High capacity image steganography using modified LSB substitution and PVD against pixel difference histogram analysis

Gandharba Swain

Department of Computer Science and Engineering, K L University,

Vaddeswaram-522502, Guntur, Andhra Pradesh, India

gswain1234@gmail.com

Abstract- The combination of pixel value differencing (PVD) and least significant bit (LSB) substitution gives higher capacity and lesser distortion. But there are three issues to be taken care, (i) fall off boundary problem (FOBP), (ii) pixel difference histogram (PDH) analysis, and (iii) RS analysis. This paper proposes a steganography technique in two variants using combination of modified LSB substitution and PVD by taking care of these three issues. The first variant operates on 2×3 pixel blocks and the second technique operates on 3×3 pixel blocks. In one of the pixels of a block embedding is performed using modified LSB substitution. Based on the new value of this pixel, difference values with other neighboring pixels are calculated. Using these differences PVD approach is applied. The edges in multiple directions are exploited. So PDH analysis can't detect this steganography. The LSB substitution is performed in only one pixel of the block, so RS analysis also can't detect this steganography. To address the FOBP suitable equations are used during embedding procedure. The experimental results such as bit rate and distortion measure are satisfactory.

Keywords: LSB substitution, PVD, RS analysis, PDH analysis, Fall off boundary problem

1. Introduction

Least significant bit (LSB) substitution is a very old image steganography approach, wherein the LSB bits (one, two, three, or four) of the pixels are substituted by secret data bits. This simplest technique is detected by RS analysis. Wu and Tsai [1] exposed the fact that, the edge regions in an image can conceal more amounts of data as compared to the smooth regions. Based on this principle they proposed pixel value differencing (PVD) steganography. The image should be partitioned into different blocks, each of size 1×2 pixels. For a block the difference value between the two pixels is computed and changed to a new value by hiding data in it. The PVD technique with block size 2×2 has been proposed to enhance the embedding capacity [2, 3]. In blocks of size 2×2, edges in three directions are considered. Chang and Tseng [4] considered the values of 2, 3, and 4 neighboring pixels, to calculate the pixel value differences. But they did not address the fall in error problem (FIEP). Yang et al. [5] calculated varieties of pixel value differences in 4 pixel blocks for data hiding. Hong et al. [6] used diamond encoding with pixel value differencing to achieve better peak signal-to-noise ratio (PSNR). LSB substitution techniques offer higher embedding capacity, but PVD techniques offer higher imperceptibility. Thus PVD and LSB substitution techniques have been combined to obtain larger hiding capacity and better imperceptibility [7, 8]. Chen [9] proposed a PVD steganography using two reference tables to randomize the data embedding. Based on pixel value differences adaptive LSB substitution has been performed in [11]. Khodaei and Faez [10] proposed a hybrid approach by combining LSB substitution and PVD in 1×3 pixel block. It is extended to 2×2 size block in [12] and 2×3 size block in [13] to achieve better performance.

The traditional PVD steganography techniques follow a static range table. Due to this the pixel difference histogram of the stego-image becomes zig-zag in nature. This is called as step effect. This step effect can be avoided by applying two tricks, (i) exploiting the edges in multiple directions, and (ii) introducing adaptive range table. Luo et al. [14] also proposed an adaptive PVD steganography with three pixel blocks, which does not suffer with the step effect. Swain [15] proposed two adaptive PVD steganography techniques using vertical, horizontal and diagonal edges, which does not suffer with step effect. The first technique uses pixel blocks of size 2×2 and the second technique uses pixel blocks of size 3×3. In general, adaptive image steganography schemes possess lower embedding capacity. Anita et al. [16] optimized the performance of adaptive PVD by using 6 pixel blocks. The edges can be predicted by some prediction functions and hiding capacity depends upon this prediction. If we hide in smooth regions distortion will be more. Based on the level of complexity of the edge regions, adaptive embedding can be applied [17]. In this way capacity can be increased and chance of detection can be decreased. Balasubramanian et al. [18] proposed a PVD scheme with 3×3 size pixel blocks, to achieve higher hiding capacity. To prevent the detection from pixel difference histogram (PDH) analysis, multi-directional edges have been exploited in [19]. Darabkh et al. [20] also proposed PVD steganography using eight directional PVD which is an extension in principle from Wu and Tsai's original PVD. Any PVD technique which is an extension of Wu and Tsai's approach should qualify through PDH analysis.

Exploiting modification direction (EMD) steganography was initiated by Zhang and Wang [21], wherein the main idea was to convert a group of bits to a digit in (2n+1)-ary notational system, and hide it in a pixel of the block. The hiding capacity of this technique is very poor. It has been improved by Kim [22] using $(2^{n+x} - 1)$-ary notational system, where n and x are user defined values. Shen and Huang [23] combined PVD with EMD to achieve higher hiding capacity and better PSNR.

This paper proposes a combination of modified LSB substitution (M-LSB) and PVD. It is judiciously designed in such a manner that the fall off boundary problem (FOBP) does not arise; and neither PDH analysis nor RS analysis can detect it. There are two main contributions in this paper, (i) discover the FOBP that exist in Khodaei and Faez's [10] technique, (ii) and address it by proposing an improved technique with larger block size.

2. Related work

Khodaei and Faez [10] in 2012 proposed a steganography method using both PVD and LSB substitution. The embedding procedure of this technique is as described below. The image is divided into non-overlapping blocks of size 1×3, i.e. a block comprises of 3 pixels from one row and three adjacent columns of the image, as shown in Fig.1(a). Image is viewed as a two dimensional matrix of pixels/bytes. On middle pixel g_x, k bit LSB substitution is applied. The k can be chosen from 3, 4, or 5. An ideal value for k will be 3. After k bit LSB substitution, g_x becomes g'_x. Suppose the decimal values of k LSBs of g_x is L and the decimal value of k LSBs of g'_x is S. The deviation, d is equal to L-S. Now g'_x is optimized by equation (1).

$$g'_x = \begin{cases} g'_x + 2^k, \ \text{if } d > 2^{k-1} \text{ and } 0 \leq g'_x + 2^k \leq 255 \\ g'_x - 2^k, \ \text{if } d < -2^{k-1} \text{ and } 0 \leq g'_x - 2^k \leq 255 \\ g'_x, \ \text{otherwise} \end{cases} \quad (1)$$

This g'_x value is final. Two difference values $d_1 = |g'_x - g_l|$ and $d_2 = |g'_x - g_r|$ are calculated. Table 1 is the range table for type 1 and table 2 is the range table for type 2.

Table 1. Range table 1 (for type 1)

Range	[0,7]	[8,15]	[16,31]	[32,63]	[64, 255]
capacity	3	3	3	4	4

Table 2. Range table 2 (for type 2)

Range	[0,7]	[8,15]	[16,31]	[32,63]	[64, 255]
capacity	3	3	4	5	6

The value d_1 belongs to one of the ranges in range table whose lower bound is l_1 and embedding capacity is t_1. From the secret data stream t_1 bits are taken and its decimal equivalent is s_1. To hide t_1 bits of data in g_l, the new value for d_1 is d'_1. Similarly, the value d_2 belongs to a range in range table whose lower bound is l_2 and embedding capacity is t_2. From the secret data stream t_2 bits are taken and its decimal equivalent is s_2. To hide t_2 bits of data in g_2, the new value for d_2 is d'_2. These new difference values, d'_1 and d'_2 are calculated using equation (2).

$$d'_1 = l_1 + s_1 \ , \ d'_2 = l_2 + s_2 \qquad (2)$$

Two new values of g_l and two new values for g_r are calculated as below using equation (3).

$$g''_l = g'_x - d'_1 \ , \quad g'''_l = g'_x + d'_1 \ , \quad g''_r = g'_x - d'_2 \ , \quad g'''_r = g'_x + d'_2 \qquad (3)$$

Now, g'_l the final value of g_l is calculated using equation (4). Similarly, the final value of g_r known as g'_r is calculated using equation (5).

