Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 39 – 44

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

A steganographic method combining LSB substitution and PVD in a block

Gandharba Swain*

Department of Computer Science & Engineering, KL University, Vaddeswaram-522502, India

Abstract

In the recent past some steganography techniques by combining least significant bit (LSB) substitution and pixel value differencing (PVD) have been proposed to improve upon the hiding capacity and peak signal-to-noise ratio (PSNR). This paper proposes a steganographic technique by using both LSB substitution and PVD with in a block. The image is partitioned into 2×2 pixel blocks in a non-overlapping fashion. For every 2×2 pixel block the upper-left pixel is embedded with k-bits of data using LSB substitution. Then the new value of this pixel is used to calculate three pixel value differences with the upper-right, bottom-left, and bottom-right pixels of the block. Then data bits are hidden using these three difference values in three directions. Both horizontal and vertical edges are considered. There are two variants proposed by using two different range tables. In the first variant (Type 1) the PSNR is improved and in the second variant (Type 2) both PSNR and hiding capacity are improved.

Peer-review under responsibility of the Organizing Committee of CMS 2016

Keywords: data hiding, least significant bit substitution, pixel value differencing, steganography

1. Introduction

Steganography is an art of secret data hiding. Its main objective is to send secret data by hiding it in a carrier file like image such that it looks very innocent and not suspected by the intruder. For proposing a steganographic scheme, there are two important properties, (i) hiding capacity, and (ii) un-detectability to be considered. There should be a tradeoff between these two properties. To get more capacity, we have to sacricifice the un-detectibility and vice versa. The image steganography schemes are generally classified into two types, (i) spatial domain schemes, and (ii) frequency domain schemes. In spatial domain the most popular approach is the least signoficant bit (LSB) substitution. The LSB substitution may be extended upto four LSB planes to achieve higher embedding capacity. But it can be captured by the RS-analysis [1] and Chi-square attack [2]. Researchers have been trying to improve the un-detectibility of LSB substitution schemes by adding some flavours to it. In [3] authors have considered the LSBs of the different pixels as an array and embedded the message at a location, where the distortion was minimum. Similarly, in [4] the binary words of the message are hidden at different locations in the LSB array, where the distortion is minimum. The embedding locations (three least significant bit positions) in the different pixels can be randomized based on the binary message [5].

In the smooth areas of the image, the pixel value difference between two adjacent pixels is very small. So this smooth areas can not hide more number of bits. In the edge areas of the image, the pixel value difference between two adjacent pixels is very large, so more number of bits can be hidden. Wu and Tsai [6] partitioned the image into non-overpapping 1×2 pixel blocks by accessing the image in a zig-zag manner. The number of bits that can be hidden in this pair of pixels depends upon the difference value between them. Further, the hiding capacity is improved by considering 2×2 pixel blocks and calculating three directional differences [7, 8].

Corresponding author Tel: +91-9573975571
E-mail address: gswain1234@gmail.com

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.174

But Zhang and Wang [9] found that the PVD technique can be identified using histogram based analysis. In the pixel difference histogram the step effects are detected.

Chang and Tseng [10] proposed another PVD scheme called side match methods, wherein the embedding decision on a target pixel depends on it's neighboring pixel values. This method suffered with fall in error problem (FIEP), as observed by Swain and Lenka [11]. Furthermore, to improve the hiding capacity, the side match methods based upon the maximum difference amongst the neighboring pixel values have been proposed in [12]. Tseng and Leng [13] have proposed a PVD scheme based on perfect square.

LSB substitution scheme possesses higher capacity, but the PVD scheme possesses higher un-delectability. Wu et al. [14] have combined the LSB substitution with PVD to achieve both higher capacity and higher un-delectability. If the pixel value difference is more than 15, they applied PVD scheme, otherwise they applied 3-bit LSB substitution. But, Yang et al. [15] observed that a majority of blocks fall under LSB substitution in Wu et al.'s LSB & PVD approach. Furthermore, they proposed a varied LSB & PVD approach with reduced distortion. Liao et al. [16] categorized the 4-pixel blocks into two levels (low and high), and embedded k-bits in a block using modified LSB substitution approach. This k-value is different for low and high levels. Swain [17] categorized the 3×3 pixel blocks into four levels (lower, lower-middle, higher-middle, and higher) and then applied modified LSB substitution. This technique possesses higher embedding capacity and lesser distortion as compared to Liao et al.'s technique. Luo et al. [18] proposed a PVD technique using 1×3 pixel blocks, with adaptive range calculation. Balasubramanian et al. [19] proposed a PVD scheme with 3×3 pixel blocks using eight directional differences. Chen [20] proposed a PVD technique with 2×2 pixel blocks using two reference tables. Wang et al. [21] proposed a PVD technique using modulus function, wherein they modified the remainder of two consecutive pixels instead of the pixel value difference. They achieved higher embedding capacity and better imperceptibility. Joo et al. [22] observed that, histogram based attacks can detect this technique. So they proposed an improved PVD approach using modulus function. Shen et al. [23] proposed a scheme based on pixel value differencing and exploiting modification directions.

