Indian Journal of Science and Technology, *Vol 7(9), 1444–1450, September 2014*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Digital Image Steganography using Nine-Pixel Differencing and Modified LSB Substitution

Gandharba Swain

Department of Information Technology, GMR Institute of Technology, Rajam-532127, Srikakulam, Andhra Pradesh, India; gswain1234@gmail.com

Abstract

To provide higher embedding capacity without sacrificing the imperceptibility, a novel steganographic technique based on nine-pixel differencing with modified Least Significant Bit (LSB) substitution is proposed. The image is divided into 3×3 non-overlapping blocks. In each block the average difference value is calculated. Based on this value the block is classified to fall into one of the four levels such as, lower, lower-middle, higher-middle, and higher. If a block belongs to lower level then 2-bit LSB substitution is used in it. Similarly, for lower-middle, higher-middle, and higher level blocks 3, 4, and 5 bit LSB substitution is used. After LSB substitution the pixel values are readjusted to minimize distortion such that these modified values do not disturb the embedded bits. The experimental results reveal that the stego-images are imperceptible and hiding capacity is higher.

Keywords: Modified LSB Substitution, Nine-Pixel Differencing, Pixel Value Differencing, Steganography

1. Introduction

Steganography is an art of invisible communication, wherein the secret message is sent through a cover medium like image, audio, and video[1]. Digital Image steganography methods are of two categories such as, (i) spatial domain methods, and (ii) frequency domain methods. The image with which the secret message is transmitted is called as the stego-image. By hiding the secret message inside an image, there will be the change in statistics, but this change should be very less such that the intruder will not suspect it[2]. The Least Significant Bit (LSB) substitution method is the simplest and well known image steganographic method. But it is vulnerable to varieties of attacks. So it is strengthened by making some alterations. The LSBs of the various pixels can be grouped together to form an array and the binary secret message can be embedded at a maximum matching portion of it, so that the distortion will be minimum[3,4]. Pharwaha[5] proposed a Moderate Bit Substitution (MBS) data hiding scheme such that a secret data bit is embedded at a position next to first zero appearing at any of the first three LSB positions in the pixel, but the pixel is avoided if the first three LSBs in it are '111'. This scheme leads to the random selection of bit positions in the given image pixel, so that security is enhanced. If we hide adaptive number of bits in different pixels, then both the security and capacity can be increased[6,7]. Swain and Lenka[8–10] proposed message bit dependent LSB embedding schemes, wherein the embedding locations in a pixel are randomized depending on the bit pattern of the secret data. For smaller size secret messages only the LSBs of brighter and darker pixels can be targeted, so that embedding can be randomized and security can be improved[11,12]. A pixel in a colored image comprises of 3 bytes. The LSB substitution for colored images can be done differently. One of the bytes can be the indicator to indicate the existence of hidden data in other two bytes[13–16].

Wu and Tsai[17] proposed Pixel Value Differencing (PVD) steganography with an idea that more number of bits can be embedded in edge areas compared to smooth areas of the image. This scheme is based on the substitution

**Author for correspondence*

of a pixel value difference by a new difference value in every non-overlapping block of two consecutive pixels. Other improved forms of PVD techniques have also been proposed in literature[18–20]. With a slight modification to these original PVD techniques, the side match techniques based on the correlation of a pixel with its surrounding pixels has also been evolved. Chang and Tseng[21] proposed two-sided, three-sided and four-sided side match methods by exploiting the correlation of a target pixel with its two, three, and four neighboring pixels respectively. PVD techniques with maximum difference of neighboring pixel values have been proposed in[22,23]. The Fall In Error Problem (FIEP) which was observed in Chang and Tseng's method is addressed in[24]. LSB substitution provides high capacity and less distortion, but not secured. PVD techniques provide high security and more distortion. Wu et al.[25] proposed a technique with 2-pixel blocks using PVD and 3-bit LSB substitution to achieve high embedding capacity and more security. But it is observed that this technique enforces 3-bit LSB substitution in almost 90% of the blocks[26]. Furthermore Liao et al.[27] has proposed a modified LSB substitution in 4-pixel blocks after calculating pixel value differences. But the step-6 of the embedding procedure i.e. readjusting procedure, searches the new value of the pixels from a large number of possible values, which is not computationally feasible.

