I.J. Image, Graphics and Signal Processing, **2015, 5, 66-74**
Published Online April 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2015.05.08

A High Capacity Secured Image Steganography Method with Five Pixel Pair Differencing and LSB Substitution

Avinash K. Gulve
Government College of Engineering, Aurangabad, Maharashtra, India. 431 005
Email: akgulve@yahoo.com, akgulve@geca.ac.in

Madhuri S. Joshi
JNEC College of Engineering, Aurangabad, Maharashtra, India. 431 005
Email: madhuris.joshi@gmail.com

***Abstract*—**Most of the steganography techniques, based on pixel value difference, use the difference between the pixel values to hide the information. In this paper, an algorithm is proposed which combines the LSB and PVD steganography techniques to provide high data hiding capacity with acceptable stego image quality. Instead of using the original difference to hide the information, the difference is revised before it is used for hiding the information. This introduces an additional layer of security for the secret information. The algorithm divides the cover image in the blocks of 2 × 3 pixels. One of the pixels in the block is used as common pixel, which forms five pixel pairs with remaining five pixels in the block. The algorithm hides three secret bits in the common pixel using the LSB substitution method and then use the PVD based approach to hide data in five pixel pairs in each block. The algorithm determines the average (*N*) of the number of bits that can be hidden in the block. If the difference value allows *M*-bits to be hidden in the pair, then bits ≤ N are hidden in that pair. The result shows that the algorithm provides higher hiding capacity with better PSNR values as compared to other methods investigated in this study.

***Index Terms*—**Information security, LSB substitution, Pixel value differencing, PSNR.

I. Introduction

Internet is commonly used for sharing of information. Since Internet is an open channel of communication, there is a need to protect the information that is transmitted over the Internet. To protect the secret information, steganography is widely used. Steganography involves hiding information so that it appears that no information is hidden. But currently there is no steganography system which can resist all the steganalysis attacks. Hence there is always a need to develop new steganography methods to provide security to the secret data. The secret data is kept within other harmless multimedia document. It is relatively easy to place information in multimedia documents. In such documents, lots of redundant areas are available where the secret information could be placed in an imperceptive way. Apart from providing security to the secret information, the steganography systems should maximize the embedding capacity while maintaining the quality of the stego image.

The secret information can be hidden in the files such as images, videos, audios or texts. Image steganography allows the text message to be hidden in the digital images.

The image steganography methods based on PVD approach use the difference between two pixels of a pair to hide the secret message. Wu et al. [1] has proposed steganography method based on PVD approach. The method uses the difference between two pixels in pair as a feature for embedding the secret message. A gray scale cover image is partitioned into non-overlapping blocks of two consecutive pixels, P_i and P_{i+1}. Difference value d_i is calculated for each block by subtracting P_i from P_{i+1}. A range table R, with table range from 0 to 255, is designed with n contiguous ranges (R_k where k = 1,2,3,…..,n). The difference $|d_i|$ is mapped on the range table to locate the suitable range R_k. The lower and upper boundaries of R_k are denoted by l_k and u_k, respectively. The width w_k of R_k is calculated by $w_k = u_k - l_k + 1$. The width w_k is used to estimate the number of bits t_i ($t_i = \log_2 w_k$) of secret message that can be hidden using the difference d_i. After hiding t_i bits, values of P_i and P_{i+1} are modified. During the phase of extraction, the same range table as it was used during embedding of secret data in the cover image is required. The difference value $d^{'}_{i}$ for each pair of two consecutive pixels P_i and P_{i+1} in the stego-image is calculated. $|d^{'}_{I}|$ is used to locate the suitable range R_k. The decimal equivalent of the secret information hidden in the block is given by $|d^{'}_{i}|-l_k$ which is then transformed into a binary sequence with t_i bits[1].

Zaker et al. [2] has proposed modification in the original PVD method so as to make it more resistive to histogram attacks. The author has suggested two rules, first rule causes the absolute difference between two pixels of a block to be less than or equal to its initial value.

And the other range overlapping rule is used to allow some new difference values to be shifted to the left neighbor range. The second rule increases the hiding capacity of the cover image [2].

In order to improve the capacity of the hidden secret data and to provide an imperceptible stego-image quality, a novel steganographic method based on least-significant-bit (LSB) replacement and pixel-value differencing (PVD) method is presented by Wu et al.[3]. The range table is divided into lower level (smooth area) and higher level (edged area). In the smooth area, 6 bits of the secret data are hidden by LSB method while in the higher-level secret data is hidden using the PVD method.

