ from their neighboring pixels by a large amount. Therefore, by checking the difference between two consecutive pixel values smooth or edge area of an image are determined in this technique. Actually, secret data bits are embedded in the image by modifying the difference between two consecutive pixel values.

In this technique, the entire cover image is divided into a number of 2 X 1 non-overlapping blocks. The difference between two consecutive pixel values of each 2 X 1 block is calculated and is checked in which range in the following range table the difference actually falls.

| Range | Difference within the Range | Range Length |
|-------|-----------------------------|--------------|
| R1 | From 0 to 7 | 8 |
| R2 | From 8 to 15 | 8 |
| R3 | From 16 to 31 | 16 |
| R4 | From 32 to 63 | 32 |
| R5 | From 64 to 127 | 64 |
| R6 | From 128 to 255 | 128 |

Then the length of the range is found. If the range length is L, then log₂L number of bits is embedded and the decimal value of the embedded bits is calculated. The calculated decimal value is then added to the lower bound of the range to find the new difference. After this, the two pixel values are modified in such a way that the difference between these two pixel values is equal to the new difference.

Similarly, during the extraction phase, the difference between two consecutive pixel values is calculated and the range of that difference is found. Depending on the length of the range, hidden data bits are extracted.

C. An Introduction to Tri-way PVD Technique

This method is actually an improvement of the PVD method in terms of hiding capacity. In PVD method only one direction is referenced whereas in this method three directional edges i.e. horizontal, vertical and diagonal edges are taken into consideration in order to hide the secret data bits. At first, the entire cover image is divided into a number of non-overlapping 2 X 2 blocks. Three pixel pairs of each block are

used for embedding purpose. The pixel pair that is taken into consideration is in the horizontal, vertical and diagonal directions. Data bits are embedded on the basis of the difference between the two pixel values of each pixel pair.

The last row of blocks of the cover is reserved for storing the number of pixel-pairs used for embedding purpose.

In case of color image, the pixel value is taken as the value of the blue component i.e. in other words; the difference between the blue channel values of two pixels of each pixel-pair is used to embed the data bits. Actually, the pixel located in the first column of first row of each 2 X 2 block is taken as the first pixel of each pixel-pair. During embedding operation, each of the three pixel pairs of each 2 X 2 block is modified based on the difference value of each pixel pair. After this modification, the optimal pixel pair is found depending on some calculation. After determining the optimal pixel pair, the pixel value of the first pixel of the optimal pixel pair is taken as the pixel value of the pixel located in the first column in the first row of the 2 X 2 block under consideration. Based on the optimal pixel pair, the other two pixel pairs are modified so that the pixel values of the first pixel of those pairs become equal to the pixel value of the first pixel of the optimal pair.

The extraction process is same as that of PVD method except that the differences between the pixel values of three pixel pairs of each 2 X 2 block are checked instead of only one pixel pair in one direction.

D. An Introduction to Gutub's Pixel Indicator Technique

The pixel indicator technique uses the least two significant bits of one of the channel from Red, Green and Blue as an indicator for existence of data in the other two channels. The indicator channels are chosen in sequence, with Red being the first. The following table shows the relation between the indicator bits and the amount of hidden data stored in the other.

| Indicator Bits | Channel 1 | Channel 2 |
|----------------|-----------------------|-----------------------|
| 00 | No Hidden Data | No Hidden Data |
| 01 | No Hidden Data | 2 bits of Hidden Data |
| 10 | 2 bits of Hidden Data | No Hidden Data |
| 11 | 2 bits of Hidden Data | 2 bits of Hidden Data |

The disadvantage of the algorithm is that the capacity depends on the indicator bits and based on the cover image, the capacity can be very low. Also, the algorithm uses fixed number of bits per channel (2 bits) to store data and the image may get distorted if more bits are used per channel.

III. PROPOSED APPROACH

Our proposed steganographic technique works under the spatial domain. It is a blind, non reversible approach means that the hidden data can be easily extracted from the stego-media without the help of the cover data and though the hidden data is extracted, the cover data cannot be recovered.

This approach takes 24 bit color images as cover and the embedding data may be text of image.