Being inspired by Wu et al.[25] and Liao et al.[27] schemes and to achieve higher capacity and higher security, a steganographic tehnique with nine-pixel differencing and modified LSB substitution has been proposed in this paper.

In section 2 the proposed technique is described. The results are discussed and compared with the results of Wu et al.'s LSB+PVD scheme in section 3. Finally, the paper is concluded in section 4.

2. Nine-Pixel Differencing and Modified LSB Substitution Technique

The image is scanned in raster scan order and is partitioned into non-overlapping blocks consisting 3 × 3 pixels as shown in Figure 1, where $x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7$, and x_8 are the different pixel values.

The average difference value, d of the block is calculated as in equation 1, where x_{min} is the minimum value of x_i, for i = 0, 1, 2, …, 8.

x_0	x_1	x_2
x_3	x_4	x_5
x_6	x_7	x_8

Figure 1. A 3 × 3 sample block.

$$d = \frac{1}{8}\sum_{i=0}^{8} |x_i - x_{min}| \quad (1)$$

If d ≤ 7, then the block belongs to lower-level and 2-bit LSB substitution is applied. If 8 ≤ d ≤ 15, then the block belongs to lower-middle level and 3-bit LSB substitution is applied. If 16 ≤ d ≤ 31, then the block belongs to higher-middle level and 4-bit LSB substitution is applied. If d ≥ 32, then the block belongs to higher level and 5-bit LSB substitution is applied.

Suppose n-bit LSB substitution is applied in a block, where n value is 2, 3, 4, and 5 corresponding to lower, lower-middle, higher-middle, and higher level respectively. The two LSBs of x_8 i.e. 7th and 8th bit locations are reserved to behave as indicator during extraction, but the other bit locations like 4th, 5th, and 6th can be utilized for data embedding if granted as per the block-level. These 7th and 8th bits are set to 00 if the block belongs to lower level. Similarly, these two bits are set to 01, 10, and 11 if the block belongs to lower-middle, higher-middle, and higher level respectively. Thus a block can hide a total of (9 × n – 2) number of bits. Let $y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7$, and y_8 are the new pixel values corresponding to $x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7$, and x_8 respectively.

After applying the n-bit LSB substitution, now the adjustments are applied to y_i, for i = 0, 1…8, as in equation 2 below, to minimize the distortion. Where z_i, for i = 0, 1…8, modified values.

$$z_i = \begin{cases} y_i - 2^n, & \text{if } y_i \geq (x_i + 2^{n-1} + 1 \\ y_i + 2^n, & \text{if } y_i \leq (x_i - 2^{n-1} + 1 \\ y_i, & \text{otherwise} \end{cases} \quad (2)$$

After this adjustment if the z_i value falls off boundary {0, 255}, then the equation 3 is applied to enforce it to fall with in boundary {0, 255}.

$$z_i = \begin{cases} z_i + 2^n, & \text{if } z_i < 0 \\ z_i - 2^n, & \text{if } z_i > 255 \end{cases} \quad (3)$$

Now, the final stego-block comprises of the pixel values z_0, z_1, z_2, z_3, z_4, z_5, z_6, z_7, and z_8 as in Figure 2 corresponding to the original pixel block given in Figure 1.

The extraction procedure is very simple. The stego-image is scanned in raster scan order and is partitioned into non-overlapping blocks consisting 3 × 3 pixels as in embedding. Let s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, and s_8 are the different stego-pixel values and the pixel s_8 is represented by the eight bits as: $s_8 = b_1b_2\, b_3b_4b_5\, b_6b_7b_8$, where each b_i for i = 1, 2... 8 is a bit.