In the PVD method, two horizontal and consecutive pixels represent a vertical/ horizontal edge, but the edge can have different directions. This motivates to improve the PVD method by considering three directions. Chang et al. [4][5] has proposed a method that hides in vertical and diagonal edges along with the horizontal edges. The cover image is divided into non-overlapping blocks of 2 × 2 pixels. Each block has four pixels i.e. $P_{(x,y)}$, $P_{(x+1,y)}$, $P_{(x,y+1)}$ and $P_{(x+1,y+1)}$ where x and y are the pixel location in the image. One of the pixels is grouped with other three pixels in the block to form 3 pixel pairs. Thus three pixel pairs are formed by grouping $P_{(x,y)}$, with the other three pixels in the block. These three pairs are PP_0, PP_1 and PP_2 where $PP_0 = (P_{(x,y)},P_{(x+1,y)})$, $PP_1 = (P_{(x,y)}, P_{(x,y+1)})$ and $PP_2 = (P_{(x,y)}, P_{(x+1,y+1)})$, respectively. For each pair the difference value d_i is calculated. Based on the value of d_i, the block is differentiated as either in smooth area or in edged area. It is possible to hide more data in sharply edged area than in smooth area because the difference in sharply edged area is not noticeable by human vision system. After embedding the secret data, pixel values of both the pixels in each pair gets modified. The new pixel values in each pair are different from their original values. That is, three different values are obtained for the starting pixel $P_{(x,y)}$. However, pixel $P_{(x,y)}$ can have only one value. Therefore, one of three pairs is selected as the reference pair. The new pixel values of reference pair are close to their original values. The two pixel values of reference pair are used to adjust the values of pixels in other two pairs and construct a new 2 × 2 block. The embedded secret data is unaffected because difference values for three pixel pairs are unaltered [4][5].

Asmari et al. [6] has proposed a steganography method based on pixel value differencing and LSB substitution. The cover image is divided into sub-blocks of 4 × 4 pixels each. The data is hidden in two consecutive pixels vertically depending on the pixel value difference. The embedding process begins with hiding 3 bits of secret data in each pixel at the corner. Thus 12 bits of secret data are directly hidden in the 4 pixels at corner of the block. The remaining 12 pixels form the semi hexagonal shape. The embedding of data is applied on two consecutive pixels vertically. The embedding process determines the range using the difference of two pixel values for each pair. If the range is higher, then PVD method is used for hiding the data. Otherwise 3 bits are directly hidden in each pixel of the pair using the 3 bit LSB substitution method. This method offers higher data hiding capacity and produces stego images of good quality [6].

In PVD based steganography approach, after embedding the information using the difference in the values of two pixels in the pixel pair, the pixel values may exceed the grey scale range. Mandal et al. [7] has proposed an adaptive steganography method based on modified pixel-value differencing through management of pixel values within the range of gray scale. The method uses the PVD approach and check whether the pixel value exceeds the range on embedding. Position where the pixels exceeds boundary has been marked and a delicate handle is used to keep the value within the range. [7]

Liao et al. [8] has proposed a method to improve the embedding capacity and provide an imperceptible visual quality, based on four-pixel differencing and modified least significant bit (LSB) substitution. The block is classified as smooth area or edged area using the average difference value of a four-pixel block. The k-bit modified LSB substitution method is used to hide secret data into each pixel. The number k is decided by the level, in which the average difference value falls into. Readjustment is executed to guarantee the same level that the average difference value belongs to before and after embedding, and to minimize the perceptual distortion. [8]

Khodaei et al. [9] has presented a new adaptive data-hiding method based on least-significant-bit (LSB) substitution and pixel value differencing (PVD) for grey-scale images. The cover image is partitioned into non overlapping blocks each having three consecutive pixels in raster scan manner The method embeds k-bits of secret data in the base pixel by using LSB substitution and optimal pixel adjustment process (OPAP). The ranges are divided into two levels: low level and high level. The difference between the base pixel and other two pixels is used to estimate the number of bits to be hidden. [9].

Gulve et al. [10] has proposed a steganography method based on PVD approach. The method provides improved security to the hidden data. The cover image is partitioned into blocks of 2 × 3 pixels. In each block five pixel pairs are formed. Instead of using the difference of two pixels in each pair to hide the secret data, it is revised and then used for hiding the data. The t_i bits of secret message that can be hidden in each pair are converted to gray code form and then hidden in the pair. Thus without having the overload of encryption and decryption of secret message, the method provides higher security to the secret data.

II. The Proposed System

The methods suggested in [3][6][8][9] use PVD approach with LSB substitution to hide the secret data. These methods not only increase the hiding capacity of the cover image but also improve the security of the hidden information. One of the two pixels in the pair is used to hide data, first by LSB substitution and then, the PVD approach is used to hide the secret data in that pair.

The proposed approach outperforms the existing approaches that uses the combination of LSB substitution and PVD approach to hide secret data in terms of hiding capacity of cover image and security of the secret data. The proposed algorithm is based on the steganography method proposed by Chang [4][5] and Gulve [10]. In the proposed method, the steganography method proposed by Gulve [10] is improved to provide increase in the data hiding capacity of the cover image. The algorithm splits the image data into blocks of 2×3 pixels. One pixel in the block (common pixel) participates with remaining 5 pixels in that block to form 5 pairs as compared to PVD approach, which can form 3 pairs out of the 6 pixels. A greater number of pairs provide extra space for hiding secret data resulting in increased hiding capacity. The amount of data to be hidden in the pixel pair depends on the difference of the pixel values in the pair. If the difference value is directly used to hide the data, it is easy to retrieve the embedded data in case the steganography system fails. To enhance the security of the hidden data, the proposed algorithm modifies the difference between the pixel values in the pixel pair and this modified difference value is used to hide the message. This imposes extra layer of security making harder extraction of original secret data from stego image using the difference values directly [10].

