Digital image steganography using LSB substitution, PVD, and EMD

Anita Pradhan, K. Raja Sekhar, Gandharba Swain*

Department of Computer Science and Engineering, K L University, Vaddeswaram-522502, Andhra Pradesh, India

anita.pradhan15@gmail.com, raja.sekhar@owasp.org, gswain1234@gmail.com

*Author for Correspondence

Abstract: To protect from pixel difference histogram (PDH) analysis and RS analysis, two hybrid image steganography techniques by appropriate combination of LSB substitution, pixel value differencing (PVD) and exploiting modification directions (EMD) has been proposed in this paper. The cover image is traversed in raster scan order and partitioned into blocks. The first technique operates on 2×2 pixel blocks and the second technique operates on 3×3 pixel blocks. For each block, the average pixel value difference, d is calculated. If d value is greater than 15, the block is in an edge area, so a combination of LSB substitution and PVD is applied. If d value is less than or equal to 15, the block is in a smooth area, so a combination of LSB substitution and EMD is applied. Each of these two techniques exists in two variants (Type 1 and Type 2) with respect to two different range tables. The hiding capacities and PSNR of both the techniques are found to be improved. The results from experiments prove that PDH analysis and RS analysis can't detect these proposed techniques.

Keywords: data hiding, LSB substitution, PVD steganography, EMD steganography, PDH analysis, RS analysis

1. Introduction

The fundamental principle of a steganography technique is to hide the secret data in image, audio or video files [1]. Data can be hidden in images using spatial domain or frequency domain. LSB substitution is the most common technique of data hiding in spatial domain. But it can be easily detected by RS analysis [2]. To augment security in LSB substitution techniques, some precautionary measures need to be taken. The LSB planes that will carry the secret data can be selected based upon the bit pattern hidden in neighboring pixels [3]. The bits from one or more LSB planes of the pixels can be joined together to make an array. The binary data bits can be concealed in this array at appropriate portions to minimize distortion and to improve the security [4]. The PVD steganography is another familiar data hiding technique [5]. This technique exploits the smooth areas to hide lesser number of secret bits and edge areas to hide more number of secret bits. Many variants of PVD technique has been found in literature. A technique of Khodaei and Faez uses both LSB and PVD concepts [6]. It possesses higher hiding capacity and lesser distortion. The problem in the PVD techniques is that they are attacked by pixel difference histogram (PDH) analysis. One mechanism that addresses this problem is the adaptive range table [7, 8]. Instead of a fixed range table for all the pixels, it can be varied for every pixel. Even the number of LSB bits to be hidden in different pixels can be varied based on the smoothness of the block into which the pixel belongs to [9], so that security can be improved.

Zhang and Wang [10] proposed exploiting modification direction (EMD) steganography. The principal goal in it is that a group of secret bits be converted to a digit in (2n+1)-ary notational system, where n is the size of pixel block. This secret digit could be hidden in the pixel block by adding ±1 to only one pixel. In this technique the hiding capacity is not good. The hiding capacity has been improved in two stage technique in [11] and 8-ary technique in [12]. Lee et al. [13] proposed EMD technique using pixel segmentation. In a pair of pixels, each pixel is segmented into two segments. The MSB segments of the two pixels together is called the vector of coordinates (VCA) and the LSB segments of the two pixels together is called vector modification area (VMA). The bits of VCA decide about embedding. Jung and Yoo [14] proposed an EMD technique in a block of one pixel to increase the hiding capacity. The EMD technique based on diamond encoding also could improve the hiding capacity [15]. Joo et al.'s EMD technique using modulus function preserved the pixel difference histogram [16]. Kim et al. [17] has proposed two EMD techniques, namely EMD-2 and 2-EMD. In EMD-2 technique at most two pixels are modified and in 2-EMD technique, two consecutive EMDs are used. Both these techniques achieve higher hiding capacity. Wang et al. [18] said that a number of pixel groups could be combined to derive more number of embedding directions, so that distortion can be reduced. Kieu and Chang's [19] EMD technique used eight modification directions. It fully exploited all modification directions and measured the hiding capacity and distortion for different values of the parameter, s. Wang et al.'s [20] EMD technique combined multiple groups to hide the data according to a designed switch map, so that the hiding capacity can be increased and distortion can be decreased. Fu et al. [21] used EMD and multilayer embedding mechanism with histogram shifting to achieve reversibility. Kim [22] advanced the EMD technique using basis vector, and $(2^{n+x} - 1)$-ary notational system, where n and x are user defined values. Shen and Huang [23] made the hiding capacity of a block adaptive by using PVD with EMD. This PVD with EMD technique provides higher hiding capacity and better PSNR. To improve upon the security keys are used to generate pseudo random numbers, which can be used to find the embedding locations [25].

It is found that Shen and Huang's [23] PVD with EMD technique is detectable by PDH analysis. To advance further in this paper we judiciously combined LSB substitution, PVD, and EMD techniques to protect against PDH analysis and to possess larger hiding capacity without sacrificing the PSNR. There are two techniques proposed, the first technique is designed using 2×2 pixel blocks and the second technique is designed using 3×3 pixel blocks.

2. The Proposed technique 1 (LSB+PVD+EMD in 2×2 pixel blocks)

2.1 The Embedding Procedure

Step 1: The image is traversed in raster scan order and partitioned into non-overlapping blocks of size 2×2. A sample block is shown in Fig.1(a).

P_c	P_1
P_2	P_3

(a)

p'_c	p'_1
p'_2	p'_3

(b)

p^*_c	p^*_1
p^*_2	p^*_3

(c)

Fig.1. (a) cover pixel block, (b) stego block, and (c) stego block used for extraction

Step 2: For every block the average pixel value difference, $d = \frac{1}{3}\sum_{i=1}^{3}|P_c - P_i|$ is computed. If d is greater than 15, then the block is said to be an edge area, otherwise it is a smooth area.

Step 3: In an edge area embedding is done using LSB substitution and PVD.

Step 4: In a smooth area embedding is done using LSB substitution and EMD.