$$g'_l = \begin{cases} g''_l \ , & \text{if } |g_l - g''_l| < |g_l - g'''_l| \text{ and } 0 \le g''_l \le 255 \\ g'''_l \ , & \text{otherwise} \end{cases} \qquad (4)$$

$$g'_r = \begin{cases} g''_r \ , & \text{if } |g_r - g''_r| < |g_r - g'''_r| \text{ and } 0 \le g''_r \le 255 \\ g'''_r \ , & \text{otherwise} \end{cases} \qquad (5)$$

Thus the block of Fig.1(a) is converted to its stego-block as shown in Fig.1 (b).

g_l	g_x	g_r

(a)

g'_l	g'_x	g'_r

(b)

Fig.1 original and stego blocks of size 1×3

The extraction of the secret embedded data is done by the procedure as described below. The image is partitioned into blocks as was done in embedding procedure. A stego-block is as shown in Fig.1 (b). From the middle pixel g'_x k LSBs are extracted. Two differences d'_1 and d'_2 are calculated using equation (6).

$$d'_1 = | g'_l - g'_x | \ , \quad d'_2 = | g'_r - g'_x | \qquad (6)$$

The difference d'_1 belongs to a range of range table whose embedding capacity is t_1 and lower bound is l_1. Similarly, the difference d'_2 belongs to a range of range table whose embedding capacity is t_2 and lower bound is l_2. Note that out of two range tables the one which was used during embedding, the same should be used during extraction. The decimal equivalents of secret bit streams embedded in g_l' and g_r' are s_1 and s_2 respectively as in equation (7).

$$s_1 = d_1' - l_1 \ , \ s_2 = d_2' - l_2 \qquad (7)$$

Finally, s_1 and s_2 are converted to t_1 and t_2 binary bits respectively. These are the bits actually hidden.

3. Proposed Technique

3.1 Proposed Variant 1: Five directional PVD with modified LSB substitution

The image is divided into non-overlapping blocks of size 2×3, i.e. a block comprises of 6 pixels from two adjacent rows and three adjacent columns of the image, as shown in Fig.2 (a). The image is viewed as a two dimensional matrix of pixels/bytes. On pixel g_x , k bit LSB substitution is applied. The k value can be chosen from 3, 4 or 5. An ideal value for k is 3. After k bit LSB substitution g_x becomes g_x'. Suppose the decimal values of k LSBs of g_x is L and the decimal value of k LSBs of g_x' is S. The deviation, d is equal to L-S. Now g_x' is optimized using equation 1. This g_x' value is final.

For i=1 to 5, five difference values $d_i = |g_x' - g_i|$ are calculated. Table 1 is the range table for type 1 and table 2 is the range table for type 2. The value d_i belongs to a range in range table whose lower bound is l_i and embedding capacity is t_i. For i=1 to 5, take t_i binary bits from secret data stream and convert to decimal value s_i. Now, for i=1 to 5 calculate new difference values using equation (8).

$$d_i' = l_i + s_i \qquad (8)$$

For i = 1 to 5, for each g_i, two new values namely g_i'' and g_i''' are calculated using equation (9).

$$g_i'' = g_x' - d_i' \ , \quad g_i''' = g_x' + d_i' \qquad (9)$$

Now, for i=1 to 5, the stego-value of g_i is known as g_i'. It is calculated using equation (10).

$$g_i' = \begin{cases} g_i''' \ , & \text{if } g_i'' < 0 \\ g_i'' \ , & \text{if } g_i''' > 255 \\ g_i'' \ , & \text{if } |g_i - g_i''| < |g_i - g_i'''| \text{ and } g_i'' \geq 0 \text{ and } g_i''' \leq 255 \\ g_i''' \ , & \text{otherwise} \end{cases} \qquad (10)$$

Thus the block of Fig.3 (a) is converted to its stego-block as shown in Fig.2 (b).

g_5	g_x	g_1
g_4	g_3	g_2

(a)

g_5'	g_x'	g_1'
g_4'	g_3'	g_2'

(b)

Fig.2 Original and stego blocks of size 2×3

The extraction of the secret embedded data is done by the procedure as described below. The image is partitioned into blocks as was done in embedding procedure. A stego-block is shown in Fig.2 (b). From the pixel g_x' , the k least significant bits are extracted. For i= 1 to 5, five difference values are calculated using equation (11).

$$d_i' = | g_x' - g_i' | \qquad (11)$$

The difference d_i' belongs to a range of the range table whose embedding capacity is t_i and lower bound is l_i. Note that out of two range tables the one which was used during embedding, the same should be used during extraction. The decimal equivalents of secret bit streams embedded in g_i' is s_i. It is calculated using equation (12).

$$s_i = d'_i - l_i \qquad (12)$$

Finally, for i= 1 to 5, each s_i is converted to t_i binary bits. These bits are the embedded data.

3.2 Example of Embedding and Extraction for proposed technique-variant 1 and FOBP

To understand the embedding procedure, let us consider the original block in Fig.3 (a). Suppose the secret data to be embedded is 100 1111 101 000 001 001. Let us choose the k value as 3 and Table 1 as the range table. The value of g_x is 181. The values of g_1, g_2, g_3, g_4, and g_5 are 255, 200, 190, 192, and 182 respectively. The g_x in binary is 10110101_2. Taken 3 bits of data, i.e. 100 from the secret data stream and embed in g_x using LSB substitution. The new binary value is 10110100_2 and its decimal equivalent is 180, thus g'_x is 180. The decimal value of 3 LSBs of g_x is 5 and the decimal value of 3 LSBs of g'_x is 4. The deviation, d is equal to 5-4=1. Now g'_x is optimized using equation (1). Hence final value of g'_x after optimization is 180.

Now the five difference values are $d_1=|180-255|=75$, $d_2=|180-200|=20$, $d_3=|180-190|=10$, $d_4=|180-192|=12$ and $d_5=|180-182|=2$. The value d_1 belongs to the range [64, 255], so $t_1=4$ and $l_1=64$. The value d_2 belongs to the range [16, 31], so $t_2=3$ and $l_2=16$. Similarly, $t_3=3$, $l_3=8$, $t_4=3$, $l_4=8$, $t_5=3$ and $l_5=0$. Take t_1 , t_2 , t_3, t_4 and t_5 binary bits from secret data stream and convert to decimal values s_1 , s_2 , s_3, s_4 and s_5 respectively. Hence $s_1=15$, $s_2=5$, $s_3=0$, $s_4=1$ and $s_5=1$.

Using equation (8), $d'_1=64+15=79$, $d'_2=16+5=21$, $d'_3=8+0=8$, $d'_4=8+1=9$ and $d'_5=0+1=1$. Using equation (9), $g''_1=180-79=101$, $g'''_1=180+79=259$, $g''_2=180-21=159$, $g'''_2=180+21=201$, $g''_3=180-8=172$, $g'''_3=180+8=188$, $g''_4=180-9=171$, $g'''_4=180+9=189$, $g''_5=180-1=179$ and $g'''_5=180+1=181$.

Using equation (10), $g'_1=101$, $g'_2=201$, $g'_3=188$, $g'_4=189$ and $g'_5=181$. Hence the stego-block is as shown in Fig.3(b).

182	181	255
192	190	200

(a) Original block

181	180	101
189	188	201

(b) Stego block

Fig. 3 Examples of 2×3 original and stego blocks

To understand the extraction procedure, let us consider the stego-block in Fig.3 (b). The value of g'_x is 180, in binary 10110100_2, the three LSBs, 100_2 are extracted. Using equation (11), $d'_1=|180-101|=79$, $d'_2=|180-201|=21$, $d'_3=|180-188|=8$, $d'_4=|180-189|=9$, and $d'_5=|180-181|=1$. The value d'_1 belongs to [64, 255], so $t_1=4$ and $l_1=64$. The value d'_2 belongs to [16, 31], so $t_2=3$, $l_2=16$. Similarly, $t_3=3$, $l_3=8$, $t_4=3$, $l_4=8$, $t_5=3$ and $l_5=0$.