If b_7b_8 is 00, then two LSBs from each of the pixels s_0, s_1, s_2, s_3, s_4, s_5, s_6, and s_7, are extracted and from s_8 nothing is extracted. If b_7b_8 is 01, then three LSBs from each of the pixels s_0, s_1, s_2, s_3, s_4, s_5, s_6, and s_7, are extracted and from s_8 the bit from 6th location, i.e. b_6 is extracted. If b_7b_8 is 10, then four LSBs from each of the pixels s_0, s_1, s_2, s_3, s_4, s_5, s_6, and s_7, are extracted and from s_8 the bits from 5th and 6th locations, i.e. b_5b_6 are also extracted. If b_7b_8 is 11, then five LSBs from each of the pixels s_0, s_1, s_2, s_3, s_4, s_5, s_6, and s_7, are extracted and from s_8 the bits from 4th, 5th and 6th locations, i.e. $b_4b_5b_6$ are also extracted.

z_0	z_1	z_2
z_3	z_4	z_5
z_6	z_7	z_8

Figure 2. The 3 × 3 stego-block.

This proposed scheme differs from Liao et al.[27] scheme in the following points. Firstly, the proposed scheme is based on nine pixel differencing and Liao et al.'s scheme is based on four pixel differencing. Secondly, the proposed scheme adaptively embeds messages using four levels (lower, lower-middle, higher-middle, and higher), where as Liao et al.'s scheme uses only two levels (lower and higher). Thirdly, the sixth step in Liao et al.'s scheme called as "readjustment procedure", searches the new value of the pixels from a large number of possible values, which is not computationally feasible. The readjustment procedure in the proposed scheme is complete different and is as given in equation 2.

3. Results and Discussion

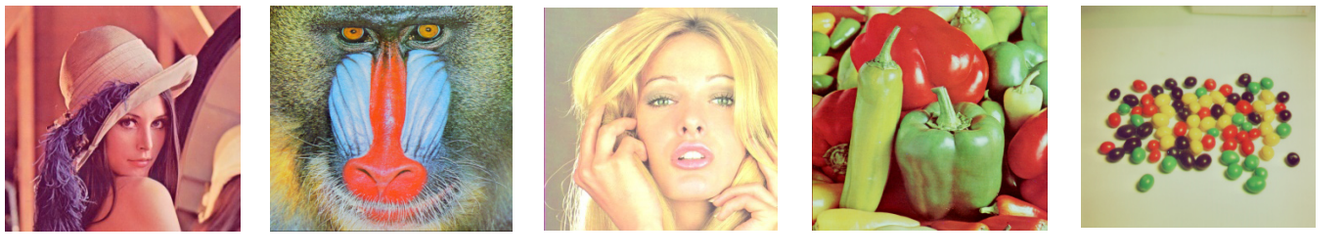
The proposed scheme is implemented using MATLAB. Figure 3 represents a set of original color images of size 256 × 256 and Figure 4 represents the corresponding stego-images with 3,50,000 bits of data hidden in each. Similarly, Figure 5 represents a set of original color images of size 512 × 512 and Figure 6 represents the corresponding stego-images with 14,000,000 bits of data hidden in each.

(a) Girl1 (b) Couple (c) House1 (d) Tree (e) Jelly beans2

Figure 3. Original Images (256 × 256).

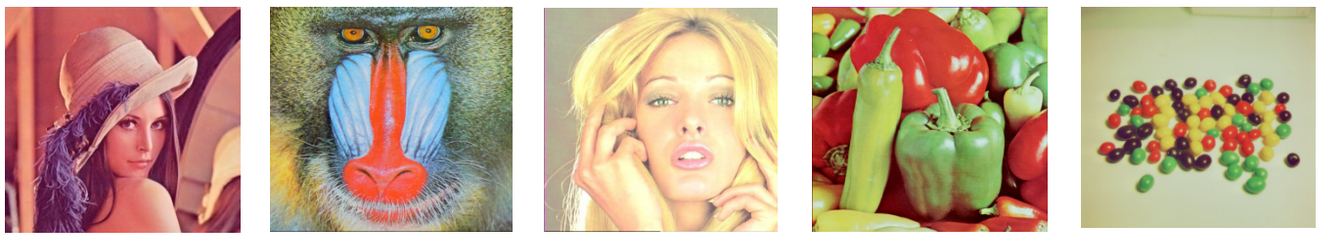
(a) Girl1 (b) Couple (c) House1 (d) Tree (e) Jelly beans2

Figure 4. Stego-images with 3,50,000 bits of data hidden in each.