The LSB+PVD embedding approach: The first LSB of pixel P_c is substituted by bit 1, to act as an indicator during extraction. The other 2 LSBs are substituted by 2 data bits. A new value of this pixel p_c' is obtained. Suppose, the decimal value of the three LSBs of p_c' is s_1 and the decimal value of the three LSBs of P_c is i_1. A difference value $df_1 = i_1 - s_1$ is calculated and p_c' is optimized by equation 1.

$$p_c' = \begin{cases} p_c' + 2^3, & \text{if } df_1 > 2^{3-1} \text{ and } 0 \le (p_c' + 2^3) \le 255 \\ p_c' - 2^3, & \text{if } df_1 < -2^{3-1} \text{ and } 0 \le (p_c' - 2^3) \le 255 \\ p_c', & \text{otherwise} \end{cases} \quad (1)$$

Now calculate three difference values, $d_i = |p_c' - p_i|$ for i = 1, 2, 3. It falls into one of the ranges in range table. Based on the range of d_i, the number of bits to be hidden (n_i) can be decided. Table 1 can be referred as Type 1 and Table 2 can be referred as Type 2. Now convert each n_i bits of confidential data to its decimal value ds_i for i = 1, 2, 3. Then compute the new value for this difference as $d_i' = l_i + ds_i$ for i = 1, 2, 3. Now for each p_i where i = 1, 2, 3, calculate two new values $p_i'' = p_c' - d_i'$ and $p_i''' = p_c' + d_i'$. Select one of these two values as p_i' by applying equation 2.

$$p_i' = \begin{cases} p_i'', & \text{if } |p_i - p_i''| < |p_i - p_i'''| \text{ and } 0 \le p_i'' \le 255 \\ p_i''', & \text{otherwise} \end{cases} \quad (2)$$

Table 1. Range table (Type 1)

Range,$\{l_i, u_i\}$	R_1={0, 7}	R_2={8, 15}	R_3={16, 31}	R_4={32, 63}	R_5={64,127}	R_6={128, 255}
No of bits to be hidden, n_i	3	3	3	3	4	4

Table 2. Range table (Type 2)

Range,$\{l_i, u_i\}$	R_1={0, 7}	R_2={8, 15}	R_3={16, 31}	R_4={32, 63}	R_5={64,127}	R_6={128,255}
No of bits to be hidden, n_i	3	3	4	5	6	6

The LSB+EMD embedding approach: The first LSB bit of pixel p_c is substituted by bit 0, which can act as an indicator during extraction. The other two LSBs of p_c are substituted by two data bits. Thus a new value p_c' of the pixel p_c is obtained. Suppose, the decimal value of the three LSBs of p_c' is s_1 and the decimal value of the three LSBs of P_c is i_1. A difference value $df_1 = i_1 - s_1$ is calculated and p_c' is optimized by equation 1.

Suppose we denote the remaining pixels (p_1, p_2, p_3) by a name p_k, where k = 1, 2, 3. Now apply EMD for each p_k as follows. Each p_k has to hide 2 bits of data. The decimal equivalent of the two data bits is m_k. Now select x from {-3, -2, -1, 0} and calculate $p_k'' = p_k + x$ such that the condition, (p_k'' mod 4 = m_k) satisfies. Similarly select x from {1, 2, 3} and calculate $p_k''' = p_k + x$ such that the condition (p_k''' mod 4 = m_k) satisfies. If for all the three values in list {1, 2, 3}, the condition (p_k''' mod 4 = m_k) does not satisfy then set p_k''' = -10. Now calculate the stego value p_k' for p_k by equation 3.

$$p_k' = \begin{cases} p_k'' , & \text{if } \{(p_k''' < 0 \text{ or } p_k''' > 255) \text{ and } 0 \le p_k'' \le 255\} \text{ or} \\ & \{\, 0 \le (p_k'', p_k''') \le 255 \text{ and } |p_k - p_k''| \le |p_k - p_k'''| \,\} \\ p_k''' , & \text{if } \{(p_k'' < 0 \text{ or } p_k'' > 255) \text{ and } 0 \le p_k''' \le 255\} \text{ or} \\ & \{\, 0 \le (p_k'', p_k''') \le 255 \text{ and } |p_k - p_k'''| \le |p_k - p_k''| \,\} \end{cases} \qquad (3)$$

Thus Fig.1 (b) represents the stego pixel block.

2.2 The extraction procedure

Step 1: The stego image is traversed in raster scan order and partitioned into non-overlapping blocks of size 2×2. Fig.1(c) represents a sample 2×2 stego-pixel block.

Step 2: The LSB bit of p_c^* is checked, if it is 1 then for this block the extraction procedure of LSB+PVD approach is used as follows. The next two LSBs of p_c^* are extracted. Furthermore, the d_i^* = $|p_c^* - p_i^*|$ and s_i^* = d_i^* - l_i for i = 1, 2, 3 are calculated. Where, d_i^* belongs to the range R_i and l_i is the lower bound of this range. Now each of these s_i^* is converted to n_i binary bits. Where n_i is the value corresponding to the same range R_i of d_i^*. Note that the same range table (Table 1 or Table 2) which was used during embedding should be used during extraction.

Step 3: If the LSB bit of p_c^* is 0, then for this block the extraction procedure of LSB+EMD is applied as follows. The next two LSBs of p_c^* are extracted. For all the remaining pixels (p_1^* , p_2^* , p_3^*) the decimal equivalent of the embedded bits, m_k is calculated as $m_k = p_k^*$ mod 4, for k= 1, 2, 3. Now each m_k is converted to 2 binary bits.

3. The Proposed technique 2 (LSB+PVD+EMD in 3×3 pixel blocks)

3.1 The Embedding Procedure

Step 1: The image is traversed in raster scan order and partitioned into non-overlapping blocks of size 3×3. A sample block is shown in Fig.2(a).

P_4	P_3	P_2
P_5	P_c	P_1
P_6	P_7	P_8

(a)

p_4'	p_3'	p_2'
p_5'	p_c'	p_1'
p_6'	p_7'	p_8'

(b)

p_4^*	p_3^*	p_2^*
p_5^*	p_c^*	p_1^*
p_6^*	p_7^*	p_8^*

(c)

Fig.2. (a) cover pixel block, (b) stego block, and (c) stego block used for extraction

Step 2: An average pixel value difference, d = $\frac{1}{8}\sum_{i=1}^{8}|P_c - P_i|$ is calculated.