Using equation (12), $s_1=15$, $s_2=5$, $s_3=0$, $s_4=1$ and $s_5=1$. Converting s_1, s_2, s_3, s_4 and s_5 to t_1, t_2, t_3, t_4 and t_5 binary bits, we get 1111 101 000 001 001. From g'_x , we had extracted 100_2. Thus the total data extracted is, 100 1111 101 000 001 001.

Fall of Boundary Problem (FOBP): A pixel of a gray image is represented in 8 bits. The decimal value of a pixel falls in the range {0, 255}. If a stego-pixel value is less than zero or greater than 255, then we declare that a FOBP has arose. Khodaei and Faez's LSB+PVD approach is a very fantastic one and have higher embedding capacity and PSNR. But it suffers with FOBP.

Khodaei and Faez's technique suffers with FOBP. It can be understood from the following discussion. Let us consider a 1×3 pixel block as shown in Fig.4 (a). The secret data stream to be embedded is: 100 001 1111 000 etc. The middle pixel i.e. g_x is 181, its binary value in 8 bits is: 10110101_2. The values of g_l and g_r are 182 and 255 respectively. Let us choose k=3 and Table 1 as range table. The 3 bits of data from the secret data stream is 100. After applying 3 bit LSB substitution, the binary value of g_x changes to 10110100_2, which is equal to 180 in decimal. Thus the value of g'_x is 180. The three least significant bits of g_x are 101, in decimal it is 5. The three least significant bits of g'_x are 100, in decimal it is 4. Thus d=L-S=5-4=1. By applying equation (1), the optimized value of g'_x is 180, as shown in Fig.4 (b).

182	181	255

(a)

182	180	255

(b)

181	180	259

(c)

Fig.4 Embedding example in 1×3 blocks

Now we calculate two difference values $d_1 = |g'_x - g_l| = |180 - 182| = 2$ and $d_2 = |180 - 255| = 75$. The difference d_1 belongs to the range {0, 7}, so l_1 and t_1 value are 0 and 3 respectively. The next 3 bits of data from the secret data stream are 001, its decimal value is 1, i.e. s_1=1. The new difference d'_1 is 0+1=1, as per equation (2). The difference d_2 belongs to the range {64, 255}, so l_2 and t_2 value are 64 and 4 respectively. The next 4 bits of data from the secret data stream are 1111, its decimal value is 15, i.e. s_2=15. The new difference d'_2 is 64+15=79, as per equation (2).

Now by referring equation (3), $g''_l = g'_x - d'_1 = 180 - 1 = 179$, $g'''_l = g'_x + d'_1 = 180+1 = 181$, $g''_r = g'_x - d'_2 = 180-79 = 101$, and $g'''_r = g'_x + d'_2 = 180+79 = 259$. By referring equations (4) and (5) g'_l and g'_r are calculated. This is shown as equations (13) and (14) respectively.

$$g'_l = \begin{cases} 179, & \text{if } |182 - 179| < |182 - 181| \text{ and } 0 \le 179 \le 255 \\ 181, & \text{otherwise} \end{cases} = 181 \quad (13)$$

$$g'_r = \begin{cases} 101, & \text{if } |255 - 101| < |255 - 259| \text{ and } 0 \le 101 \le 255 \\ 259, & \text{otherwise} \end{cases} = 259 \quad (14)$$

Hence the g'_l=181 and g'_r=259. The stego-block is as shown in Fig.4(c). A FOBP occurred. Thus the embedding procedure of Khodaei and Faez's technique needs some modification.

3.3 Proposed Variant 2: Eight directional PVD with modified LSB substitution

The image is divided into non-overlapping blocks of size 3×3, i.e. a block comprises of 9 pixels from three adjacent rows and three adjacent columns of the image, as shown in Fig.5 (a). Image is viewed as a two dimensional matrix of pixels/bytes. On pixel g_x, k bit LSB substitution is applied. The k value can be chosen from 3, 4 or 5. An ideal value for k will be 3. After k bit LSB substitution g_x becomes g'_x. Suppose the decimal values of k LSBs of g_x is L and the decimal value of k LSBs of g'_x is S. The deviation, d is equal to L-S. Now g'_x is optimized using equation 1. This g'_x value is final.

For i=1 to 8, eight difference values $d_i = |g'_x - g_i|$ are calculated. Table 1 is the range table for type 1 and table 2 is the range table for type 2. The value d_i belongs to a range in range table whose lower bound is l_i and embedding capacity is t_i. For i=1 to 8, take t_i binary bits from secret data stream and convert to decimal value s_i. Now, for i=1 to 8 calculate new difference values using equation (15).

$$d_i' = l_i + s_i \qquad (15)$$

For i= 1 to 8, for each g_i, two new values namely g_i'' and g_i''' are calculated using equation (16).

$$g_i'' = g_x' - d_i' , \quad g_i''' = g_x' + d_i' \qquad (16)$$

Now, for i=1 to 8, g_i' , the stego-value of g_i is calculated using equation (17).

$$g_i' = \begin{cases} g_i''' & , \text{ if } g_i'' < 0 \\ g_i'' & , \text{ if } g_i''' > 255 \\ g_i'' & , \text{ if } |g_i - g_i''| < |g_i - g_i'''| \text{ and } g_i'' \geq 0 \text{ and } g_i''' \leq 255 \\ g_i''' & , \text{ otherwise} \end{cases} \qquad (17)$$

Thus the block of Fig.5 (a) is converted to its stego-block as shown in Fig.5 (b).

g_6	g_7	g_8
g_5	g_x	g_1
g_4	g_3	g_2

(a)

g_6'	g_7'	g_8'
g_5'	g_x'	g_1'
g_4'	g_3'	g_2'

(b)

Fig.5 Original and stego-blocks of size 3×3

The extraction of hidden data is done by the procedure as described below. From the stego-image blocks are formed as in embedding procedure. A stego-block is as shown in Fig.5 (b). From the pixel g_x' , k least significant bits are extracted. For i= 1 to 8, eight difference values are calculated using equation (18).

$$d_i' = |\, g_x' - g_i' \,| \qquad (18)$$

The difference d_i' belongs to a range of range table whose embedding capacity is t_i and lower bound is l_i. Note that out of two range tables the one which was used during embedding, the same should be used during extraction. The decimal equivalents of secret bit stream embedded in g_i' is s_i. It is calculated using equation (19).