Khodaei and Faez [24] proposed a steganographic technique using LSB substitution and PVD with in a single block. The quantization ranges are divided into two categories, (i) lower level and (ii) higher level. They followed two types of division for hiding the number of bits as per the ranges. In Type 1 division the ranges R_1={0, 7}, R_2={8,15} and R_3={16, 31} are lower level ranges. The ranges R_4={32, 63}and R_5={64, 255} are higher level ranges. The hiding capacities for lower level ranges are 3 bits and higher level ranges are 4 bits. In Type 2 division the ranges, R_1={0, 7}, R_2={8, 15}, R_3={16, 31} and R_4={32, 63} fall in lower level and the range R_5={64, 255} fall in higher level. In Type 2 the number of bits that can be hidden in ranges, R_1, R_2, R_3, R_4 and R_5 are 3, 3, 4, 5 and 6 respectively. The image is scanned in raster scan order and partitioned into 1×3 non-overlapping blocks. For each block the central pixel is P_C, the left pixel is P_L and the right pixel is P_R. In central pixel P_C, k-bits are hidden by using LSB substitution, where k belongs to {3, 4, 5, 6}. Then some optimal adjustment is applied to get the new value, P_C'. Then the difference values $d_1=|P_L - P_C'|$, and $d_2=|P_R - P_C'|$ are calculated. After hiding the secret bits these differences are changed to new difference values and the P_L and P_R values are changed to new values P_L' and P_R' respectively. Thus the stego pixel block is P_L', P_C' and P_R'. In the first variant (Type 1) they got higher PSNR value and in the second variant (Type 2) they got very high embedding capacity. But they did not prove that their technique is not vulnerable to pixel difference histogram analysis.

This paper proposes a steganographic technique using both LSB substitution and PVD in a block of 2×2 pixels. There are two variants like that of Khodaei and Faez's [24] scheme. The proposed variant-1 provides higher PSNR value and the variant-2 provides both higher PSNR and higher capacity as compared to Khodaei and Faez's scheme.

2. The Proposed Technique

2.1 Embedding Process

Step 1- Partition the cover image into 2×2 non-overlapping blocks by scanning the image in a raster scan order. For a 2×2 pixel block as shown in Fig.1(a), the pixels are designated as g_x, g_{ur} , g_{bl} , and g_{br}.

Step 2- The pixel, g_x is embedded with k-bit LSB substitution. The k value is 3. After embedding suppose the new value is g_x'. Suppose the decimal value for the k LSBs is L and the decimal value of k-data bits is S. Then calculate, d=L-S. Now apply the adjustment as below.

$$g_x' = \begin{cases} g_x' + 2^k, & \text{if } d > 2^{k-1} \text{ and } 0 \le g_x' + 2^k \le 255 \\ g_x' - 2^k, & \text{if } d < -2^{k-1} \text{ and } 0 \le g_x' - 2^k \le 255 \\ g_x', & \text{otherwise} \end{cases}$$

Step 3- Calculate differences d_1, d_2 and d_3 as given below.

$$d_1 = |g_x' - g_{ur}|$$

$$d_2 = |g_x' - g_{br}|$$

$$d_3 = |g_x' - g_{bl}|$$

Step 4- The quantization ranges for variant-1 is as in Table 1 and for variant-2 is as in Table 2.