(a) Lena (b) Baboon (c) Tiffany (d) Peppers (e) pot

Figure 5. Original Images (512 × 512).



(a) Lena (b) Baboon (c) Tiffany (d) Peppers (e) pot

Figure 6. Stego-images with 14,000,000 bits of data hidden in each.

The performance of the proposed scheme is compared with Wu et al.'s LSB+PVD scheme by the parameters, (i) mean square error (MSE), (ii) peak signal-to-noise ratio (PSNR), (iii) correlation, (r), and (iv) capacity. The capacity is measured in bits. A steganography technique should strive for getting higher capacity and lesser distortion. The smaller value of MSE refers to lesser distortion. Unlike MSE the higher PSNR value refers to lesser distortion. The correlation (r) is an estimation of similarity between the cover image and its stego-image. The maximum value of r can be 1, if both cover image and stego-image are the same. Thus a higher value of r implies lesser distortion. The equations to measure MSE, PSNR and correlation are as in[28].

Table 1 represents a comparison between Wu et al.'s scheme with the proposed scheme in terms of MSE, PSNR, r, and capacity. The results for ten test images are as shown in this table. It can be observed from Table 1 that the hiding capacity is larger for the proposed scheme in seven images except the Jelly beans2, Tiffany and Pot. The PSNR value in the proposed scheme is higher in nine images except Baboon. So for the majority of the images the proposed scheme performs better than Wu et al.'s scheme. Furthermore, by taking the average value of the different comparison parameters the following advantages are observed in the proposed scheme. The MSE decreases by 0.5375, which is 8.19%. The increase in PSNR is 0.74, which is 1.83%. The correlation value, r is also increased by 0.0002 and the capacity is increased by 187069 bits, which is 14.66%.

In Table 2 the distribution of PVD and LSB blocks of Wu et al.'s scheme and the distribution of blocks to various levels in the proposed scheme are presented. It can be observed that in Wu et al.'s scheme almost 86.38% of the blocks are using 3-bit LSB substitution. In the proposed scheme only 74.74% of the blocks are using 3-bit LSB substitution. The rest 25.26% of the blocks are using 2-bit, 4-bit and 5-bit LSB substitution. By scattering the distribution of the blocks to these four levels and embedding variable number of bits in the different pixels, the security aspect has been addressed.

It can also be observed from Figure 4 and Figure 6 that the stego-images are of good quality, they do not show any visible marks to be suspected and they are very much similar to their respective original images in Figure 3 and Figure 5.

The proposed scheme can escape from RS steganalysis. In the traditional 1-bit LSB substitution steganography if the LSB of cover image pixel value is equal to the message bit, the pixel value is not altered. Otherwise, the pixel value is altered from 2n to 2n + 1 or from 2n + 1 to 2n. But the alterations from 2n to 2n − 1 or 2n + 1 to 2n + 2 do not occur. This asymmetry could be caught by RS steganalysis. In the proposed scheme n-bit LSB substitution is applied in a block, where n value is 2, 3, 4, and 5 corresponding to lower, lower-middle, higher-middle, and