The hiding capacity is further increased by hiding 3 extra secret data bits in the common pixel using the LSB substitution method. The algorithm then embeds the secret data in five pixel pairs of a block using the PVD approach. After embedding the secret data in the pair, the original difference is modified to get new difference value, which subsequently results in assignment of new values to the two pixels in that pair. Since the common pixel is a part of every pair, five different values are associated with it for five pixel pairs. But the common pixel can have only one value. Hence it is necessary to assign one value to the common pixel out of the five values that are associated with it. After assigning a value to the common pixel which is close to its original value, remaining pixels are adjusted maintaining the new difference value for every pair. But the value assigned to common pixel may be different than the value assigned to after embedding 3 secret bits in it. The assignment of different value to the common pixel can destroy the data which is already hidden in it using LSB substitution method. Hence another level of pixel adjustment process is applied such that the 3 LSBs of the common pixel remains unchanged keeping the new difference value between pixels in each pair unchanged.

A. Embedding algorithm

The cover image is a grey scale image, which is divided into non-overlapping 2 × 3 blocks of pixels. Five pairs of pixels are formed and these pairs are used to embed the secret information. The arrangement of pixels into non-overlapping blocks of 2 × 3 pixels is shown in fig. 1.

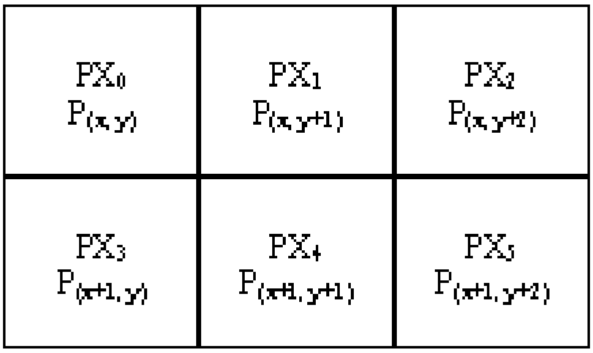


Fig. 1. Pixel Block

As shown in fig. 1, each 2 × 3 block includes six pixels $P_{(x,y)}$, $P_{(x,y+1)}$, $P_{(x,y+2)}$, $P_{(x+1,y)}$, $P_{(x+1,y+1)}$ and $P_{(x+1,y+2)}$ where x and y are the pixel locations in the image. Let PX_1 ($P_{(x,y+1)}$) be the common pixel. The embedding process begins with hiding 3 secret message bits in the pixel PX_1 using simple LSB substitution method. The three rightmost bits of Pixel PX_1 are replaced with 3 bits of binary sequence of secret information. Pixel PX_1, with its modified value, is used as common pixel to form five pixel pairs.

$PP_0 = (P_{(x,y+1)}, P_{(x,y)})$,
$PP_1 = (P_{(x,y+1)}, P_{(x,y+2)})$,
$PP_2 = (P_{(x,y+1)}, P_{(x+1,y)})$,
$PP_3 = (P_{(x,y+1)}, P_{(x+1,y+1)})$,
$PP_4 = (P_{(x,y+1)}, P_{(x+1,y+2)})$.

The difference value d_i is calculated for each pair PP_i by subtracting the common pixel from other pixel in that pair. This difference value is used to identify the range R_i from the range table R. The range table is designed with ranges [0-7], [8-15], [16-31], [32-63], [64-127], [128-255]. The width W_i of range R_i is used to determine the number of bits t_i ($t_i = \log_2 W_i$) that can be hidden in each pair. This t_i is then used to calculate the average (*N*) number of bits that can be hidden in each pair of the block. The average value ***N*** is used to calculate the revised difference $d1_i$ as $d1_i$ = remainder ($d_i/2^N$) so that $d1_i \leq 2^N$ where d_i is the original difference. The offset difference OD_i is calculated as $|d_i|$ - $|d1_i|$ for each pair in the block. The revised difference $d1_i$ is then used to determine the number of bits t_i for each pair in the block. Thus if the original difference value d_i allows M bits to be hidden in the pair, then ≤ N bits are hidden in that pair.

After embedding t_i bits of the secret information in the pixel pair PP_i, new difference d'_i is calculated as $OD_i + l_{i,k} +$ b where $l_{i.k}$ represents lower boundary of the range R_i in the range table R and b represents the decimal equivalent of t_i message bits hidden in that pair.

Embedding t_i bits in a pair modifies the values of both the pixels in that pair. The new pixel values in each pair are different from their original values. That is, five different values are obtained for the common pixel. Since, the common pixel is shared by five other pixels to form five pairs in the block; it can have only one value. Therefore, one pixel pair is selected as reference pair having new pixel values close to the original values. For selecting the reference pair, the difference ***m*** between d_i and d'_i is calculated for the pairs PP_i. The new pixel values of the pair with minimum $|\boldsymbol{m}|$ are close to the original pixel values. So the pair with minimum $|\boldsymbol{m}|$ is selected as reference pair. Two pixel values of the reference pair are used to adjust the values of pixels in other pairs. Then the block is reconstructed with the new pixel values [10].