In this approach we have considered each pixel one by one and embedded the secret data into it depending upon the number of color channel information's in each pixel. To embed the secret data, we have checked the number of 1's and 0's in red channel of consecutive pixels starting from the first till the last (if, necessary) to hide the entire secret data. Then, we have calculated the absolute difference value of number of 1's and 0's in each red channel which is again divided by the number of channels to be embedded in a pixel which is 2 for a 24 bit color image as there are three channels namely red, green and blue whereas embedded channel is only green and blue in our proposed approach.

Now, we are giving an example of how the above method works. Let we assume, the bit pattern (R, G and B) for two consecutive pixels of a 24-bit color image is as shown below:

11011011 00010110 10000011 01001100 00110110
10101011

Now, if we want to embed a character 'A' (has the binary value 01000001), we need to follow the above method. So, as per our method the number of one's in Red byte is 6 and number of 0's in Red byte is 2. So, the absolute difference value is $(6-2) = 4$. Dividing the above results by 2 yields $= 4/2 = 2$. So, bit embedded on the LSB part of the green byte is 2 and bit embedded on the LSB part of the blue byte is also 2.

Also, for the second R byte the number of one's is 3 and number of zeroes is 5. So, the absolute difference results value is $= (5-3) = 2$. Dividing the above results value by 2 yields $= 2/2 = 1$. So, bit embedded on the LSB part of the green byte is 1 and bit embedded on the LSB part of the blue byte is also 1. Now, the bit stream of the stego image will be as shown below:

11011011 000101**01** 100000**00** 01001100 001101**00**
101010**01**

So, by replacing only 6 bits in 4 numbers of selected bytes, we can hide the binary string 01000001.

Embedding Procedures :

Step 1: Load the 24-bit color image as cover.

Step 2: Load the data (usually, text or image) which is to be embedded.

Step 3: Consider the Red, Green and Blue channels of pixels starting from the first to a maximum of the end pixel to hide the secret information in the cover. That means, only the requisite number of pixels is needed from the cover which can hide the entire secret information.

Step 4: Calculate the number of 1's and number of 0's in the Red channel of each pixel.

Step 5: Calculate the absolute difference value of number of 1's and 0's in red channel.

Step 6: Divide the difference value results by the number of channels to be embedded in a pixel which is 2 for a 24 bit color image.

Step 7: Now, the resultant number of bits of the embedding size is to be embedded till a specified number of pixels and then data is to be embedded on the LSB (up to 3rd bit position) part of the Green and Blue bytes of each pixel of the cover image where the Red channel will act as an indicator.

Step 8: The final stego image is to be produced.

Extracting Procedures :

Step 1: Load the 24-bit color stego- image.

Step 2: Consider the Red, Green and Blue channel of pixels starting from the first of the stego-image to a maximum of the end pixel.

Step 3: Calculate the number of 1's and 0's in the Red channel of each pixel.

Step 4: Calculate the absolute difference value of number of 1's and number of 0's in red channel.

Step 5: Divide the difference value results by 2 in the same manner.

Step 6: Now, the resultant number of bits of the size data is to be extracted by traversing a specified number of pixels and depending on the size of the hidden data, the requisite secret data is to be extracted from the LSB part of the Green and Blue channels of each pixel of the stego image where the Red channel will act as an indicator.

Step 7: Now, the hidden data will be extracted from the stego image.

IV. DISCUSSION

This section discusses the results of using our proposed steganographic method to hide data in an image. The cover image used to hide data is shown in *Figure 1*. The data hidden in the file *Lena.bmp* is the image file *JU.bmp* is shown in *Figure 2*.

After embedding, the final result of the stego image is shown on *Figure 3*, where the distortion is very less and usually quite tough to find out any differences by human eyes.

| | | |
|---|---|---|
|  |  |  |
| <i>Lena.bmp</i> 512 X 512 Bit Depth:3 Fig.1 | <i>JU.bmp</i> 85 X 88 Bit Depth:3 Fig. 2 | <i>Lena_Stego.bmp</i> 512 X 512 Bit Depth:3 Fig. 3 |

The proposed technique has been tested on a database containing 100 images. In the below figure, we can see some

sample stego-images and their corresponding experimental results are shown in *TABLE 1* and *TABLE 2*.