Step 3: If d value is greater than 15 then a combination of LSB substitution and PVD is applied.

Step 4: If d value is less than or equal to 15 then a combination of LSB substitution and EMD is applied.

The LSB+PVD embedding approach: In the central pixel, P_c 3 LSBs are substituted by 3 data bits. A new value of the central pixel is found. Say it is p'_c. In pixel p_8 the first LSB is substituted by bit 1, which will be used as indicator during extraction procedure. The other two LSBs in it are substituted by two data bits. After substituting, three LSBs, suppose the new value of pixel p_8 is p'_8. The decimal value of the three LSBs of p'_c is s_1 and the decimal value of three LSBs of P_c is i_1. Similarly, the decimal value of three LSBs of p'_8 is s_2 and the decimal value of three LSBs of p_8 is i_2. Now calculate the differences df_1 and df_2 as, $df_1 = i_1 - s_1$ and $df_2 = i_2 - s_2$. Now optimize the values of p'_c and p'_8 using equations 1 and 4 respectively.

$$p'_8 = \begin{cases} p'_8 + 2^3, & \text{if } df_2 > 2^{3-1} \text{ and } 0 \leq (p'_8 + 2^3) \leq 255 \\ p'_8 - 2^3, & \text{if } df_2 < -2^{3-1} \text{ and } 0 \leq (p'_8 - 2^3) \leq 255 \\ p'_8, & \text{otherwise} \end{cases} \quad (4)$$

Now calculate seven difference values, $d_i = |p'_c - p_i|$ for i = 1, 2, …,7. These difference values lie in one of the ranges of the range table. Table 1 can be chosen as Type 1 or Table 2 can be chosen as Type 2. Based on the range of d_i, the number of bits to be hidden (n_i) can be decided from the range table.

Now convert each n_i bits of confidential data to its decimal value ds_i for i = 1, 2, … , 7. Then compute the new values for the seven differences as $d'_i = l_i + ds_i$ for i = 1, 2, …,7. Now for each p_i where i = 1, 2, …,7, calculate two new values $p''_i = p'_c - d'_i$ and $p'''_i = p'_c + d'_i$. Select one of these two values as p'_i by applying equation 2. This p'_i is the stego value of p_i.

The LSB+EMD embedding approach: The first LSB of pixel p_8 is substituted by 0 and the next two LSBs are substituted by two data bits. After embedding, say it is p'_8. The decimal value of the three LSBs of p'_8 is s_2 and the decimal value of three LSBs of p_8 is i_2. Now calculate the difference df_2 as, $df_2 = i_2 - s_2$. Now optimize the value of p'_8 using equation 4.

Suppose we denote the remaining pixels (p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_c) by a name p_k, where k = 1, 2, 3, 4, 5, 6, 7, c. Now apply EMD for each p_k as follows. Each p_k has to hide 2 bits of data. The decimal equivalent of the two data bits is m_k. Now select x from {-3, -2, -1, 0} and calculate $p''_k = p_k + x$ such that the condition, ($p''_k \bmod 4 = m_k$) satisfies. Similarly select x from {1, 2, 3} and calculate $p'''_k = p_k + x$ such that the condition ($p'''_k \bmod 4 = m_k$) satisfies. If for all the three values in list {1, 2, 3}, the condition ($p'''_k \bmod 4 = m_k$) does not satisfy then set $p'''_k = -10$. Now calculate p'_k by equation 3. This p'_k is the stego value of p_k.
Thus Fig.2(b) represents the stego pixel block.

3.2 The extraction procedure

Step 1: The stego image is traversed in raster scan order and partitioned into non-overlapping blocks of size 3×3. Fig.2(c) represents a sample 3×3 stego-pixel block.

Step 2: The LSB bit of p^*_8 is checked, if it is 1 then for this block the extraction procedure of LSB+PVD approach is used as follows. The three LSBs of p^*_c and next two LSBs of p^*_8 are extracted. Furthermore, the $d^*_i = |p^*_c - p^*_i|$ and $s^*_i = d^*_i - l_i$ for i = 1, 2, 3,…,7 are calculated. Where, d^*_i belongs to the range R_i and l_i is the lower bound of this range. Now each of these s_i^* is converted to n_i binary bits. Where n_i is the value corresponding to the same range R_i of d_i^*. Note that the same range table (Table 1 or Table 2) which was used during embedding should be used during extraction.

Step 3: If the LSB bit of p_8^* is 0, then for this block the extraction procedure of LSB+EMD is applied as follows. The next two LSBs of p_8^* are extracted. For all the remaining pixels (p_1^*, p_2^*, p_3^*, p_4^*, p_5^*, p_6^*, p_7^*, p_c^*), the decimal equivalent of the embedded bits, m_k is calculated as $m_k = p_k^* \bmod 4$, for k=1, 2, 3, 4, 5, 6, 7, c. Now each m_k is converted to 2 binary bits.

4. Results and Discussion

The implementation work is done using MATLAB tool and with the RGB color images. The data hiding is performed in Red, Green, and Blue planes separately. It can also be applied on gray scale images. Experiments are done with many images. Few samples are shown here. Fig.3 represents four original samples. Fig.4 and Fig.5 are their stego samples for Type 1 and Type 2 of technique 1 respectively. Fig.6 and Fig.7 are the stego samples for Type 1 and Type 2 of technique 2 respectively. Each stego image has hidden 700000 (seven lakhs) bits of secret data. These stego images look innocuous and no distortion is observable.