The new value assigned to common pixel PX_1 may be different than the value assigned to it after embedding 3 secret information bits into it using LSB substitution. Accordingly two-step pixel value adjustment process is carried out and the difference d'_i is maintained for all the pixel pairs PP_i's in the block.

The algorithm for embedding the secret information in the cover image is given below.

1. Read the cover image in 2- dimensional decimal array.
2. Partition the array into non-overlapping blocks of 2 × 3 pixels
3. Read 3 leftmost bits of binary secret data and put these 3 bits into the 3 rightmost LSB's of common pixel $P_{(x,y+1)}$.
4. Calculate the difference values d_i for the five pixel pairs in each block given by

   $d_0 = P_{(x,y)} - P_{(x,y+1)}$
   $d_1 = P_{(x,y+2)} - P_{(x,y+1)}$
   $d_2 = P_{(x+1,y)} - P_{(x,y+1)}$
   $d_3 = P_{(x+1,y+1)} - P_{(x,y+1)}$
   $d_4 = P_{(x+1,y+2)} - P_{(x,y+1)}$

5. Use $|d_i|$ where i = 0,1,2,3,4 to locate suitable range $R_{i,k}$ in the designed range table. Use this range to calculate number of bits t_i that can be hidden in each pair P_i. Then calculate the average of the bits using the following equation (1)

   $$avg = \left\lfloor \left(\frac{\sum_{i=1}^{5} t_i}{5} \right) \right\rfloor \quad (1)$$

6. Calculate the revised difference $|d1_i|$ where i = 0,1,2,3,4 as $d1_i$ = remainder($d_i/2^{avg}$) so that $d1_i \leq 2^{avg}$
7. Calculate the offset difference OD_i as $OD_i = |d_i| - |d1_i|$ for each pixel pair.
8. Use $|d1_i|$ where i = 0,1,2,3,4 to locate suitable range $R_{i,k}$ in the designed range table.
9. Compute the number of bits t_i that can be embedded in each pair using the corresponding range given by $R_{i,k}$. The value t_i can be estimated from the width w_k of $R_{i,k}$, which is given by $t_i = \log_2 w_{i,k}$ where width $w_{i,k} = u_{i,k} - l_{i,k} + 1$ and $u_{i,k}$ and $l_{i,k}$ are upper and lower boundaries of the range $R_{i,k.}$
10. Read t_i bits from the binary secret data and transform the bit sequence into a decimal value b.
11. Calculate the new difference value d'_i given by
    $d'_i = OD_i + l_{i,k} + b_i$, if $d_i \geq 0$
    $d'_i = -(OD_i + l_{i,k} + b_i)$, if $d_i < 0$
12. Modify the values of pixels in pixel pair P_i by using the following equation (2)

    $$\left(P'_n, P'_{n+1}\right) = \left(P_n - \left\lceil \frac{m}{2} \right\rceil, P_{n+1} \left\lfloor \frac{m}{2} \right\rfloor \right) \quad (2)$$

    where P_n and P_{n+1} represents original values of two pixels in the pair PP_i and m is the difference between d_i and d'_i.

13. Select the pair with minimum $|m|$ as the reference pair and use this pair to adjust the values of pixels of the other four pairs. The value of the common pixel is given by P'_n of the reference pair. Modify value of other pixel P'_{n+1} of each pair such that the new difference d'_i for each pair will remain unchanged. Thus new values are assigned to remaining four pixels in the block.
14. Calculate the difference between the new value assigned to the common pixel PX_1 and the value assigned to it after embedding 3 LSB's in step 3. Subtract the difference from all the pixels in the block.
15. Check the new pixel values for fall off boundaries i.e. check whether all the pixel values are within the range 0 to 255. If not, modify the pixel values of each pair preserving the difference value.

    a. Find out smallest of all the pixel values. If smallest value is in the range -1 to – 8, add 8 in all the pixel values in that block. This is to ensure that the 3 LSB's of the common pixel $P_{(x,y+1)}$ are unchanged.
    b. Find out largest of all the pixel values. If largest is in the range 256 to 263, subtract 8 from all the pixel values in that block. This is to ensure that the 3 LSB's of the common pixel $P_{(x,y+1)}$ are unchanged.
    c. If fall of boundary problem still persists, then the cover image is not suitable for hiding secret data.

16. Now, reconstruct the block from all pixel pairs with modified pixel values.
17. Repeat steps 2 through 16 till the message gets embedded in the cover image.

B. Extraction algorithm

For extraction of the secret information from the stego-image, it is partitioned into non-overlapping blocks of 2 × 3 pixels each. The order of partitioning is same as that of embedding. For every block, five pairs of pixels are formed. The 3 LSB of common pixel are extracted and converted into binary stream with 3 bits. Then for each block, average value (N) is calculated using the same process adopted during embedding of the secret message. The average value (*N*) is used to calculate the revised difference $d1'_i$ as $d1'_i$ = remainder ($d_i/2^N$). Suitable range $R_{i,k}$ is identified using this revised difference. The secret information is extracted in the decimal form by subtracting $|d1'_i|$ from $l_{i,k}$. The secret information is then converted into a binary stream with t_i ($t_i = \log_2 w_{i,k}$) bits.