| | | | |
|---|---|---|---|
|  |  |  |  |
| Animal0.bmp | Animal1.bmp | Animal2.bmp | Animal3.bmp |
|  |  |  |  |
| Animal4.bmp | Animal5.bmp | Animal6.bmp | Animal7.bmp |
|  |  |  |  |
| Animal8.bmp | Animal9.bmp | Animal10.bmp | Cartoon0.bmp |
|  |  |  |  |
| Cartoon0.bmp | Cartoon1.bmp | Cartoon2.bmp | Cartoon3.bmp |
|  |  |  |  |
| Cartoon4.bmp | Cartoon5.bmp | Football0.bmp | Football1.bmp |
|  |  |  |  |
| Football2.bmp | Football3.bmp | Football4.bmp | Football5.bmp |
|  |  |  |  |
| Vehicle0.bmp | Vehicle1.bmp | Vehicle2.bmp | Animal0.bmp |
| Embedded Images after Applying Proposed Approach Fig. 4 | | | |

Specifically, the following tables shows the comparison results of the maximum data hiding capacity and PSNR of 28 different images for five different techniques namely, LSB, PVD, Tri-way PVD, Gutub's Pixel Indicator and another is our proposed approach.

| Comparison Results of Hiding Capacity for Different Steganographic Techniques | | | | | | |
|---|-----------------|----------------------------|---------------|-----------------------|-----------------------------------|--------------------|
| Cover Image | Embedding Image | LSB Technique | PVD Technique | Tri-way PVD Technique | Gutub's Pixel Indicator Technique | Proposed Technique |
| | | HC | HC | HC | HC | HC |
| 1024 X 1024 | 102 X 105 | HC: Hiding Capacity (Bits) | | | | |
| Animal 0.bmp | Julogo. bmp | 786432 | 1233665 | 1855070 | 1570068 | 1541242 |
| Animal 1.bmp | Julogo. bmp | 786432 | 1197315 | 1799897 | 1572900 | 1692178 |
| Animal 2.bmp | Julogo. bmp | 786432 | 1189418 | 1798045 | 1575400 | 1869612 |
| Animal 3.bmp | Julogo. bmp | 786432 | 1205494 | 1809053 | 1548526 | 2397854 |
| Animal 4.bmp | Julogo. bmp | 786432 | 1292855 | 1920677 | 1559408 | 1782850 |
| Animal 5.bmp | Julogo. bmp | 786432 | 1240930 | 1851396 | 1588042 | 2762380 |
| Animal 6.bmp | Julogo. bmp | 786432 | 1224055 | 1844310 | 1572370 | 1456352 |
| Animal 7.bmp | Julogo. bmp | 786432 | 1260912 | 1910223 | 1528616 | 2211838 |
| Animal 8.bmp | Julogo. bmp | 786432 | 1220680 | 1890265 | 1521180 | 1665308 |
| Animal 9.bmp | Julogo. bmp | 786432 | 1220121 | 1825460 | 1583486 | 1811022 |
| Animal 10.bmp | Julogo. bmp | 786432 | 1204965 | 1818378 | 1562746 | 1413360 |
| Animal 11.bmp | Julogo. bmp | 786432 | 1205304 | 1816433 | 1570336 | 1920502 |
| Cartoon 0.bmp | Julogo. bmp | 786432 | 1225106 | 1845344 | 1587466 | 1776394 |
| Cartoon 1.bmp | Julogo. bmp | 786432 | 1188785 | 1788705 | 1445882 | 2269710 |
| Cartoon 2.bmp | Julogo. bmp | 786432 | 1222165 | 1835646 | 1780122 | 1704448 |
| Cartoon 3.bmp | Julogo. bmp | 786432 | 1227011 | 1876473 | 1579054 | 1577736 |
| Cartoon 4.bmp | Julogo. bmp | 786432 | 1268773 | 1936121 | 2010940 | 3252960 |
| Cartoon 5.bmp | Julogo. bmp | 786432 | 1228975 | 1836385 | 1977838 | 3957432 |
| Cartoon 6.bmp | Julogo. bmp | 786432 | 1193054 | 1791760 | 2414698 | 4438586 |
| Football 11.bmp | Julogo. bmp | 786432 | 1233735 | 1865270 | 1552376 | 1646528 |
| Football 12.bmp | Julogo. bmp | 786432 | 1217148 | 1828724 | 1566100 | 2101722 |
| Football 13.bmp | Julogo. bmp | 786432 | 1230036 | 1855990 | 1520514 | 1818010 |
| Football 14.bmp | Julogo. bmp | 786432 | 1239290 | 1874632 | 1462316 | 3144172 |
| Football 15.bmp | Julogo. bmp | 786432 | 1206842 | 1813700 | 1518994 | 2585952 |
| Football 16.bmp | Julogo. bmp | 786432 | 1210653 | 1813377 | 1414766 | 1916470 |
| Vehicle 1.bmp | Julogo. bmp | 786432 | 1216347 | 1834058 | 6252148 | 4625356 |
| Vehicle 2.bmp | Julogo. bmp | 786432 | 1226818 | 1853596 | 2405432 | 4225508 |
| Vehicle 3.bmp | Julogo. bmp | 786432 | 1256430 | 1890410 | 1569686 | 1819196 |