(a) Lena (b) Baboon (c) Boat (d) Pot

Fig.3 Original images

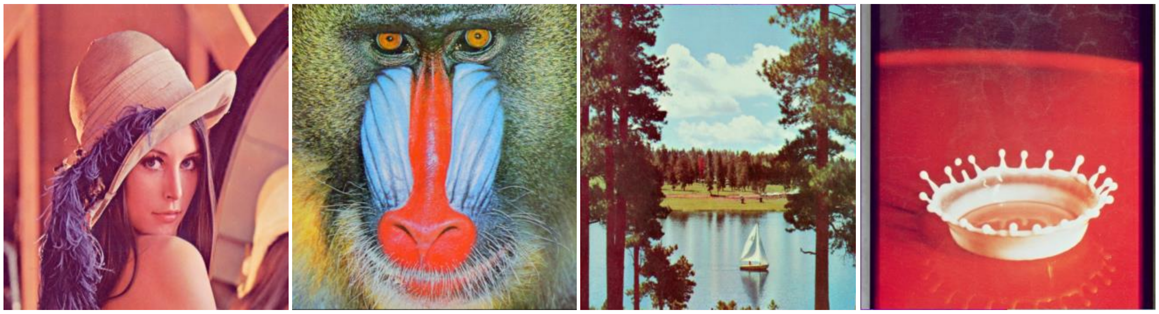


Fig.4 Stego images of technique 1 (Type 1)

Fig.5 Stego images of technique 1 (Type 2)

Fig.6 Stego images of technique 2 (Type 1)

Fig.7 Stego images of technique 2 (Type 2)

In Table 3 the results of Wu & Tsai's PVD technique and Shen & Huang's [23] PVD+EMD technique are given. In Table 4 and Table 5 the results of the proposed technique 1 and technique 2 respectively are given. These results comprises of four parameters, (i) hiding capacity [1], (ii) bits per byte (BPB) [8], (iii) PSNR [1], and (iv) quality index, Q [6].

It can be found from Tables 3, 4 and 5, that the hiding capacity and BPB of proposed technique 1 (Type 1 and Type 2) and technique 2 (Type 1 and Type 2) are significantly enhanced as compared to that of Wu & Tsai and Shen & Huang's techniques. Furthermore, the PSNR of the proposed technique 1 (Type 1 and Type 2) and technique 2 (Type 1 and Type 2) are nearly equal to that of Wu & Tsai and Shen & Huang's techniques.

Table 3. Results of Existing Techniques

Images	Wu & Tsai [5]				Shen & Huang [23]			
512× 512×3	PSNR	Capacity	Q	BPB	PSNR	Capacity	Q	BPB

Lena	43.67	1232606	0.999	1.56	38.01	1223062	0.998	1.55
Baboon	38.40	1403491	0.998	1.78	40.14	1343274	0.999	1.70
Peppers	43.13	1174751	0.999	1.49	41.57	1226139	0.999	1.55
Jet	43.97	1220544	0.999	1.55	43.35	1212350	0.999	1.54
Boat	41.33	1278971	0.999	1.62	41.35	1264742	0.999	1.60
House	41.27	1256404	0.999	1.59	41.75	1242081	0.999	1.57
Pot	44.01	1163700	0.999	1.47	43.38	1195641	0.999	1.52
Average	42.25	1247209	0.999	1.57	41.36	1243898	0.999	1.58

Table 4. Results of Proposed Technique 1

Images	Proposed 3 PVD+ 3 LSB + EMD (Type 1)				Proposed 3 PVD+ 3 LSB + EMD (Type 2)			
512× 512×3	PSNR	Capacity	Q	BPB	PSNR	Capacity	Q	BPB
Lena	44.45	1631063	0.999	2.07	41.33	1687353	0.999	2.15
Baboon	34.85	1898778	0.997	2.41	32.54	2237194	0.994	2.84
Peppers	40.26	1635779	0.999	2.08	38.73	1693901	0.999	2.15
Jet	42.88	1637898	0.999	2.08	42.04	1702029	0.999	2.16
Boat	38.50	1708242	0.999	2.17	36.09	1840256	0.998	2.34
House	40.23	1691500	0.999	2.15	39.18	1808544	0.998	2.30
Pot	46.35	1599030	0.999	2.03	42.80	1622565	0.999	2.06
Average	**41.07**	1686041	0.999	2.14	38.95	**1798834**	0.998	**2.28**

Table 5. Results of Proposed Technique 2

Images	Proposed 7 PVD+ 3 LSB + EMD (Type 1)				Proposed 7 PVD+ 3 LSB + EMD (Type 2)			
512× 512×3	PSNR	Capacity	Q	BPB	PSNR	Capacity	Q	BPB
Lena	44.98	1639022	0.999	2.09	41.26	1690031	0.999	2.15
Baboon	34.67	1987328	0.996	2.54	32.49	2338643	0.994	2.98
Peppers	38.14	1640887	0.998	2.09	34.70	1693278	0.997	2.16
Jet	43.00	1647786	0.999	2.10	40.46	1709098	0.998	2.18
Boat	37.76	1740611	0.998	2.22	34.36	1873870	0.997	2.39
House	40.12	1724458	0.998	2.20	38.79	1841047	0.998	2.35
Pot	43.28	1596123	0.999	2.04	38.80	1617011	0.999	2.06
Average	**40.28**	1710888	0.998	2.18	37.26	**1823282**	0.998	**2.32**

Furthermore, the average performance of the proposed techniques is compared with that of Kieu & Chang's [19] technique. The average BPB and PSNR for the proposed two techniques is as given in Table 6. Similarly the BPB and PSNR of Kieu & Chang's technique for different values of the parameter s is as given in Table 7. By observing Table 6 we can find that in the proposed techniques with BPB values 2.14, 2.18, 2.28 and 2.32, the PSNR values are 41.07, 40.28, 38.95 and 37.26 respectively. By observing table 7 we can find that in the Kieu & Chang's technique with BPB values 1, 2, 3 and 4; the PSNR values are 52.39, 46.74, 40.82 and 34.82 respectively. Thus the PSNR and BPB values of Kieu & Chang's technique (for s=6, BPB=2.5, and PSNR=43.29) are slightly better than that of the proposed techniques (BPB=2.32, and PSNR=41.07). But there is no experimental evidence that Kieu & Chang's technique is undetectable by PDH analysis and RS analysis. The proposed techniques are undetectable by PDH analysis; it is experimentally proved in Fig.9, and Fig.10. It is also proved in Fig.11, and Fig.12 that the proposed techniques are undetectable by RS analysis. PSNR and BPB are not only the measuring parameters; security analysis is also another parameter to be taken into consideration while judging the merit of a steganography technique.