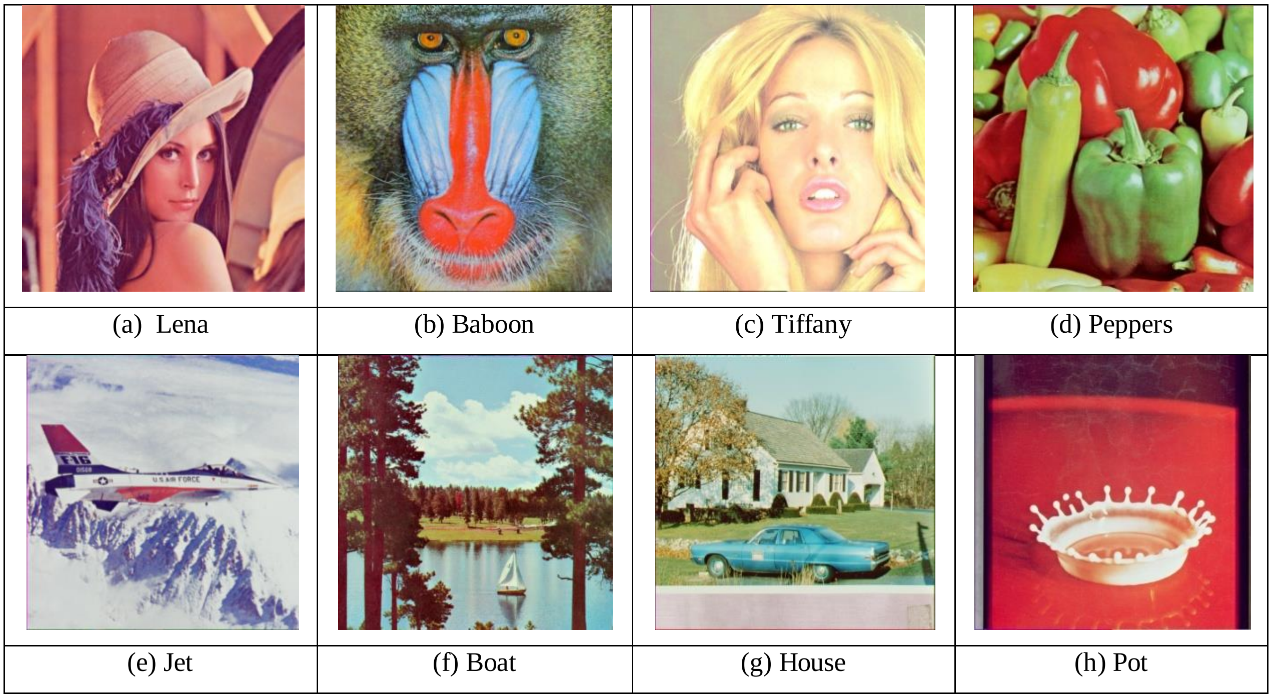
$$s_i = d_i' - l_i \qquad (19)$$

Finally, for i= 1 to 8, each s_i is converted to t_i binary bits. These bits are the embedded data.

4. Results and Discussion

The proposed technique (variant 1 and 2) is experimented using MATLAB programming. The test images are taken from SIPI database [24]. The eight sample images are shown in Fig.6. These are RGB color images of size 512×512. Each pixel consists of 3 bytes. Each byte is treated like a pixel for computation point of view. Fig.7 represents the stego-images of Lena and Baboon for proposed variant 1. Fig.8 represents the stego-images of Leena and Baboon for proposed variant 2. It can be observed from the stego-images that there is no distortion observable to be suspected as stego-images, they are as good as original images. In each of these stego-images 840000 bits (eight lakhs and forty thousand bits) of data is hidden.

The proposed technique is compared with the Khodaei and Faez's technique in terms of PSNR, hiding capacity, quality index (Q) and bits per byte (BPB). The formulae to measure these parameters are referred from [25]. The number of cases of fall off boundary arisen during execution is recorded for these techniques. From Table 3 it can be observed that in both type 1 and type 2 of Khodaei and Faez's technique FOBP arises. Further from Tables 4 and 5 it can be observed that both the variants of proposed technique do not suffer with FOBP. In proposed technique the hiding capacity and bit rate are higher than that of Khodaei and Faez's technique, but PSNR is slightly lower than that of Khodaei and Faez's technique.



(a) Lena, (b) Baboon, (c) Tiffany, (d) Peppers, (e) Jet, (f) Boat, (g) House, (h) Pot

Fig.6 Original Images

Type 1, Type 2, Type 1, Type 2

Fig.7 Stego-images of proposed variant 1: five directional PVD with M-LSB substitution

Type 1, Type 2, Type 1, Type 2

Fig.8 Stego-images of proposed variant 2: eight directional PVD with M-LSB substitution

Table 3. Results of Khodaei and Faez's PVD technique

Images 512×512×3	Type 1					Type 2				
	PSNR	Capacity	Q	bit rate	fobp	PSNR	Capacity	Q	bit rate	fobp
Lena	41.74	2375248	0.999	3.02	98	40.46	2434603	0.999	3.09	121
Baboon	37.27	2443361	0.998	3.10	12	34.19	2662080	0.996	3.38	26
Tiffany	38.7	2372396	0.997	3.01	12045	39.27	2416944	0.998	3.07	11994
Peppers	38.57	2372858	0.999	3.01	0	36.91	2435223	0.998	3.09	2
Jet	39.98	2374048	0.998	3.01	0	40.13	2418419	0.998	3.07	0
Boat	39.18	2391994	0.999	3.04	0	36.9	2504613	0.996	3.18	7
House	38.58	2387183	0.998	3.03	4	37.97	2470824	0.998	3.14	16
Pot	40.33	2366001	0.999	3.00	0	37	2387494	0.999	3.03	0
Average	39.29	2385386	0.998	3.03	1520	37.85	2466275	0.998	3.13	1521

Table 4. Results of proposed variant 1: five directional PVD with M-LSB substitution

Images 512×512×3	Type 1					Type 2				
	PSNR	Capacity	Q	bit rate	fobp	PSNR	Capacity	Q	bit rate	fobp
Lena	41.14	2379222	0.999	3.03	0	39.58	2451046	0.999	3.12	0
Baboon	34.35	2496404	0.996	3.17	0	31.72	2816768	0.993	3.58	0
Tiffany	37.27	2376135	0.996	3.02	0	35.74	2432745	0.995	3.09	0
Peppers	35.56	2379292	0.998	3.03	0	35.45	2459762	0.998	3.13	0
Jet	39.57	2384676	0.998	3.03	0	39.73	2454060	0.998	3.12	0
Boat	35.84	2409235	0.998	3.06	0	34.16	2565007	0.997	3.26	0
House	36.9	2404582	0.998	3.06	0	36.46	2533362	0.997	3.22	0
Pot	40.35	2369274	0.999	3.01	0	36.96	2399556	0.999	3.05	0
Average	37.62	2399853	0.998	3.05	0	36.23	2514038	0.997	3.20	0

Table 5. Results of proposed variant 2: eight directional PVD with M-LSB substitution

Images 512×512×3	Type 1					Type 2				
	PSNR	Capacity	Q	bit rate	fobp	PSNR	Capacity	Q	bit rate	fobp
Lena	41.04	2371255	0.999	3.02	0	39.38	2533551	0.999	3.22	0
Baboon	33.76	2502616	0.996	3.18	0	31.23	2939376	0.992	3.74	0
Tiffany	37.2	2366437	0.996	3.01	0	34.71	2511139	0.994	3.19	0
Peppers	35.15	2371837	0.998	3.02	0	34.1	2544392	0.997	3.24	0
Jet	39.52	2377031	0.998	3.02	0	39.2	2538801	0.998	3.23	0
Boat	35.32	2405009	0.998	3.06	0	33.17	2659795	0.997	3.38	0
House	37.58	2399229	0.998	3.05	0	36.66	2625804	0.998	3.34	0
Pot	40.34	2359271	0.999	3.00	0	36.33	2475977	0.999	3.15	0
Average	37.49	2394086	0.998	3.04	0	35.60	2603604	0.997	3.31	0

Furthermore the PSNR and hiding capacity of three closely related techniques discussed in [12], [13], and [19] is recorded in Table 6. Techniques in [12] and [13] are extension of Khodaei and Faez's [10] technique, so they suffer with FOBP. Technique in [19] is extension of Wu and Tsai's [1] PVD technique. It also suffers with FOBP. Although the PSNR values of these three techniques are greater than that of the proposed technique, but the hiding capacity of the proposed technique is higher than these techniques.

Table 6. Results of proposed variant 2: eight directional PVD with M-LSB substitution

Images 512×512×3	LSB+3PVD technique [12]				LSB+5PVD technique [13]				7 way PVD [19]	
	Type 1		Type 2		Type 1		Type 2			
	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity
Lena	42.22	2361875	40.83	2437700	41.84	2362944	39.98	2451046	40.81	1896662
Baboon	34.66	2393475	32.34	2772545	34.32	2396696	31.99	2816768	33.28	2226806
Tiffany	42.02	2363192	41.50	2425193	40.59	2363455	40.37	2432745	40.38	1400756
Peppers	39.27	2364428	38.04	2447737	38.16	2365366	36.50	2459762	39.63	1778072
Jet	41.81	2365839	41.90	2443492	41.26	2366486	40.62	2454060	40.36	1906254
Boat	38.04	2370147	36.13	2539530	37.10	2372127	34.76	2565007	37.14	1972086
House	39.66	2366686	38.73	2510373	38.59	2368303	37.51	2533362	37.83	1972223
Pot	42.39	2364360	41.17	2394782	40.26	2364549	36.95	2399556	41.81	1795551
Average	40.01	2368750	38.83	2496419	39.02	2369991	37.34	2514038	38.91	1868551

The proposed technique (variant 1 and variant2) use LSB substitution and PVD, so need to be analyzed by both RS analysis and PDH analysis. Fig.9 represents the PDH analysis using Lena, Baboon, Jet and Tiffany images for type 1 and type 2 of Khodaei and Faez's technique. There are eight sub-figures in it. Each sub-figure represents two curves. The solid line curve is for the original image and the dotted line curve is for the stego-image. The curve of original image will be smooth in nature means free from zig-zag appearance. This zig-zag appearance is called as step effect. For Lena image the step effect is clearly identified and for other three images it is slightly identified. For the proposed variant 1 the PDH analysis is shown in Fig.10. The step effects are reduced as compared to that of Khodaei and Faez's technique. For the proposed variant 2 the PDH analysis is shown in Fig.11. The step effects do not exist at all.