The algorithm for extraction of the secret information from the stego-image is given below.

1. Read the cover image in 2- dimensional decimal array.
2. Partition the array into non-overlapping blocks of 2×3 pixels. Keep the partition order same as data embedding.
3. Extract 3 LSB's from the common pixel $P_{(x,y+1)}$. These 3 bits are part of the secret information.
4. Calculate in difference values separately for each block in the stego-image given by

$$d_0 = P_{(x,y)} - P_{(x,y+1)}$$
$$d_1 = P_{(x,y+2)} - P_{(x,y+1)}$$
$$d_2 = P_{(x+1,y)} - P_{(x,y+1)}$$
$$d_3 = P_{(x+1,y+1)} - P_{(x,y+1)}$$
$$d_4 = P_{(x+1,y+2)} - P_{(x,y+1)}$$

5. Use $|d_i|$ where i = 0,1,2,3,4 to locate suitable range $R_{i,k}$ in the designed range table. Use this range to calculate number of bits t_i that can be hidden in each pair PP_i. Then calculate the average of the bits using the following equation (3).

$$avg = \left\lfloor \left(\frac{\sum_{i=1}^{5} t_i}{5} \right) \right\rfloor \tag{3}$$

6. Calculate the revised difference $|d1'_i|$ where i = 0,1,2,3,4 as $d1'_i$ = remainder($d_i/2^{avg}$)
7. Use $|d1'_i|$ where i = 0,1,2,3,4 to locate suitable $R_{i,k}$ in the designed range table
8. After $R_{i,k}$ is located, $l_{i,k}$ is subtracted from $|d1'_i|$ and b'_i is obtained in decimal form. b'_i represents the secret information hidden in that pair in decimal form. A binary sequence is generated from b'_i with t_i bits where $t_i = \log_2 w_{i,k}$.
9. Repeat steps 2 through 8 till embedded information gets extracted.

The process of extracting secret data hidden in the stego image is blind. It does not require the existence of original cover image.

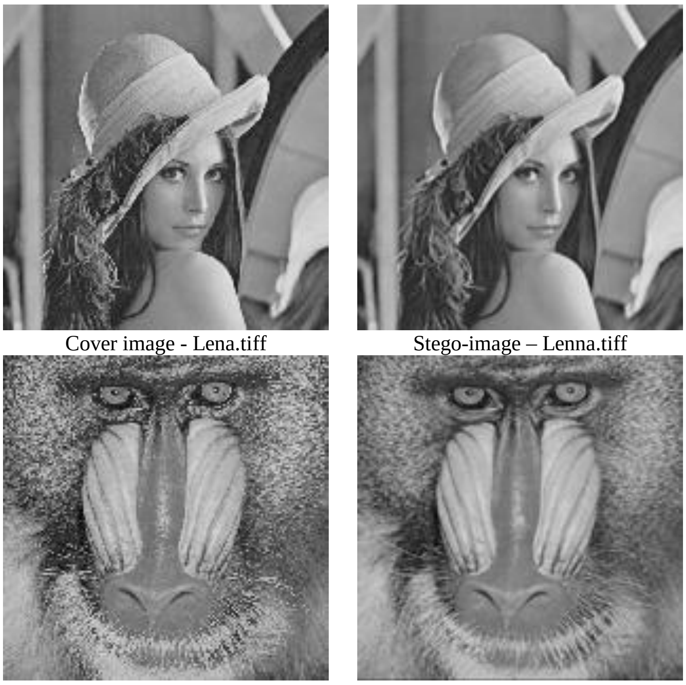
III. Results

The experimentation is carried out with a image database having 175 TIFF images. The image database has images taken from standard databases and images captured using Canon A45 camera. The standard TIFF images are obtained from the "The USC-SIPI Image Database (http://sipi.usc.edu/database/)" and the BOSS rank image database (http://exile.felk.cvut.cz/boss/BOSSFinal/Materials/BossRank.zip). Some images are captured in JPG format from Canon A45 camera and converted into gray scale TIFF format. Text files covering the full hiding capacity of the cover images are randomly generated and used as secret data. After experimentation, ~75% of the images are found suitable for hiding the secret message.

Fig. 2 shows the cover image and the corresponding stego images obtained using the proposed method. As the figures show, the difference between cover image and the stego image is imperceptible to the human vision.

Fig. 3 shows the histograms of the cover and stego images obtained using the proposed method. The shape of the two histograms is almost identical. This confirms that the stego images are of good quality.

Fig. 4 shows the pixel difference histogram of cover and stego image. From the histogram difference, it can be observed that the bins of the histogram, which are close to 0, are more in number as compared to the bins away from 0. From the pixel difference histogram, it is obvious that, for most of the pixels, the difference value is very small. Most of the difference values are spread in the short range 30 to -30. Hence the proposed algorithm is resistive to histogram analysis.