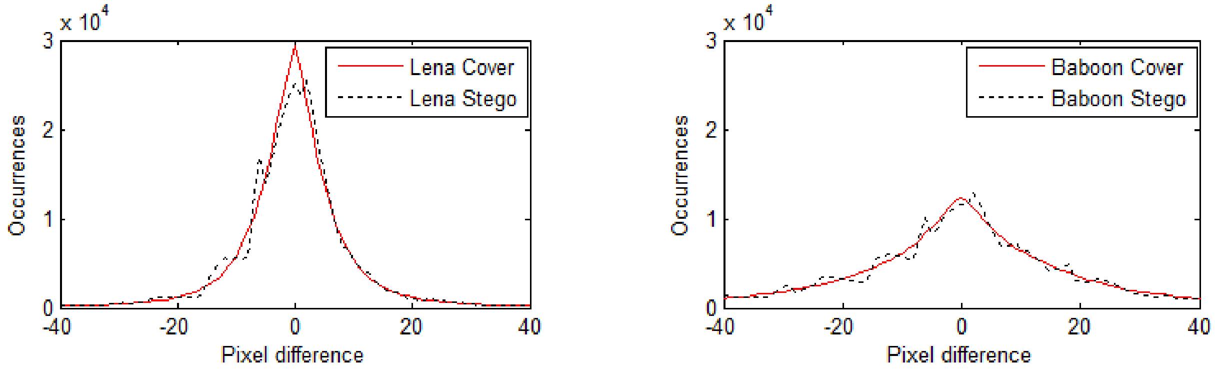
Table 6. Average results of proposed techniques

Type	BPB	PSNR
Proposed 3 PVD+ 3 LSB + EMD (Type 1)	2.14	41.07
Proposed 7 PVD+ 3 LSB + EMD (Type 1)	2.18	40.28
Proposed 3 PVD+ 3 LSB + EMD (Type 2)	2.28	38.95
Proposed 7 PVD+ 3 LSB + EMD (Type 2)	2.32	37.26

Table 7. Average results of Kieu & Chang's technique [19]

S value	BPB	PSNR
2	1	52.39
3	1.5	49.89
4	2	46.74
6	2.5	43.29
8	3	40.82
12	3.5	37.31
16	4	34.82
23	4.5	31.69

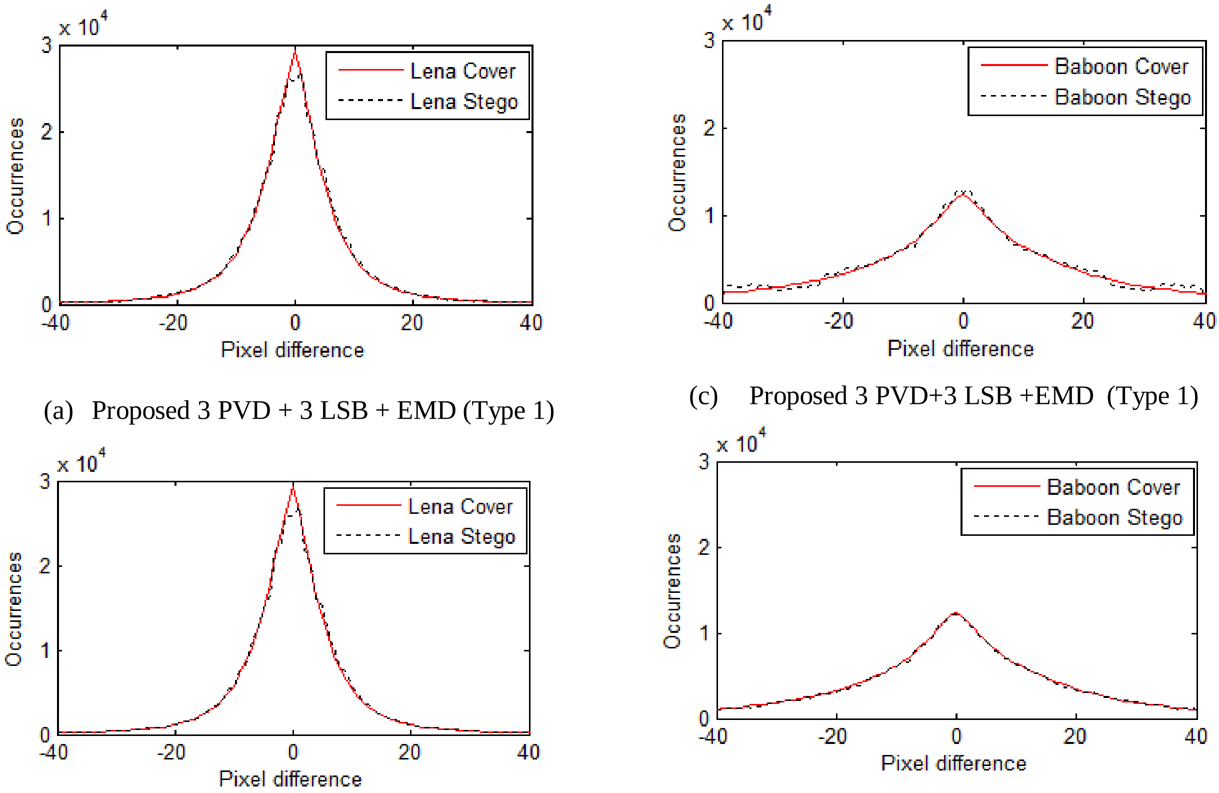
Now let us come to security analysis. The PDH analysis diagrams clearly reveals the step effects in Shen & Huang's technique, Figs.8(a)-(b). Wu & Tsai's technique is also detected by PDH analysis, proved in [24]. But for the proposed techniques, Figs.9(a)-(d) and Figs.10(a)-(d) the step effects are not observable.