The RS analysis of Khodaei and Faez's technique and the proposed technique is shown in Figs.12-14, using Lena and Baboon images. It is carried out by computing 4 parameters such as R_{-m}, S_{-m}, R_m and S_m [25]. If the condition $R_m \approx R_{-m} > S_m \approx S_{-m}$ is true, then RS analysis fails to detect the steganography technique. But if the condition $R_{-m} - S_{-m} > R_m - S_m$ is true, then the RS analysis succeeds in detecting the steganography technique. From these figures it is evident that Khodaei and faez's technique and the proposed technique, both escape from RS analysis.

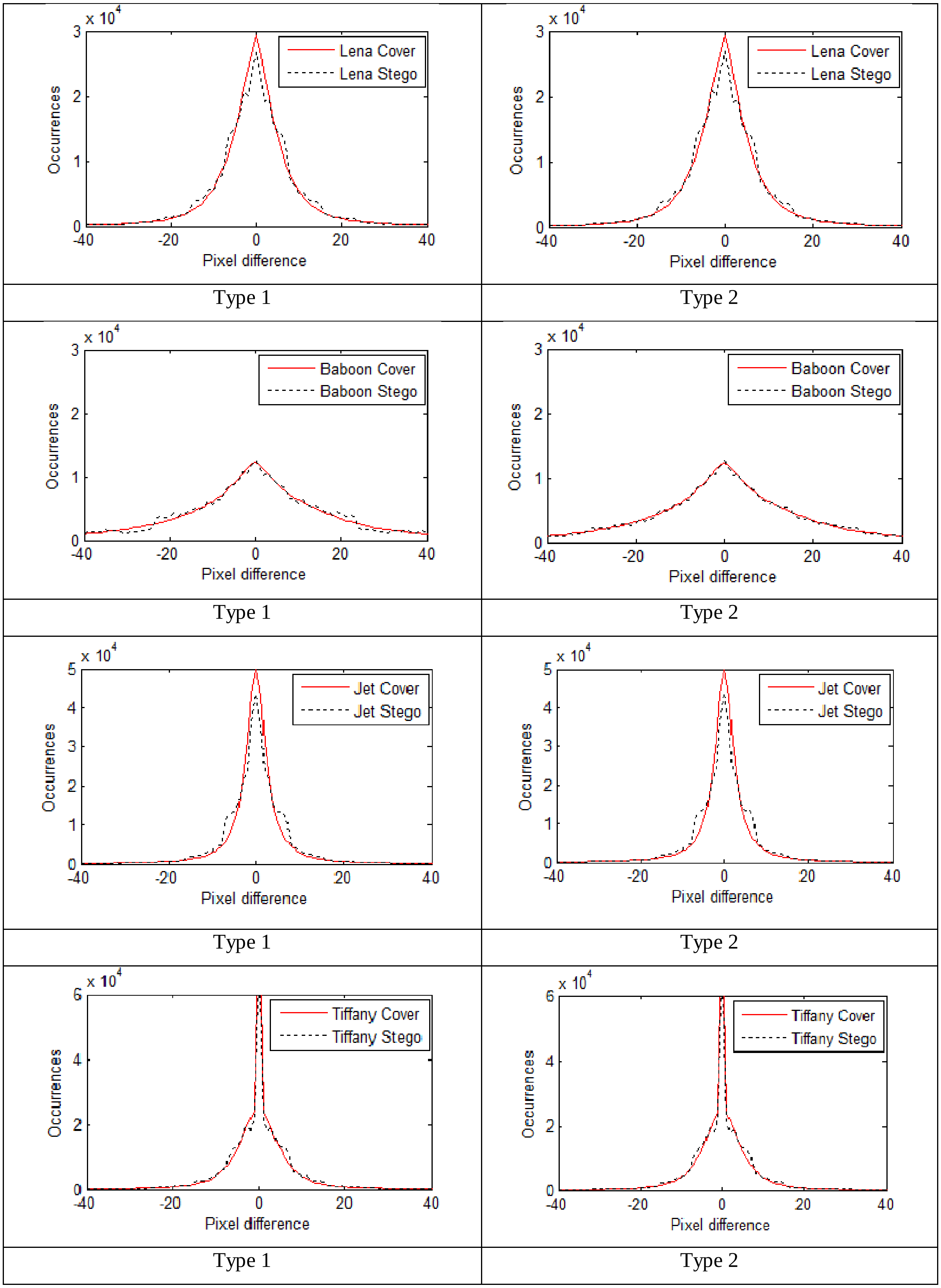


Fig.9 PDH analysis of Khodaei and Faez's PVD technique

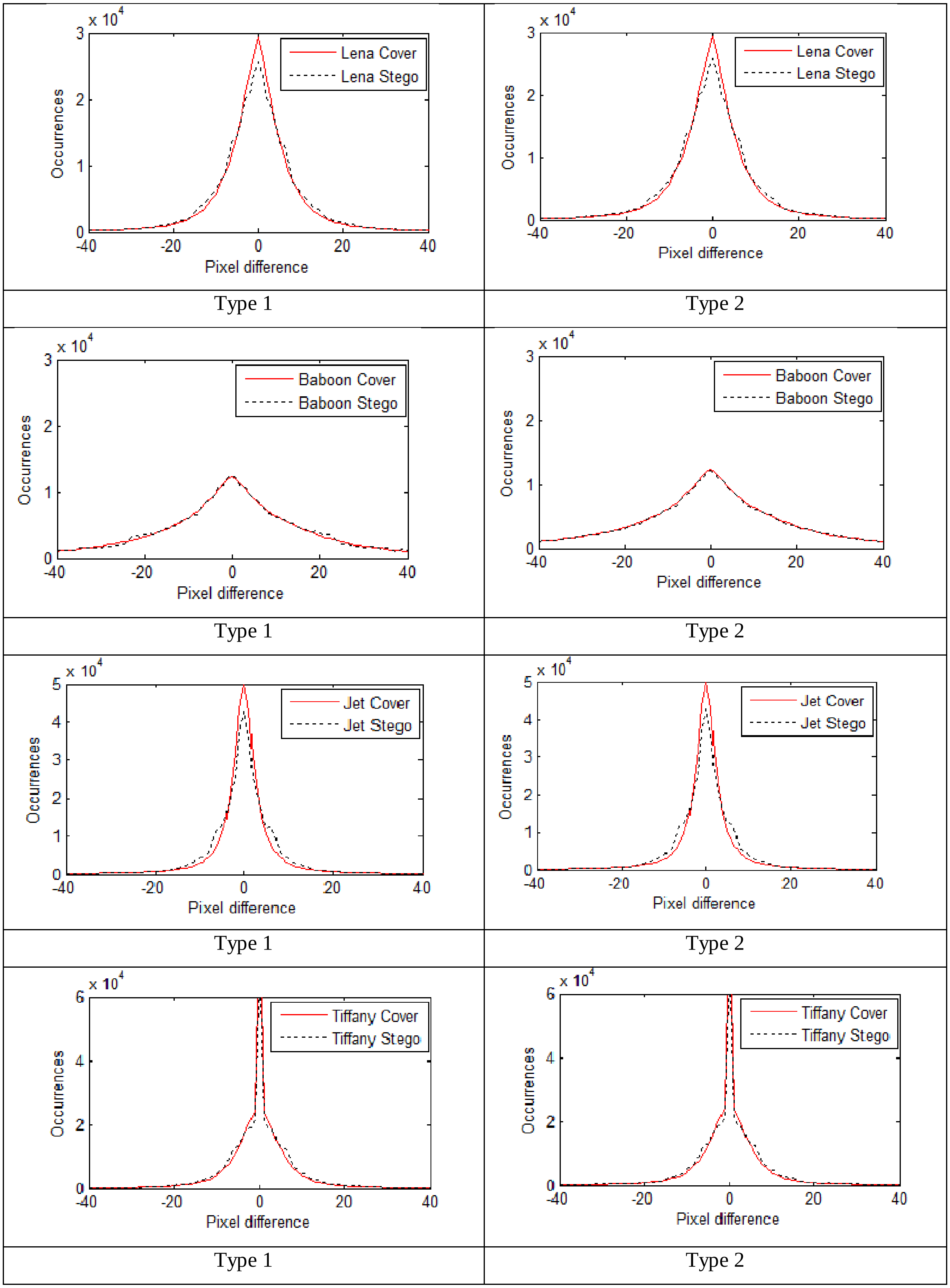


Fig.10 PDH analysis of proposed variant 1: five directional PVD with M-LSB substitution

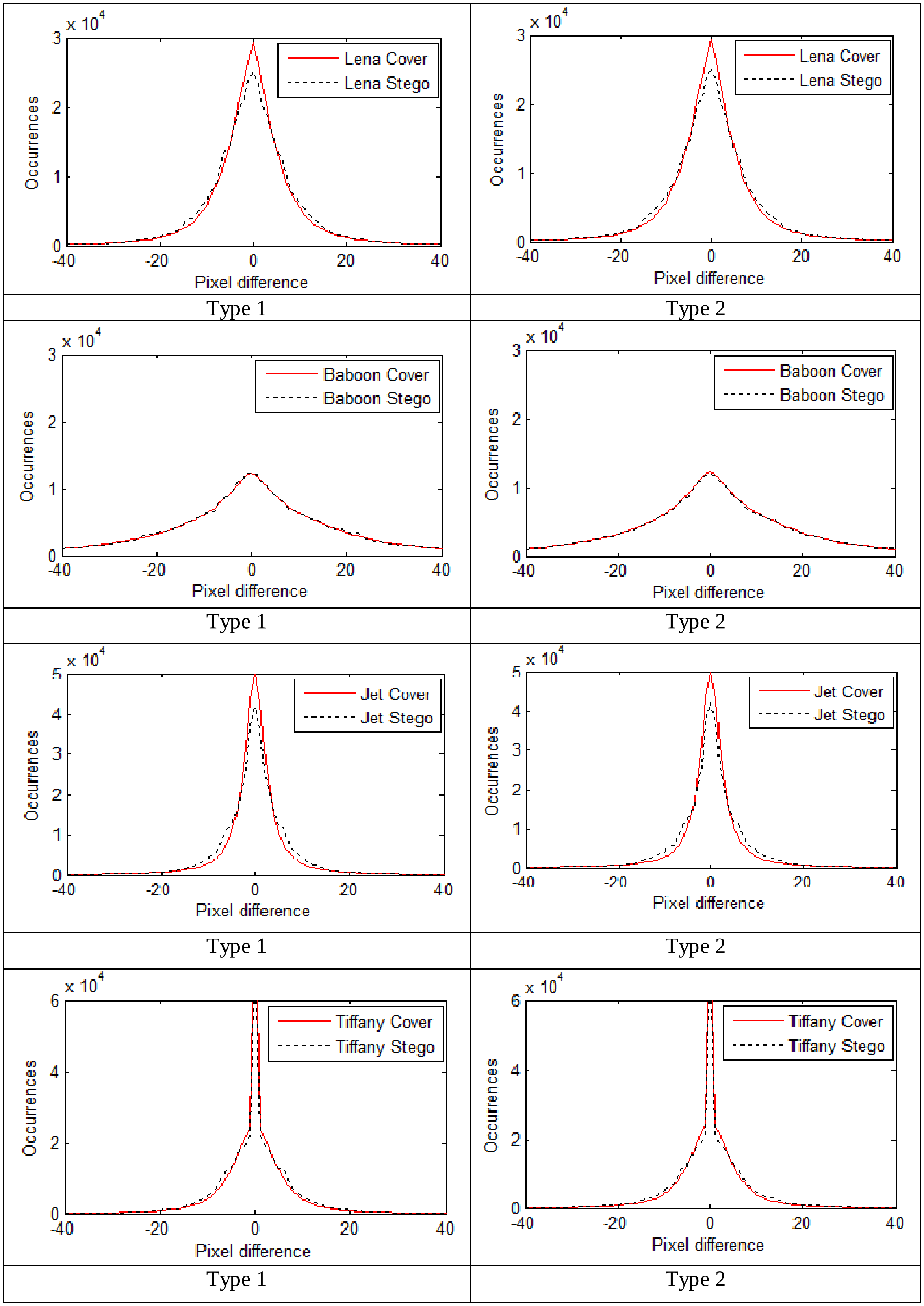
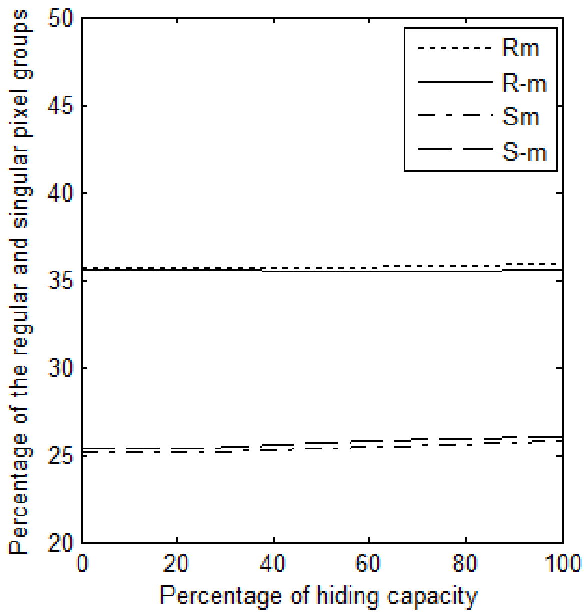
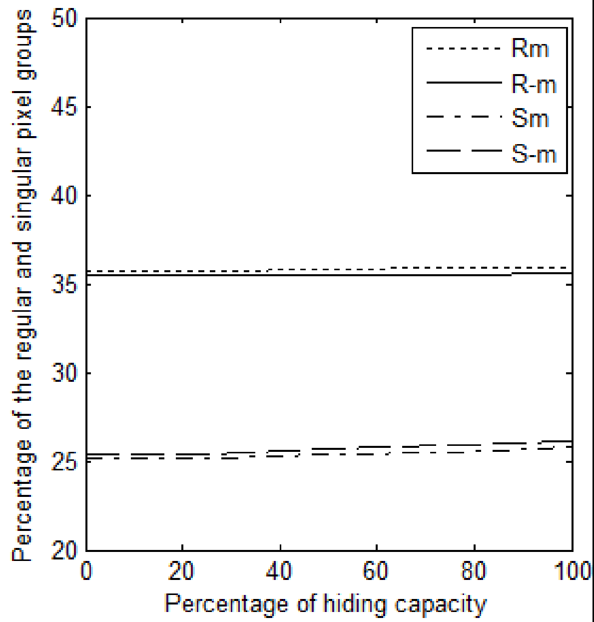