Table 1. Quantization ranges for variant 1 (Type 1)

Range	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	3	3	3	3	4	4

Table 2. Quantization ranges for variant 2 (Type 2)

Range	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	3	3	4	5	6	6

Step 5- Find the ranges R_i to which d_1, d_2 and d_3 belongs to. According to range table, find the t_{i1}, t_{i2}, and t_{i3} which are the number of bits that can be hidden with regard to these ranges and obtain the respective lower bounds, say those are l_{i1}, l_{i2}, and l_{i3}.

Step 6- Now take t_{i1}, t_{i2}, and t_{i3} bits continuously from the binary bit-stream of secret data, convert them to decimal values s_1, s_2, and s_3 respectively. Now calculate, d_1', d_2' and d_3' as below.

$$d_1' = l_{i1} + s_1$$

$$d_2' = l_{i2} + s_2$$

$$d_3' = l_{i3} + s_3$$

Step 7- Calculate the new values g_{ur}'' , g_{ur}''' for g_{ur}. Similarly, g_{br}'' , g_{br}''' for g_{br} and g_{bl}'' , g_{bl}''' for g_{bl} as below.

$$g_{ur}'' = g_x' - d_1'$$

$$g_{ur}''' = g_x' + d_1'$$

$$g_{br}'' = g_x' - d_2'$$

$$g_{br}''' = g_x' + d_2'$$

$$g_{bl}'' = g_x' - d_3'$$

$$g_{bl}''' = g_x' + d_3'$$

Step 8- Now choose the new values as below

$$g_{ur}' = \begin{cases} g_{ur}'' , & \text{if } |g_{ur} - g_{ur}''| < |g_{ur} - g_{ur}'''| \text{ and } 0 \le g_{ur}'' \le 255 \\ g_{ur}''' , & \text{otherwise} \end{cases}$$

$$g_{br}' = \begin{cases} g_{br}'' , & \text{if } |g_{br} - g_{br}''| < |g_{br} - g_{br}'''| \text{ and } 0 \le g_{br}'' \le 255 \\ g_{br}''' , & \text{otherwise} \end{cases}$$

$$g_{bl}' = \begin{cases} g_{bl}'' , & \text{if } |g_{bl} - g_{bl}''| < |g_{bl} - g_{bl}'''| \text{ and } 0 \le g_{bl}'' \le 255 \\ g_{bl}''' , & \text{otherwise} \end{cases}$$

Thus the stego block is as in Fig.1(b).

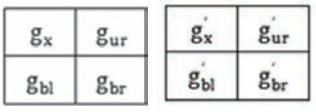

Fig.1 (a) The Original pixel block , (b) The Stego pixel block

2.2 Extraction Process

Partition the stego-image into 2×2 non-overlapping blocks by scanning the image in a raster scan order. Suppose a stego-pixel block at the receiver is as shown in Fig.1(b). Then the extraction process is as given below.

Step 1- Extract the k-rightmost LSBs of g'_x .

Step 2- Calculate the difference values

$d'_1 = | g'_{ur} - g'_x |$

$d'_2 = | g'_{br} - g'_x |$

$d'_3 = | g'_{bl} - g'_x |$

Step 3- Find the ranges R_i to which d'_1, d'_2 , and d'_3 belongs to. Suppose the respective lower bounds are l_{i1}, l_{i2}, and l_{i3}. Now find the t_{i1}, t_{i2}, and t_{i3} values by referring the range table.

Step 4- Calculate the secret bit streams as below.

$s_1 = d'_1 - l_{i1}$

$s_2 = d'_2 - l_{i2}$

$s_3 = d'_3 - l_{i3}$

Now convert s_1, s_2, and s_3 into t_{i1}, t_{i2}, and t_{i3} binary bits respectively.

3. Results and Discussion

The proposed technique is implemented using MATLAB. It is tested with the images from SIPI image database. Two sample cover images are as shown in Fig.2, and after hiding 756035 bits of data, their respective stego-images are as shown in Fig.3 (Type 1) and Fig.4 (Type 2).

(a) Lena (b) Baboon

Fig.2 Original Images

Fig. 3 Stego-images (Type 1)

Fig. 4 Stego-images (Type 2)

In Table 3, the peak signal-to-noise ratio (PSNR) value of the proposed technique is compared with that of Khodaei & Faez's technique. The proposed variant-1 (Type 1) achieves better PSNR (1.6 % increase) as compared to Khodaei & Faez's (Type 1) by sacrificing the capacity (0.7 % decrease) slightly. The proposed variant-2 (Type 2) achieves higher capacity (1.2 % increase) and higher PSNR (2.6 % increase) as compared to Khodaei & Faez's (Type 2). This proves the efficacy of the proposed technique.