(a) Shen & Huang

(b) Shen & Huang

Fig.8 PDH analysis for Shen & Huang's technique



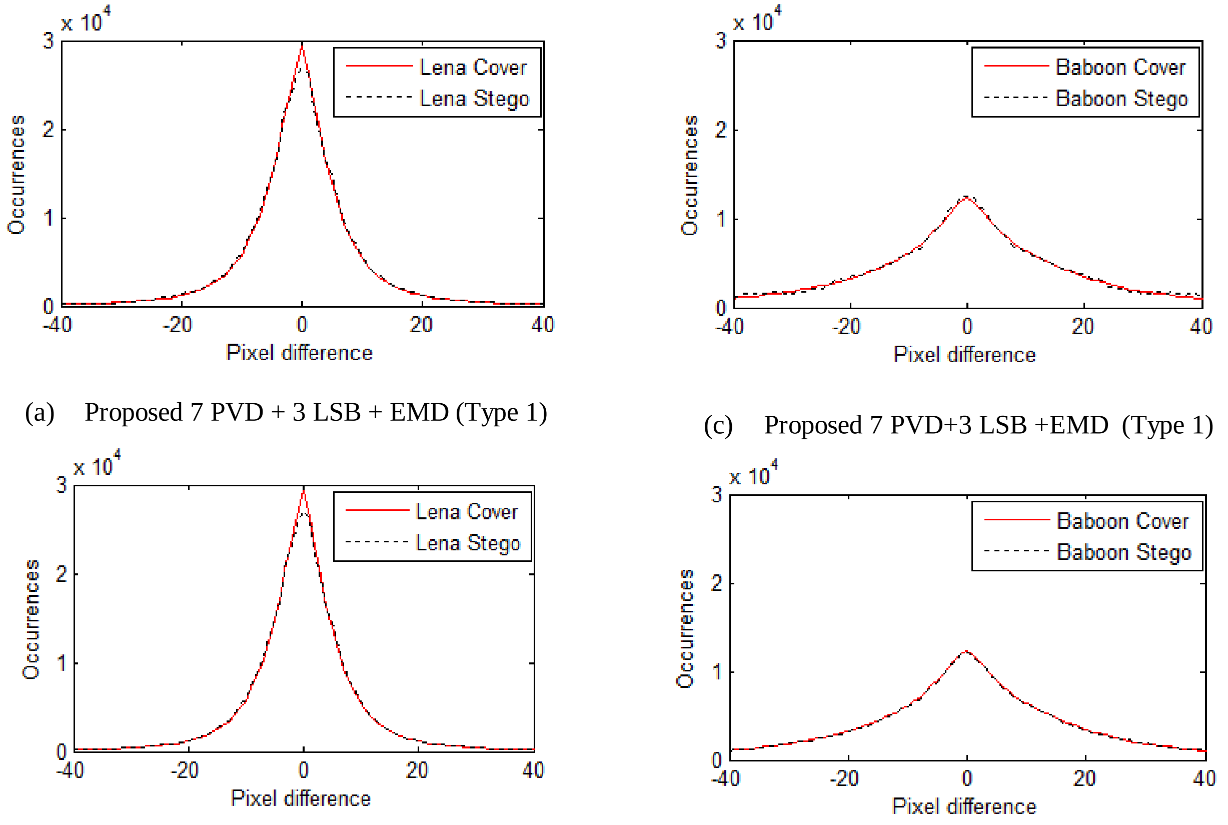
(a) Proposed 3 PVD + 3 LSB + EMD (Type 1)

(c) Proposed 3 PVD+3 LSB +EMD (Type 1)

(b) Proposed 3 PVD + 3 LSB + EMD (Type 2)

(d) Proposed 3 PVD + 3 LSB + EMD (Type 2)

Fig.9 PDH analysis for proposed technique 1 (Type 1 and Type 2)



(a) Proposed 7 PVD + 3 LSB + EMD (Type 1)

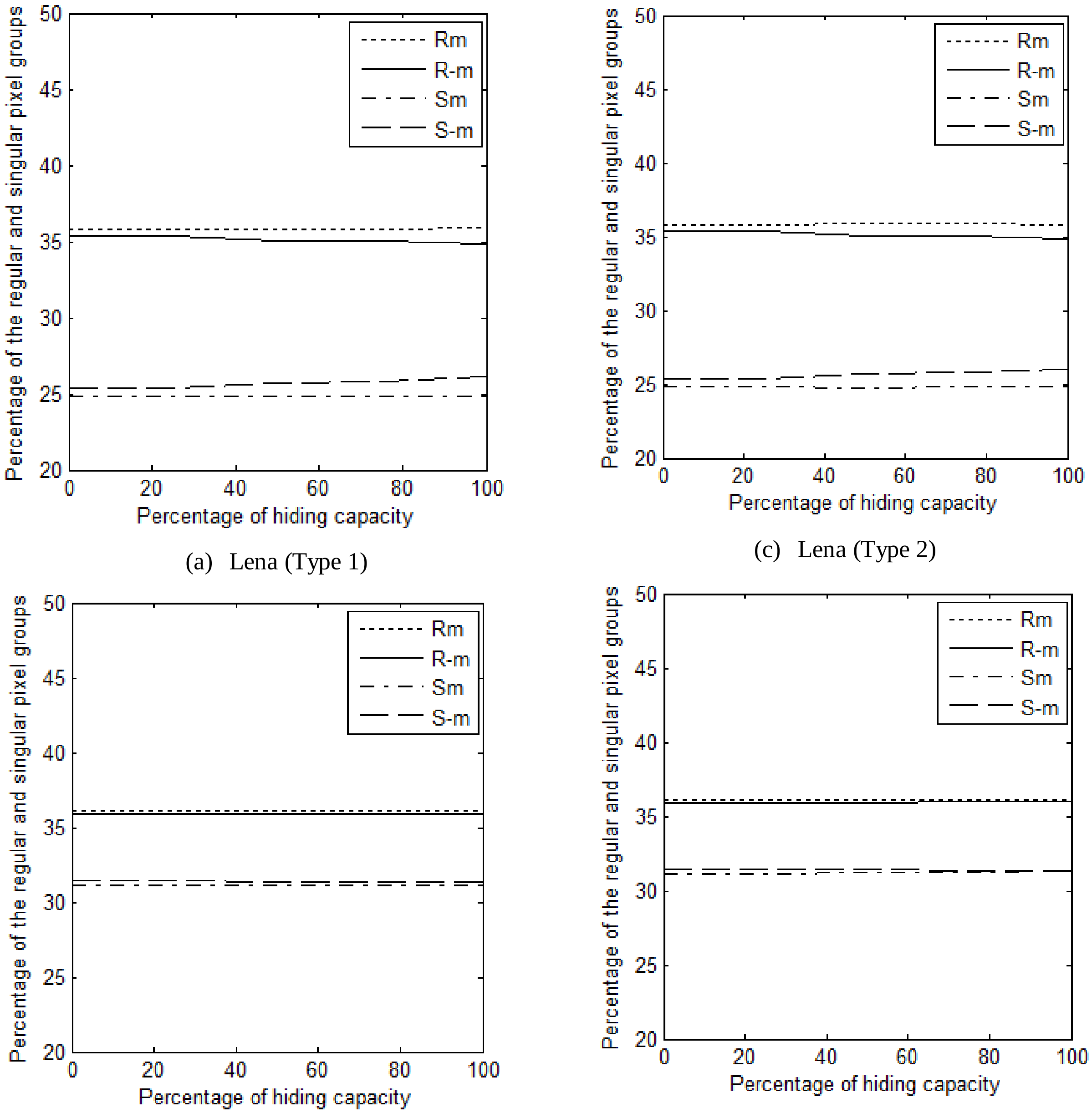
(c) Proposed 7 PVD+3 LSB +EMD (Type 1)