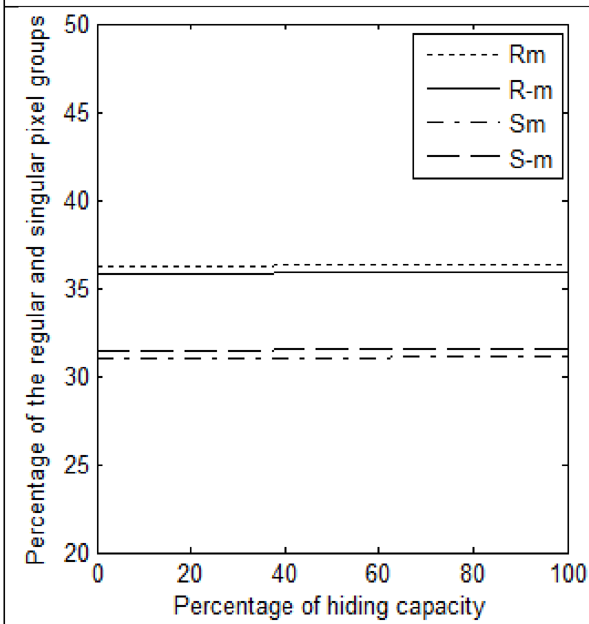
Fig.11 PDH analysis of proposed variant 2: eight directional PVD with modified LSB substitution



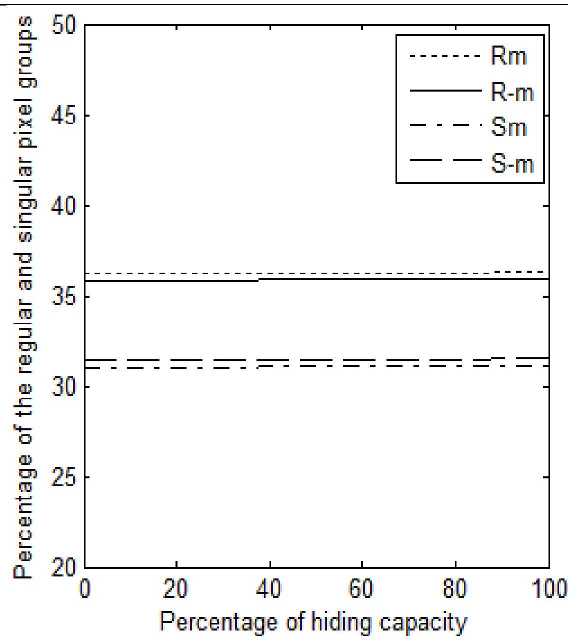
Lena- Type 1



Lena-Type 2



Baboon- Type 1



Baboon- Type 2

Fig.12 RS analysis of Khodaei and Faez's PVD technique over Lena and Baboon images

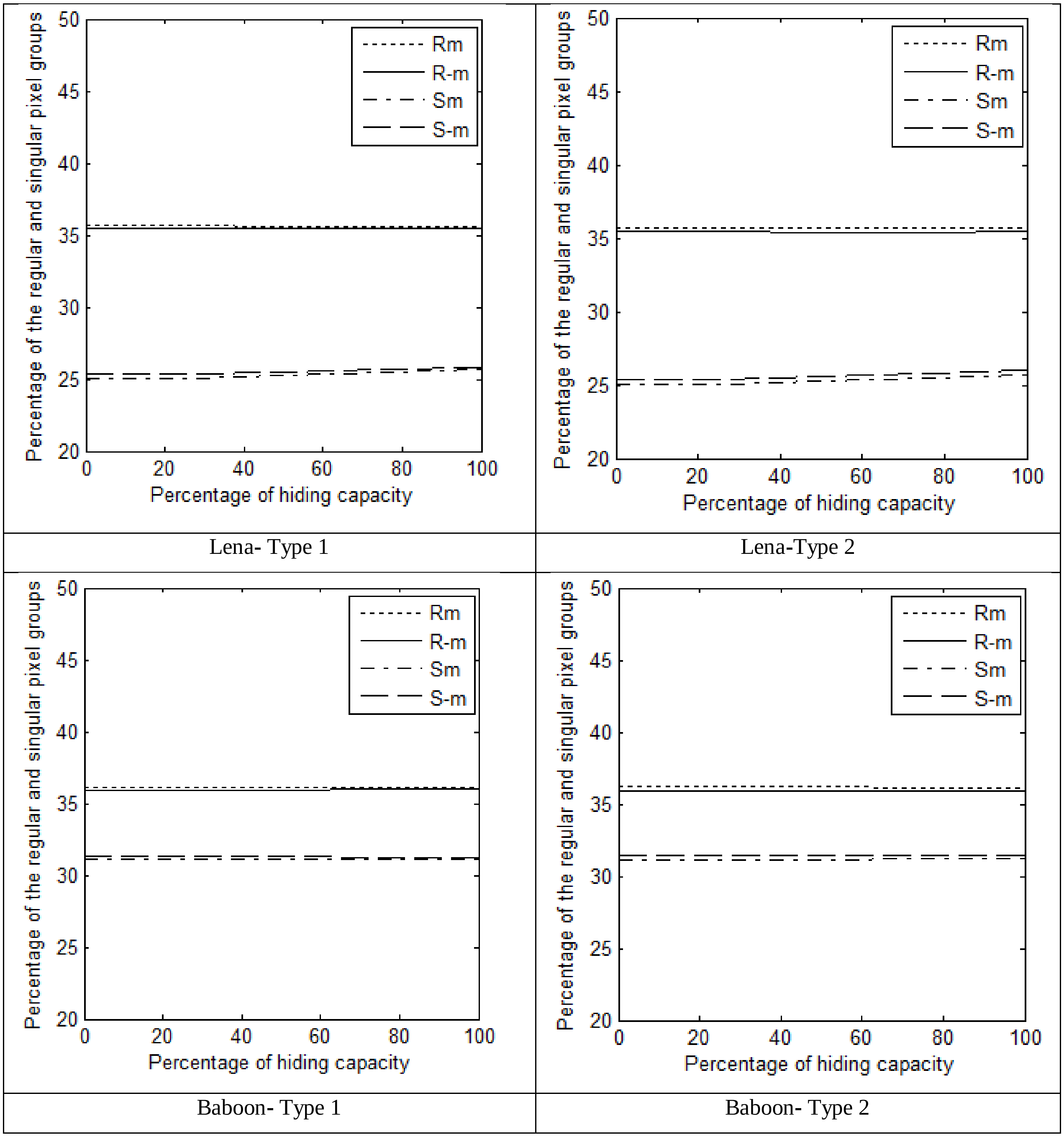


Fig.13 RS analysis of proposed variant 1: five directional PVD with M-LSB substitution over Lena and Baboon images