| Comparison Results of Quality of Image for Different Steganographic Techniques | | | | | | |
|--|-----------------|---------------------------------------|---------------|-----------------------|-----------------------------------|--------------------|
| Cover Image | Embedding Image | LSB Technique | PVD Technique | Tri-way PVD Technique | Gutub's Pixel Indicator Technique | Proposed Technique |
| | | PSNR | PSNR | PSNR | PSNR | PSNR |
| 1024 X 1024 | 102 X 105 | PSNR: Peak Signal to Noise Ratio (DB) | | | | |
| Animal 0.bmp | Julogo. bmp | 63.16 | 59.53 | 44.20 | 57.91 | 55.08 |
| Animal 1.bmp | Julogo. bmp | 62.98 | 59.34 | 55.60 | 57.94 | 56.33 |
| Animal 2.bmp | Julogo. bmp | 63.06 | 59.42 | 57.25 | 58.10 | 56.68 |
| Animal 3.bmp | Julogo. bmp | 63.50 | 60.01 | 41.23 | 57.80 | 52.54 |
| Animal 4.bmp | Julogo. bmp | 63.80 | 59.33 | 41.31 | 58.11 | 56.17 |
| Animal 5.bmp | Julogo. bmp | 63.43 | 59.53 | 33.07 | 57.81 | 55.81 |
| Animal 6.bmp | Julogo. bmp | 62.92 | 59.51 | 47.02 | 57.90 | 57.02 |
| Animal 7.bmp | Julogo. bmp | 63.01 | 60.22 | 43.62 | 57.80 | 50.19 |
| Animal 8.bmp | Julogo. bmp | 62.84 | 59.93 | 46.22 | 57.90 | 56.50 |
| Animal 9.bmp | Julogo. bmp | 63.22 | 58.94 | 47.15 | 57.73 | 56.29 |
| Animal 10.bmp | Julogo. bmp | 62.74 | 59.79 | 48.94 | 57.74 | 56.92 |
| Animal 11.bmp | Julogo. bmp | 63.63 | 59.45 | 41.01 | 57.84 | 55.03 |
| Cartoon 0.bmp | Julogo. bmp | 63.02 | 59.42 | 44.40 | 57.84 | 54.70 |
| Cartoon 1.bmp | Julogo. bmp | 63.45 | 59.10 | 46.46 | 56.94 | 55.75 |
| Cartoon 2.bmp | Julogo. bmp | 66.82 | 58.29 | 58.85 | 58.88 | 56.95 |
| Cartoon 3.bmp | Julogo. bmp | 62.65 | 58.73 | 60.38 | 58.16 | 54.59 |
| Cartoon 4.bmp | Julogo. bmp | 60.96 | 58.97 | 37.16 | 57.99 | 52.75 |
| Cartoon 5.bmp | Julogo. bmp | 61.89 | 59.16 | 31.07 | 57.40 | 48.06 |
| Cartoon 6.bmp | Julogo. bmp | 59.13 | 58.25 | 28.64 | 56.93 | 47.96 |
| Football 11.bmp | Julogo. bmp | 62.66 | 59.00 | 43.29 | 57.96 | 55.86 |
| Football 12.bmp | Julogo. bmp | 63.15 | 58.24 | 38.78 | 57.94 | 53.52 |
| Football 13.bmp | Julogo. bmp | 63.44 | 59.81 | 47.19 | 57.48 | 53.91 |
| Football 14.bmp | Julogo. bmp | 63.49 | 60.29 | 37.79 | 57.50 | 47.40 |
| Football 15.bmp | Julogo. bmp | 63.23 | 59.93 | 43.70 | 57.73 | 46.14 |
| Football 16.bmp | Julogo. bmp | 63.68 | 59.51 | 48.27 | 56.97 | 49.61 |
| Vehicle 1.bmp | Julogo. bmp | 69.32 | 67.27 | 34.41 | 58.42 | 41.95 |
| Vehicle 2.bmp | Julogo. bmp | 58.65 | 58.16 | 28.62 | 56.87 | 47.15 |
| Vehicle 3.bmp | Julogo. bmp | 65.01 | 59.13 | 45.70 | 58.30 | 56.19 |