Table 1. Comparison of MSE, PSNR, r and Capacity

Images	Wu et al.'s LSB + PVD scheme				Proposed scheme			
	MSE	PSNR (dB)	r	Capacity (bits)	MSE	PSNR (dB)	r	Capacity (bits)
Girl1	3.8995	42.22	0.9988	534994	2.9854	43.38	0.9991	569929
Couple	4.8820	41.24	0.9976	532073	3.9785	42.13	0.9980	553882
House1	3.4040	42.81	0.9991	563833	3.2775	42.97	0.9992	571801
Tree	4.6102	41.49	0.9994	468664	4.4748	41.62	0.9994	626638
Jelly beans2	3.1627	43.13	0.9991	554193	2.1138	44.88	0.9994	520483
Lena	7.6717	39.28	0.9979	2111731	5.6115	40.64	0.9984	2297680
Baboon	14.9552	36.38	0.9974	1449956	19.5127	35.22	0.9966	2877658
Tiffany	7.5496	39.35	0.9956	2167738	6.2199	40.19	0.9965	2159377
Peppers	8.1572	39.01	0.9984	2095811	7.2495	39.52	0.9986	2286574
Pot	7.3374	39.47	0.9987	2281844	4.8308	41.29	0.9991	2167504
Average	6.5629	40.44	0.9982	1276083	6.0254	41.18	0.9984	1463152
Improvement					–0.5375	0.74	0.0002	187069

Table 2. Comparison of range counts

Images	Wu et al.'s scheme		Proposed scheme			
	LSB count	PVD count	Lower-level count	Lower-middle level count	Higher-middle level count	Higher-level count
Girl1	88791	9513	761	18102	2152	745
Couple	88645	9659	2339	16690	2025	706
House1	92161	6143	1097	17807	1526	1330
Tree	78110	20194	1147	13762	3373	3478
Jelly beans2	91444	6860	6498	12683	1273	1306
Lena	351487	41729	353	75857	7787	3043
Baboon	241342	151874	12	34124	27834	25070
Tiffany	361289	31927	12428	66191	6261	2160
Peppers	349278	43938	2146	74204	6948	3742
Pot	380305	12911	6229	77129	2079	1603
Average	212285	33474	3301	40654	6125	4318
	86.38%	13.62%	6.07%	74.74%	11.26%	7.93%
	212285 + 33474 = 245759 (100%)		3301 + 40654 + 6125 + 4318 = 54398 (100%)			

higher level respectively. In case of 2-bit LSB substitution if the 2 LSBs of cover image pixel value are equal to the two message bits, the pixel value is not altered. Otherwise the pixel value alters from 2n to {2n + 1 or 2n − 1 or 2n − 2}, or 2n + 1 to {2n or 2n − 1 or 2n − 2} or 2n − 1 to {2n or 2n + 1 or 2n − 2}, or 2n − 2 to {2n or 2n + 1 or 2n − 1}. Note that a pixel value is considered in one of these four ways like {2n, 2n + 1, 2n − 1, 2n − 2}, where n = 1, 2, …, 127. Thus there is no asymmetry as arises in 1-bit LSB substitution. Similarly in 3-bit LSB, 4-bit LSB, and 5-bit LSB substitution also this asymmetry does not occur. From this discussion it is clear that the proposed scheme can escape from RS steganalysis.

4. Conclusion

To achieve higher embedding capacity and lesser distortion an adaptive and modified LSB substitution steganographic scheme has been proposed. The security has been addressed by hiding variable number of bits in different blocks by categorizing the blocks into one of the four levels (lower, lower-middle, higher-middle, and higher) based on average of pixel value differences in nine-pixel blocks. In a majority of the test cases the capacity of the proposed scheme is higher and the distortion is lower as compared to the Wu et al.'s LSB + PVD scheme. The stego-images are imperceptible and do not show any visible marks to draw the attention of the intruders. The extraction can be done very simply by using the two LSBs of the 9^{th} pixel of every 3×3 block.