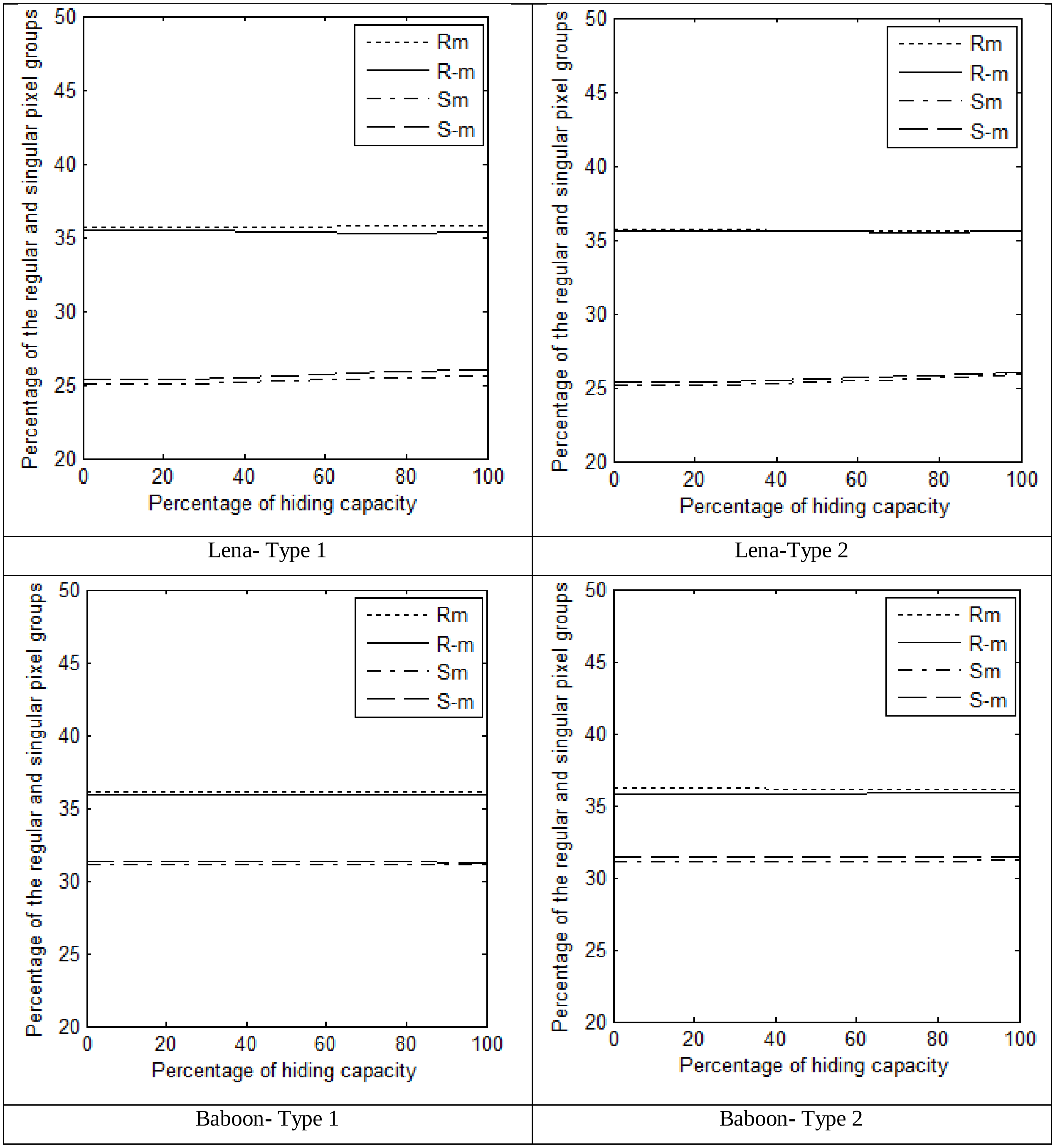


Fig.14 RS analysis of proposed variant 2: eight directional PVD with M-LSB substitution over Lena and Baboon images

5. Conclusion

Steganography techniques, those use the principles of LSB substitution and PVD need to address three issues, (i) fall off boundary problem (FOBP), (ii) pixel difference histogram (PDH) analysis, and (iii) RS analysis. This paper proposes a steganography technique in two variants using LSB substitution and PVD. The first variant operates on 2×3 pixel blocks and the second variant operates on 3×3 pixel blocks. In one of the pixels of a block embedding is performed using modified LSB substitution. Based on the new value of this pixel, difference values with other neighboring pixels are calculated. Using these differences PVD approach is applied. The edges in multiple directions are exploited. So PDH analysis can't detect this steganography. The LSB substitution is performed in only one pixel of the block, so RS analysis also can't detect this steganography. The FOBP is addressed by introducing suitable equations in the embedding procedure. The experimental results such as bit rate and PSNR are satisfactory.

Competing Interests

The author declares that there are no conflicts of interest regarding the publication of this paper.

Acknowledgements

This research is not financially supported by any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

1. D.C. Wu, W.H. Tsai, "A steganograhic method for images by pixel value differencing", Pattern Recognition Letters, vol. 24, no.9, pp.1613-1626, 2003.
2. K.C. Chang, C.P. Chang, P.S. Huang, T.M. Tu, "A novel image steganography method using tri-way pixel value differencing", Journal of Multimedia, vol.3, no.2, pp.37-44, 2008.
3. Y.P. Lee, J.C. Lee, W.K. Chen, K.C. Chang, I.J. Su, C.P. Chang, "High-payload image hiding with quality recovery using tri-way pixel-value differencing", Information Sciences, vol.191, pp.214-225, 2012.
4. C.C. Chang, H.W. Tseng, "A steganographic method for digital images using side match", Pattern Recognition Letters, vol.25, no.12, pp.1431-1437, 2004.
5. C. H. Yang, C.Y Weng, H.K Tso, S.J. Wang, "A data hiding scheme using the varieties of pixel-value differencing in multimedia images", The Journal of Systems and Software, vol.84, pp.669-678, 2011.
6. W. Hong, T.S. Chen, C.W. Luo, "Data embedding using pixel value differencing and diamond encoding with multiple-base notational system", The Journal of Systems and Software, vol.85, pp.1166-1175, 2012.
7. H.C. Wu, N.I. Wu, C.S. Tsai, M.S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEEE Proceedings Vision, Image and Signal Processing, vol.152, no.5, pp.611-615, 2005.
8. C.H. Yang, C.Y. Weng, S.J. Wang, H.M. Sun, "Varied PVD+LSB evading programs to spatial domain in data embedding systems", The Journal of Systems and Software, vol.83, pp.1635-1643, 2010.
9. J. Chen, "A PVD-based data hiding method with histogram preserving using pixel pair matching". Signal Processing, Image Communication, vol.29, pp.375-384, 2014.
10. M. Khodaei, K. Faez, "New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing", IET Image processing, vol.6, no.6, pp.677-686, 2012.
11. X. Liao, Q.Y. Wen, J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB Substitution", Journal of Visual Communication and Image Representation, vol.22, pp.1-8, 2011.
12. G. Swain, "A steganographic method combining LSB substitution and PVD in a block", Procedia Computer Science, vol.85, pp.39-44, 2016.

13. A. Pradhan, K.Raja Sekhar, G. Swain,, "Digital image steganography combining LSB substitution with five way PVD in 2×3 pixel blocks", International Journal of Pharmacy and Technology, vol.8, no.4, pp.22051-22061, 2016.
14. W. Luo, F. Huang, J. Huang, "A more secure steganography based on adaptive pixel-value differencing scheme", Multimedia Tools and Applications, vol.52, pp.407-430, 2010.
15. G. Swain, "Adaptive pixel value differencing steganography using both vertical and horizontal edges", Multimedia Tools and Applications, vol.75, pp.13541-13556, 2016.
16. A. Pradhan, K.R. Sekhar, G. Swain, "Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks", Security and Communication Networks, vol. 2017, pp.1-13, 2017.
17. Chakraborty, A.S. Jalal, C. Bhatnagar, "LSB based non blind predictive edge adaptive image steganography", Multimedia Tools and Applications, vol.76, no.6, pp.7973-7987, 2017.
18. C. Balasubramanian, S. Selvakumar, S. Geetha, "High payload image steganography with reduced distortion using octonary pairing scheme", Multimedia Tools and Applications, vol.73, no.3, pp.2223-2245, 2014.
19. A. Pradhan, K.Raja Sekhar, G. Swain, "Digital image steganography based on seven way pixel value differencing", Indian Journal of Science & Technology, vol.9, no.37, pp.1-11, 2016.
20. K.A. Darabkh, A.K. Al-Dhamari, I.F. Jafar, "A New Steganographic algorithm based on multi directional PVD and modified LSB", Journal of Information Technology and Control, vol.46, no.1, pp.16-36, 2017.
21. X. Zhang, S. Yang, "Efficient steganographic embedding by exploiting modification direction", IEEE Communication Letters, vol.10, no.11, pp.781-783, 2006.
22. C. Kim, "Data hiding by an improved exploiting modification direction", Multimedia Tools and Applications, vol.69, no.3, pp.569-584, 2014.
23. S.Y. Shen, L.H. Huang, "A data hiding scheme using pixel value differencing and improving exploiting modification directions", Computers & Security, vol.48, pp.131-141, 2015.
24. USC-SIPI Image Database. [Online]. Available: http://sipi.usc.edu/database/database.php?volume=misc
25. A. Pradhan, A.K. Sahu, G. Swain, K. Raja Sekhar, "Performance evaluation parameters of image steganography techniques", IEEE International Conference on Research Advances in Integrated Navigation Systems, 2016, doi: 10.1109/RAINS.2016.7764399.