(b) Proposed 7 PVD + 3 LSB + EMD (Type 2)

(d) Proposed 7 PVD + 3 LSB + EMD (Type 2)

Fig.10 PDH analysis for proposed technique 2 (Type 1 and Type 2)

We can observe the RS analysis curves of the proposed technique 1 in Fig.11. In Lena image there are more number of smooth blocks, but in Baboon image there are more number of edge blocks. For Baboon image curves for R_m and R_{-m} are linear and nearly parallel to each other. Similarly, curves for S_m and S_{-m} are linear and nearly parallel to each other. Hence the relation $R_m \cong R_{-m} > S_m \cong S_{-m}$ is strongly satisfied. For Lena image curve for R_m is linear and the curve for R_{-m} is slightly diverging from it. Similarly, curves for S_m is linear and the curve for S_{-m} is slightly diverging from it. Hence the relation $R_m \cong R_{-m} > S_m \cong S_{-m}$ is weakly satisfied for Lena image. Fig.12 represents the RS analysis for technique 2. In all the four cases, the graphs for R_m and R_{-m} are linear, nearly overlap with one another and the graphs for S_m and S_{-m} are linear and nearly overlap with one another. Hence the relation $R_m \cong R_{-m} > S_m \cong S_{-m}$ is strongly satisfied. Hence it can be concluded that RS analysis can't detect the proposed steganography techniques.



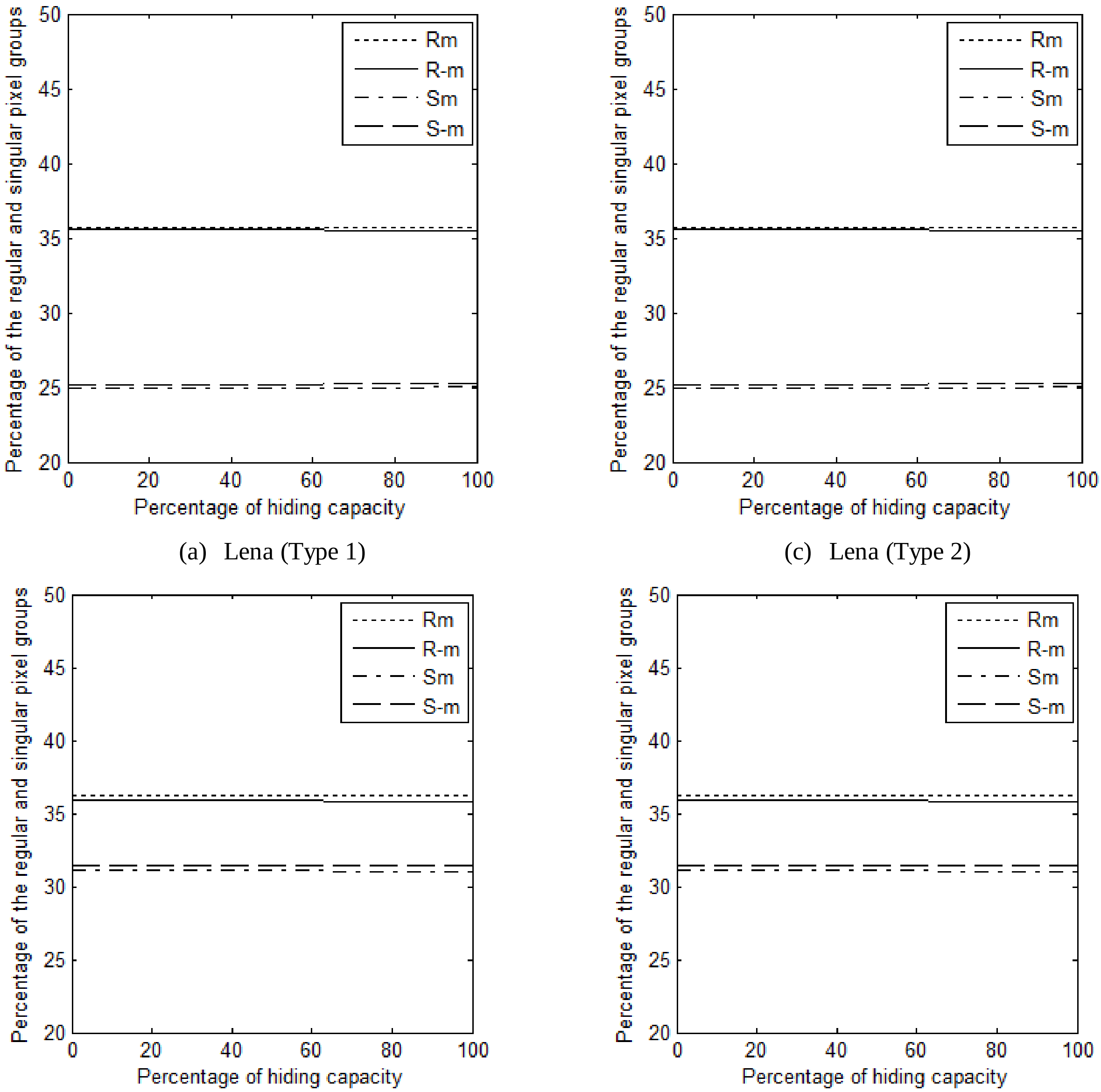
(a) Lena (Type 1)