In TABLE 2 the phrase **peak signal-to-noise ratio**, often abbreviated **PSNR**, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. If the PSNR value is greater than 45 for a stego-image, then we can treat it as a good quality image.

It is most easily defined via the mean squared error (**MSE**) which for two $m \times n$ monochrome images I and K where one of the images is considered a noisy approximation of the other is defined as:

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad \dots\dots\dots (1)$$

The PSNR is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \\ &= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \quad \dots\dots\dots (2) \end{aligned}$$

Here, MAXI is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using linear PCM with B bits per sample, MAXI is $2^{(B-1)}$. For color images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. When the two images are identical the MSE will be equal to zero, resulting in an infinite PSNR.

The degradation of the quality of images can also be visually noticed by applying the histogram analysis.

In statistics, a histogram is a graphical display of tabulated frequencies, shown as bars. It shows what proportion of cases fall into each of several categories: it is a form of data binning. So, we have compared the histogram of three different images where the histogram is calculated for R, G and B channel separately. Here, Figure 5, Figure 6 and Figure 7 shows three different comparison results of histograms of *Lena.bmp*, *Animal.bmp* and *Football.bmp* with their stego-images.

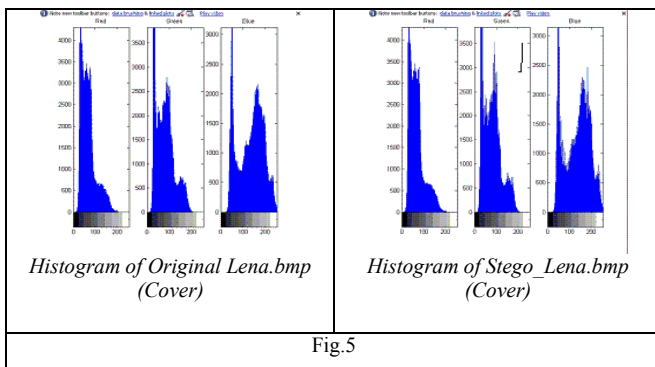


Fig.5

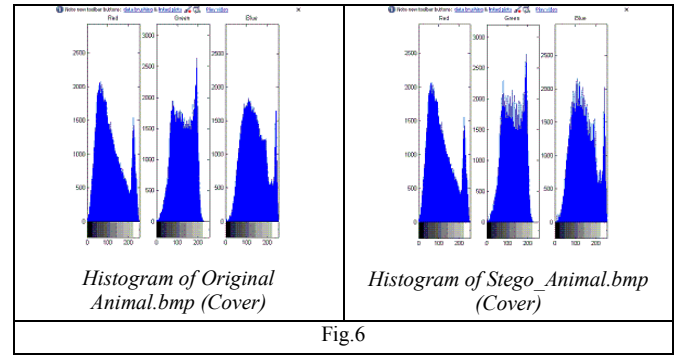


Fig.6

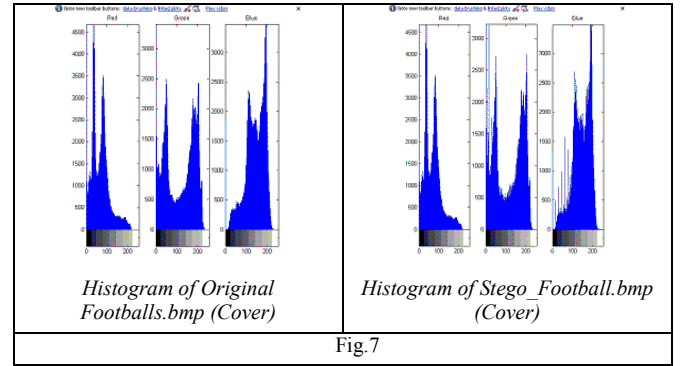


Fig.7

After seeing the above tables, figures and performing calculation based on average hiding capacity, PSNR value and after viewing the above three figures we can conclude that the average hiding capacity of the proposed technique gives better experimental results, retains good visual clarity of stego images and in the histogram analysis the histogram of Red channel is unchanged because we have used the Red channel as an indicator for bit embedding whereas significant changes in Green and Blue channel can be easily noticeable.

V. CONCLUSION AND FUTURE SCOPE

At the end of this paper, we have a much wider view of the current state of steganography technology. The proposed approach has various advantages as compared to the other methodology mentioned in the paper. The advantages are:

- ✓ This approach is a blind approach in spatial domain.
- ✓ This approach is applicable to any image formats of bit depth 3.
- ✓ It can support images of any $m \times n$ dimensions.
- ✓ The average data hiding capacity is much more than the previous techniques namely, LSB, PVD, Tri-way PVD and Gutub's Pixel Indicator technique.