The RS-analysis curves for Lena and Baboon images in Type 1 and Type 2 are as shown in Fig.5. The curves for R_m and R_{-m} are straight lines and almost overlap with each other. And the curves for S_m and S_{-m} are straight lines and almost overlap with each other. Thus the relation $R_m \cong R_{-m} > S_m \cong S_{-m}$ is true. Thus we confirm that the RS analysis can not detect the proposed technique.

Table 3. Comparison of the Proposed Technique with Khodaei & Faez's Technique

Images 512×512 (color)	Khodaei & Faez (Type 1), k=3			Proposed (Type 1), k=3			Khodaei & Faez (Type 2), k=3			Proposed (Type 2), k=3		
	PSNR	Capacity	Bit rate	PSNR	Capacity	Bit rate	PSNR	Capacity	Bit rate	PSNR	Capacity	Bit rate
Lena	42.34	2375248	3.02	42.83	2361875	3.00	41.09	2434603	3.09	41.40	2437700	3.09
Baboon	37.59	2443361	3.10	34.98	2393475	3.04	34.31	2662080	3.38	32.76	2772545	3.52
Tiffany	39.30	2372396	3.01	42.52	2363192	3.00	39.87	2416944	3.07	41.98	2425193	3.08
Peppers	39.00	2372858	3.01	39.51	2364428	3.00	37.32	2435223	3.09	38.33	2447737	3.11
Jet	40.50	2374048	3.01	42.31	2365839	3.00	40.65	2418419	3.07	42.51	2443492	3.10
Boat	39.75	2391994	3.04	38.38	2370147	3.01	37.14	2504613	3.18	36.66	2539530	3.22
House	38.91	2387183	3.03	40.13	2366686	3.00	38.42	2470824	3.14	39.19	2510373	3.19
Pot	41.10	2366001	3.00	42.86	2364360	3.00	37.51	2387494	3.03	41.50	2394782	3.04
Average	**39.81**	2385386	3.03	**40.44**	2368750	3.01	**38.29**	**2466275**	3.13	**39.29**	**2496419**	3.17