(c) Lena (Type 2)

(b) Baboon (Type 1)

(d) Baboon (Type 2)

Fig.11 RS analysis for Proposed technique 1 (Type 1 and Type 2)



(a) Lena (Type 1)

(c) Lena (Type 2)

(b) Baboon (Type 1)

(d) Baboon (Type 2)

Fig.12 RS analysis of Proposed for proposed technique 2 (Type 1 and Type 2)

5. Conclusion

Shen & Huang proposed PVD in connection with EMD to achieve greater hiding capacity and higher PSNR. But it is found to be detectable by pixel difference histogram analysis. To fix this problem, a combination of LSB substitution, PVD, and EMD is proposed in this paper. The proposed technique 1 and technique 2 operates on 2×2 and 3×3 pixel blocks respectively, by calculating the average of the pixel value differences. Based on this average value, either PVD or EMD is applied in combination with LSB. Both the techniques give higher hiding capacity compared to that of Shen & Huang's technique. The recorded PSNR values are also as good as that of Shen & Huang's technique. If we compare between the two proposed techniques, then Type 1 of technique 1 is good for

PSNR and Type 2 of technique 2 is good for hiding capacity. It has also been proved that the proposed techniques are not detectable by RS analysis.

References

1. Cheddad A, Condell J, Curran K, Kevitt PM (2010), Digital image steganography survey and analysis of current methods, Signal Processing, 90:727-752
2. Fridrich J, Goljian M, Du R (2001), Detecting LSB steganography in color and gray-scale images, Magazine of IEEE Multimedia Special issue on Security, 8(4):22–28
3. Swain G, Lenka SK (2012), A technique for secret communication by using a new block cipher with dynamic steganography, International Journal of Security and Its Applications, 6(2):1-12
4. Swain G, Lenka SK (2015), A novel steganography technique by mapping words with LSB array, International Journal of Signal and Imaging Systems Engineering, 8(1):115-122
5. Wu DC, Tsai WH (2003), A steganograhic technique for images by pixel value differencing, Pattern Recognition Letters, 24(9-10):1613-1626
6. Khodaei M, Faez K (2012), New adaptive steganographic technique using least-significant-bit substitution and pixel-value differencing, IET Image processing, 6(6): 677-686
7. Luo W, Huang F, Huang J (2010), A more secure steganography based on adaptive pixel-value differencing scheme, Multimedia Tools and Applications, 52:407-430
8. Pradhan A, Sekhar KR, Swain G (2017) Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks, Security and Communication Networks, vol.2017, pp.1-13
9. Liao X, Wen QY, Zhang J (2011), A steganographic technique for digital images with four-pixel differencing and modified LSB Substitution, Journal of Visual Communication and Image Representation, 22:1-8
10. Zhang X, Yang S (2006), Efficient steganographic embedding by exploiting modification direction, IEEE Communication Letters, 10(11):781-783
11. Chang CC, Tai WL, Chen KN (2007), Improvements of EMD embedding for large payloads, IIHMSP, pp.473-476
12. Lee CF, Wang YR, Chang CC (2007), A steganographic technique with high hiding capacity by improving exploiting modification direction, IIHMSP, pp. 497–500
13. Lee CF, Chang CC, Wang KH (2008), An improvement of EMD embedding technique for large payloads by pixel segmentation strategy, Image and Vision Computing, 26:1670-1676
14. Jung KH, Yoo KY (2009), Improved modification direction technique by modulus operation, International Journal of Signal Processing, Image Processing and Pattern, 2(1):79-87
15. Chao RM, Wu HC, Lee CC, Chu YP (2009), A novel data hiding scheme with diamond encoding, EURASIP Journal on Information Security, doi:10.1155/2009/658047
16. Joo JC, Lee HY, Lee HK (2010), Improved steganographic technique preserving pixel-value differencing histogram with modulus function, EURASIP Journal on Advances in Signal Processing, doi:10.1155/2010/49826

17. Kim HJ, Choi Y, Wang S, Zhang X (2010), Improved modification direction techniques, Computers and Mathematics with Applications, 60:319-325
18. Wang J, Sun Y, Xu H, Chen K (2010), An improved section-wise exploiting modification direction technique, Signal Processing, 90:2954-2964
19. Kieu TD, Chang CC (2011), A steganographic scheme by fully exploiting modification directions, Expert Systems with Applications, 38:10648-10657
20. Wang XT, Chang CC, Lin CC, Li MC (2012), A novel multi-group exploiting modification direction technique based on switch map, Signal Processing, 92:1525-1535
21. Fu DS, Jing ZJ, Zhao SG, Fan J (2014), Reversible data hiding based on prediction-error histogram shifting and EMD mechanism, International Journal of Electronics and Communications, 68: 933-943
22. Kim C (2014), Data hiding by an improved exploiting modification direction, Multimedia Tools and Applications, 69:569-584
23. Shen SY, Huang LH (2015), A data hiding scheme using pixel value differencing and improving exploiting modification directions, Computers & Security, 48:131-141
24. Pradhan A, Sekhar KR, Swain G (2016), Digital image steganography based on seven way pixel value differencing, Indian Journal of Science & Technology, 9(37):1-11
25. Soria-Lorente A, Berres B (2017), A secure steganographic algorithm based on frequency domain for transmission of hidden information, Security and Communication Networks, vol.2017, pp.1-14