5. References

1. Cheddad A, Condell J, Curran K, Kevitt PM. Digital image steganography: survey and analysis of current methods. Signal Processing. 2010; 90:727–52.
2. Martin A, Sapiro G, Seroussi G. Is image steganography natural?. IEEE Trans Image Process. 2005; 14(12):2040–50.
3. Juneja M, Sandhu PS. Designing of robust image steganography technique based on LSB insertion and encryption. International Conference on Advances in Recent Technologies in Communication and Computing; 2009 Oct 27–28; Kottayam, Kerala. IEEE; 2009 Nov. p.302–5.
4. Swain G, Lenka SK. LSB array based image steganography technique by exploring the four least significant bits. CCIS. 2012; 270(2):479–88.
5. Pharwaha APS. Secure data communication using moderate bit substitution for data hiding with three layer security. IE(I) Journal-ET. 2010; 91:45–50.
6. He J, Tang S, Wu T. An adaptive steganography based on depth-varying embedding. Congress on Image and Signal Processing. 2008 May 27–28; Sanya, China. IEEE; 2008. p.660–3.
7. Jain YK, Ahirwal RR. A novel image steganography method with adaptive number of least significant bits modification based on private stego-keys. IJCSS. 2010; 4(1):40–9.
8. Swain G, Lenka SK. A robust image steganography technique using dynamic embedding with two least significant bits. Adv Mater Res. 2012; 403-408:835–41.
9. Swain G, Lenka SK. A dynamic approach to image steganography using the three least significant bits and extended hill cipher. Adv Mater Res. 2012; 403-408:842–9.
10. Swain G, Lenka SK. A technique for secret communication by using a new block cipher with dynamic steganography. International Journal of Security and Its Applications. 2012; 6(2):1–12.
11. Swain G, Lenka SK. A hybrid approach to steganography-embedding at darkest and brightest pixels. International Conference on Communication and Computational Intelligence; 2010 Dec 27–29; Erode. IEEE; 2010. p.529–34.
12. Swain G, Lenka SK. Application of a large key cipher in image steganography by exploring the darkest and brightest pixels. Int J Comput Sci Comm. 2012; 3(1):49–53.
13. Parvez MT, Gutub AA. RGB based variable-bits image steganography. IEEE Asia Pacific Services Computing Conference; 2008 Dec 9–12; Yilan. IEEE; 2008. p.1322–7.
14. Tiwari N, Shandilya M. Secure RGB image steganography from pixel indicator to triple algorithm- an incremental growth. International Journal of Security and Its Applications. 2010; 4(4):53–62.
15. Swain G, Lenka SK. A better RGB channel based image steganography technique. CCIS. 2012; 270(2):470–8.
16. Swain G, Lenka SK. A novel approach to RGB channel based image steganography technique. International Arab Journal of e-Technology. 2012; 2(4):181–6.
17. Wu DC, Tsai WH. A Steganographic method for images by pixel-value differencing. Pattern Recogn Lett. 2003; 24:1613–26.
18. Zhang X, Wang S. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recogn Lett. 2004; 25:331–9.
19. Chang KC, Chang CP, Huang PS, Tu TM. A novel image steganographic method using tri-way pixel-value differencing. Journal of Multimedia. 2008; 3(2):37–44.
20. Lee YP, Lee JC, Chen WK, Chang KC, Su IJ, Chang CP. High-payload image hiding with quality recovery using tri-way pixel-value differencing. Inform Sci. 2012; 191:214–25.
21. Chang CC, Tseng HW. A steganographic method for digital images using side match. Pattern Recogn Lett. 2004; 25:1431–7.
22. Pradhan A, Sharma DS, Swain G. Variable rate steganography in digital images using two, three and four neighbor pixels. Indian Journal of Computer Science and Engineering. 2012; 3(3):457–63.
23. Swain G. Steganography in digital images using maximum difference of neighboring pixel values. International Journal of Security and Its Applications. 2013; 7(6):285–94.
24. Swain G, Lenka SK. Steganography using two sided, three sided and four sided side match methods. CSI Transactions on ICT. 2013; 1(2):127–33.
25. Wu HC, Wu NI, Tsai CS, Hwang MS. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEEE Proceedings-Vision, Image and Signal Processing. 2005; 152(5):611–5.

26. Yang CH, Weng CY, Wang SJ, Sun HM. Varied PVD + LSB evading programs to spatial domain in data embedding systems. J Syst Software. 2010; 83:1635–43.
27. Liao X, Wen QY, Zhang J. A steganographic method for digital images with four-pixel differencing and modified LSB Substitution. Journal of Visual Communication and Image Representation. 2011; 22:1–8.
28. Swain G, Lenka SK. Classification image steganography techniques in spatial domain: A study. Int J Comput Sci Eng Tech. 2014; 5(3):219–32.