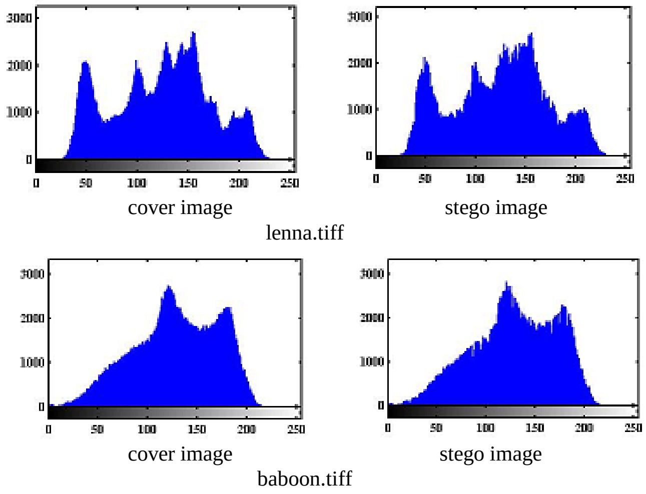
Cover image - Lena.tiff

Stego-image – Lenna.tiff

Cover image-Baboon.tiff

Stego-image-Baboon.tiff

Fig. 2. Cover and stego images using the proposed method



cover image stego image

lenna.tiff

cover image stego image

baboon.tiff

Fig. 3. Histograms of Cover and stego image

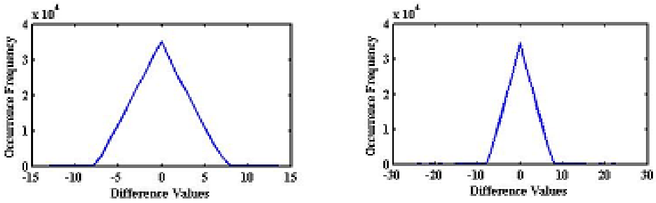


Fig. 4. Pixel difference histogram

Histogram of the cover image is represented as $[h_0,h_1,\ldots,h_{255}]$ whereas histogram of stego-image is represented as $[h'_0,h'_1,\ldots,h'_{255}]$. The change in histogram [11] can be measured by (4)

$$D_h = \sum_{m=1}^{255} |h'_m - h_m| \tag{4}$$

Fig. 5 compares the value of D_h of the 3 bit LSB replacement method and the proposed method after hiding secret data of various sizes in the cover image (Lenna.tiff). It can be observed that the change in histogram of the proposed method is smaller than the 3 bit LSB substitution methods.

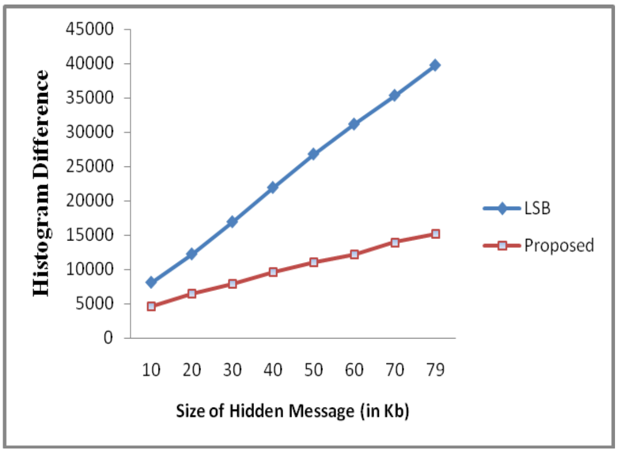


Fig. 5. Histograms comparision

The output images (lenna.tiff) are tested under the RS steganalysis[12]. It is observed from fig. 6 that the difference between R_M and R_{-M}, S_M and S_{-M} is very small. The rule $R_M \cong R_{-M}$ and $S_M \cong S_{-M}$ is satisfied for the output images. So the proposed method is secure against RS attack.

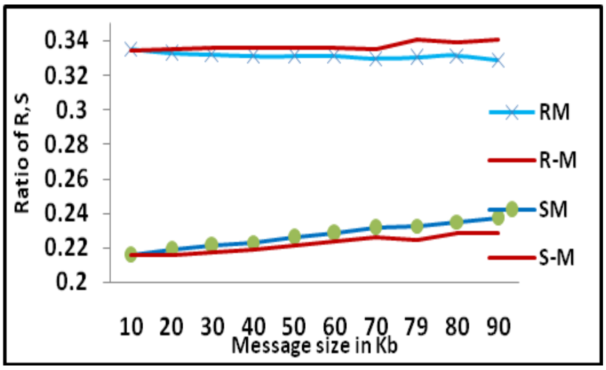


Fig. 6. Result of RS steganalysis

In table 1, the data hiding capacity and PSNR values of the proposed method are compared with Wu's Method [3], Chang's Method [4][5] and Xin Liao's Method [8], Khodaei'e Method [9] and Gulve's Method [10]. The text file of size 96136 bytes is hidden in the cover image. Although the hiding capacity of the proposed method for a special image like baboon is smaller than Xin liao's method, the PSNR is better than that of Xin Liao's Method. The capacity provided by the proposed method is comparable with that of M. Khodaei's method [9] with better PSNR values.