- ✓ The quality of the stego-images is also highly acceptable by the human eyes which are measured in terms of PSNR values.

Though there are so many advantages, some disadvantages are also there. We know the data hiding capacity is higher in spatial domain than transform domain steganography. But, in transform domain, we can do make some transformation without losing the hidden data which is not possible in spatial

domain. So, the cover media is much robust in transform domain steganography. Also, we believe that steganography when combined with encryption provides a secure means of secret communications in between two parties. So, it can be improved by combining this approach with a novel encryption algorithm to enhance the security of the hidden data. Moreover, if hiding capacity of the cover image creates the major role then we can use some other steganographic method whose data hiding capacity will be higher than our proposed method.

VI. REFERENCES

- [1] W. Bender, 1).Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. IBM Sgsterns Journal, 35(3 & 4), 1996.
- [2] I. J. Cox, J. Kilian, T. Leighton, and T. Shamooun. Secure spread spectrum watermarking for images, audio and video. *Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland*, 111:243–246, September 1996.
- [3] J. R. Smith and B.O. Comisky. Modulation and information hiding in images. In R. Anderson, editor, *Information Hiding, First International Workshop*, volume 1174 of *Lecture Notes in Computer Science*, pages 207–226. Springer-Verlag, Berlin, 1996.
- [4] R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques", 2001 International Conference on Image Processing, October 7-10, 2001, Thessaloniki, Greece, Vol. 3, pp. 1019-1022.
- [5] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition* Vol. 34, pp. 671–683, 2001.
- [6] C.-C. Chang, J.-Y. Hsiao, C.-S. Chan, "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy," *Pattern Recognition* Vol. 36, Issue 7, pp. 1583-1595, 2003.
- [7] C.-K. Chan, L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition* Vol. 37, Issue 3, pp. 469-474, 2004.
- [8] W.-N. Lie, and L.-C. Chang, "Data hiding in images with adaptive numbers of least significant bits based on the human visual system," *IEEE International Conference on Image Processing*, Vol. 1, pp. 286–290, 1999.
- [9] Ahmad T. Al-Taani and Abdullah M. AL-Issa, "A Novel Steganographic Method for Gray-Level Images", *International Journal of Computer, Information, and Systems Science, and Engineering* 3:1 2009.
- [10] Ross, J., Fabien, A., on the limits of Steganography, *IEEE Journal*, 16(4): 474-481, 1998.
- [11] D. C. Wu and W. H. Tsai, A steganographic method for images by pixel-value differencing, *Pattern Recognition Letters*, 24(9-10), pp.1613–1626, 2003.