The PSNR and MSE are used to evaluate the quality of the stego image. The simplest and most widely used full-reference quality metric is the mean squared error (MSE), computed by averaging the squared intensity differences of distorted and reference image pixels, along with the related quantity of peak signal-to-noise ratio (PSNR) [13]. Lower MSE values and higher PSNR values are indicative of good quality of stego images. It is hard for any human being to perceive any difference between the cover image and the stego-image if the PSNR value of the stego-image goes beyond 36 dB [14]. PSNR is given by the equation (5)

$$\text{PSNR}=10 \log_{10}\left(\frac{R^2}{\text{MSE}}\right) \tag{5}$$

Where R is 255 for grey scale images.
Mean square error (MSE) is given by (6)

$$MSE=\frac{\sum_{M,N} [I_1(m,n)-I_2(m,n)]^2}{M*N} \tag{6}$$

Where I_1 and I_2 represents cover image and stego image respectively.

The hiding capacity (H.C.) is calculated for each cover image. The algorithm provides the hiding capacity @37% of the cover image size. The quality of the stego image is analyzed using PSNR, MSE, Structural Similarity Index (SSIM) [13] and Universal Quality Index (Q) [15]. Q and SSIM are full reference image quality assessment models and require the cover image to be available while assessing the quality of the stego image.

Table 2 shows the PSNR values, MSE and universal quality index for different images obtained using proposed method after hiding a text file of 96136 bytes with bit per pixel ratio of 2.97. The PSNR values are well above the threshold of 36 DB even after utilizing more than 95 % of the hiding capacity. Also universal quality index (Q) values and structural similarity index values are close to 1, which proves that the stego images are visually indistinguishable from original cover images. The proposed method provides a promising performance in increasing the hiding capacity of the cover-images and maintaining the imperceptible quality of the stego-image simultaneously.

So as to improve the performance of a steganography system, it is expected to select a reasonable cover image. S. A. Sayyedi et al [16] has proposed an unsupervised image classification algorithm for selection of a proper cover image based on edge and texture features of the image.

IV. Conclusions

This paper describes the novel approaches of steganography to hide information into gray scale images while making the stego image imperceptive. The proposed algorithm hides 3 bits of secret information in the common pixel using LSB substitution method. Then the common pixel again participates to form five pixel pairs in a block and a PVD based approach is used to hide information in the block. The algorithm revises the original difference between two pixels in the pair and this revised difference is used for hiding the data in that pair. This makes estimation of exact number of bits hidden in the pair difficult. Image steganography techniques hiding textual data requires 100% accuracy for successful retrieval of hidden data from stego image. If the steganography method fails, correct estimation of number of bits hidden in the pair will be a challenge for the invader.

Unlike the other image steganography methods, where the hiding capacity and PSNR values are dependent on the texture of the cover image, the algorithm provides uniform hiding capacity of approximately 95 Kb and consistent PSNR values close to 41 for the images of size 512 × 512.

The proposed algorithm provides increased hiding capacity while maintaining the quality of the stego image. The direct visual inspection of the stego-images did not reveal any clues about the presence of the embedded messages. The algorithm produces better PSNR values with minimum MSE. This demonstrates that better quality stego images are produced even after utilizing full data hiding capacity. The secret data hidden in the stego image can be extracted correctly without the participation of original cover image.

Table 1. Comparison of hiding capacity (In bytes) and PSNR values

Cover Image/Method	Lenna		Baboon		Pepper	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Wu’s Method [3] (2-LSB in smoothness)	66064	38.80	68007	33.33	66032	37.50
Wu’s Method [3] (3-LSB in smoothness)	95755	36.16	89731	32.63	96281	35.34
Chang’s Method [5]	75836	38.89	82407	33.93	75579	38.50
Xin Liao’s Method with 2-4 division & t=12 [8]	73761	41.87	100457	37.09	72052	42.49
M. Khodaei’s Method (Type 1 division and k = 3) [9]	98906	38.18	101266	36.72	98748	38.35
Gulve’s Method [10]	81305	42.86	81766	41.99	81326	42.80
Proposed Method	**97568**	**41.53**	**98027**	**41.00**	**97576**	**41.50**

Table 2. Results

Cover Image	Size of cover image (Kb)	Hiding Capacity (Kb)	% of Hiding capacity	Message file size (Kb)	PSNR	MSE	Q	SSIM
Resolution of cover image – 256 x 256								
Baboon	65	23.73	36.50	23	41.48	4.617	0.971	0.975
Lena	65	23.78	36.58	23	41.55	4.543	0.923	0.957
Resolution of cover image – 512 x 512								
Elaine	257	95.25	37.06	94	41.41	4.691	0.910	0.985
Baboon	264	95.72	36.25	94	41.00	5.153	0.970	0.993
Lena	259	95.28	36.77	94	41.53	4.567	0.831	0.983
Tank	257	95.24	37.05	94	41.33	4.784	0.920	0.985
Peppers	263	95.29	36.23	94	41.50	4.599	0.852	0.982
Barbara	263	95.65	36.36	94	41.28	4.834	0.879	0.987
Boat	259	95.34	36.81	94	41.32	4.787	0.906	0.987
Resolution of cover image – 1024 x 1024								
Wall	1025	382.87	37.35	380	41.32	4.790	0.919	0.997
Grass	1025	382.87	37.35	380	41.01	5.148	0.984	0.999

REFERENCES

[1] D.C Wu and W.H. Tsai, "A Steganographic Method for Images by Pixel-Value Differencing", *Pattern Recognition Letters*, Vol. 24, pp. 1613–1626, 2003.

[2] Zaker, Hamzeh, Katebi and Samavi,"Improving Security of Pixel Value Differencing Steganographic Method" , *3rd IEEE International conference on New Technologies, Mobility and Security (NTMS)*, pp. 1-4 , Cairo, 2009.

[3] H.C. Wu, N.I. Wu, C.S. Tsai and M.S. Hwang, "Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods", *IEE Proceedings on Vision, Image and Signal Processing*, Vol. 152, No. 5, pp. 611-615, 2005.

[4] Ko-Chin Chang, Huang, Tu and Chien-Ping Chang, "Adaptive Image Steganographic Scheme Based on Tri-way Pixel-Value Differencing", *IEEE International conference on Systems, Man and Cybernetics*, pp. 1165-1170, Montreal, 2007.

[5] Ko-Chin Chang, Chien-Ping Chang and Huang Tu,"A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing", *Journal Of Multimedia*, Vol. 3, No. 2, pp. 37-44, 2008.

[6] Asmari and Ghamdi,"High Capacity Data Hiding Using Semi-Hexagonal Pixels Value Difference ", *International Conference on High Performance Computing, Networking and Communication Systems (HPCNCS-09)*, pp. 14-17, Orlando, Florida, USA, 2009.

[7] J. K. Mandal and Debashis Das, "Steganography Using Adaptive Pixel Value Differencing(APVD) of Gray Images Through Exclusion of Overflow/Underflow", *Second International Conference on Computer Science, Engineering and Applications (CCSEA-2012), pp. 93-102, Delhi, 2012.*

[8] Xin Liao, Qiao-yan Wen and Jie Zhang,"A Steganographic Method for Digital Images with Four-Pixel Differencing and Modified LSB Substitution", *Journal of Visual Communication and Image Representation*, Volume 22, Issue 1, pp.1-8, 2011.

[9] M. Khodaei1 and K. Faez, "New Adaptive Steganographic Method using Least Significant Bit Substitution and Pixel-Value Differencing", *IET Image Process*., Vol. 6, Iss. 6, pp. 677–686, 2012.

[10] Gulve A.K.and Joshi M.S.," An Image Steganography Algorithm with Five Pixel Pair Differencing and Grey Code Conversion", *International Journal of Image, Graphics and Signal Processing,* Vol-6, No-3, PP. 12-20, 2014.

[11] Xinpeng Zhang and Shuozhong Wang, "Efficient Data Hiding with Histogram-Preserving Property", *Telecommunication Systems*, Volume 49- 2, p.p.179-185, 2012.

[12] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB Steganography in Color, and Gray-Scale Images", *IEEE Multimedia Magazine*, vol. 8, no. 4, pp. 22–28, 2001.

[13] Z. Wang, A. C. Bovik, H.R. Sheikh and E.P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity", *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-612, 2004.

[14] N.I. Wu and C.S. Hwang, "Data Hiding: Current Status and Key Issues", *International Journal of Network Security*, vol. 4, no. 1, pp. 1-9, 2007.

[15] Z. Wang and A.C. Bovik," Universal Image Quality Index", *IEEE SP letters*, vol. 9, pp. 81-84, 2002 .

[16] Seyyed A Seyyedi and Nick Ivanov,"Statistical Image Classification for Image Steganographic Techniques", *International Journal of Image, Graphics and Signal Processing*, Vol. 6, No. 8, pp. 19-24, 2014.

Authors' Profiles

Gulve Avinash K., received the M.E. in Computer Science and Engineering from MNIT, Allahabad in 1998. He is a faculty member of MCA department of Government College of Engineering, Aurangabad, Maharashtra, India. His areas of interest are steganography and image processing.

Joshi Madhuri S., has completed her BE from College of Engineering, Pune (1985), M.Tech. (CS) (1993) from IIT, Madras and Ph.D. from SRT University, Maharashtra, India. She has published 24 research papers in various international journals, international and national conferences. Her areas of interest are data mining and pattern recogniti.

How to cite this paper: Avinash K. Gulve, Madhuri S. Joshi,"A High Capacity Secured Image Steganography Method with Five Pixel Pair Differencing and LSB Substitution", IJIGSP, vol.7, no.5, pp. 66-74, 2015.DOI: 10.5815/ijigsp.2015.05.08