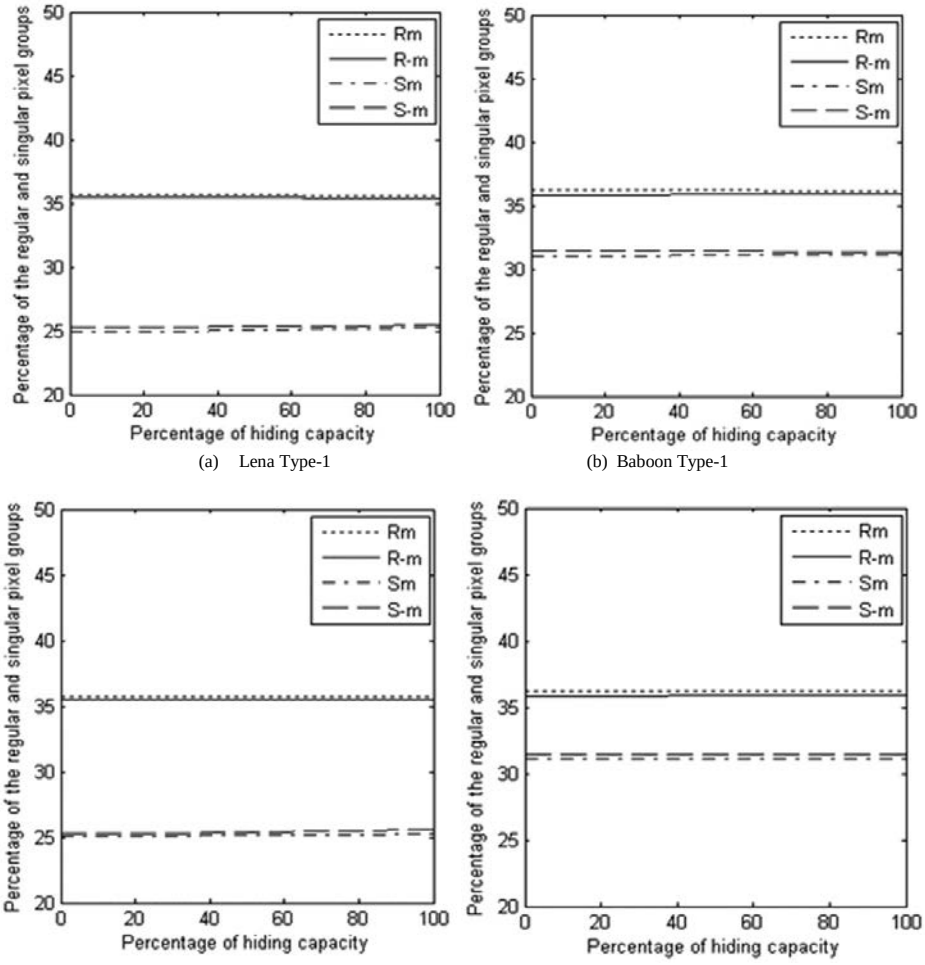

Fig. 5 The RS Analysis curves for Lena and Baboon images

4. Conclusion

A steganographic technique based on LSB substitution and three directional PVD in 2×2 pixel blocks is proposed. There are two variants of this proposed technique. The proposed variant-1 (Type 1) achieves higher PSNR as compared to Khodaei & Faez's technique (Type 1). The proposed variant-2 (Type 2) achieves both higher PSNR and higher capacity as compared to Khodaei & Faez's technique (Type 2). However if we compare the two variants of the proposed technique, then variant-1 is preferable for higher PSNR and the variant-2 is preferable for higher hiding capacity. The extraction process is very simple and does not require the original cover image. This technique can be further extended to 3×3 pixel blocks.

References

1. Fridrich J, Goljian M, Du R. Detecting LSB Steganography in Color and Gray-Scale Images. Magazine of IEEE Multimedia and Security, 2001, p.22-28.
2. Westfeld A, Pfitzmann A. Attacks on steganographic systems. Lecture Notes in Computer Science. 2000, 1768:61-76.
3. Swain G, Lenka SK. LSB array based image steganography technique by exploring the four least significant bits. CCIS, 2012, 270(2): 479-488.
4. Swain G, Lenka SK. A novel steganography technique by mapping words with LSB array. International Journal of Signal and Imaging Systems Engineering. 2015, 8(1/2):115-122.
5. 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.
6. Wu DC, Tsai WH. A steganograhic method for images by pixel value differencing. Pattern Recognition Letters. 2003, 24(9-10):1613-1626.
7. Chang KC, Chang CP, Huang PS, Tu TM. A novel image steganography method using tri-way pixel value differencing. Journal of Multimedia. 2008, 3(2):37-44.
8. 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. Information Sciences. 2012, 191:214-225.
9. Zhang X, Wang S. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognition Letters. 2004, 25:331-339.
10. Chang CC, Tseng HW. A steganographic method for digital images using side match. Pattern Recognition Letters. 2004, 25(12):1431-1437.
11. Swain G, Lenka SK. Steganography using two sided, three sided, and four sided side match methods. CSI Transactions on ICT. 2013, 1(2):127-133.
12. Swain G. Steganography in digital images using maximum difference of neighboring pixel values. International Journal of Security and Its Applications. 2013, 7(6):285-294.
13. Tseng HW, Leng HS. A steganographic method based on pixel-value differencing and the perfect square number. Journal of Applied Mathematics, 2013, article ID 189706.
14. 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): 611-615.
15. Yang CH, Weng CY, Wang SJ, Sun HM. Varied PVD+LSB evading programs to spatial domain in data embedding systems. The Journal of Systems and Software. 2010, 83:1635-1643.
16. 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.
17. Swain G. Digital image steganography using nine-pixel differencing and modified LSB Substitution. Indian Journal of Science and Technology. 2014, 7(9):1444-1450.
18. Luo W, Huang F, Huang J. A more secure steganography based on adaptive pixel-value differencing scheme. Multimedia Tools and Applications. 2010, 52:407-430.
19. Balasubramanian C, Selvakumar S, Geetha S. High payload image steganography with reduced distortion using octonary pixel pairing scheme. Multimedia Tools and Applications. 2013, doi: 10.1007/s11042-013-1640-4.
20. Chen J. A PVD-based data hiding method with histogram preserving using pixel pair matching. Signal Processing: Image Communication. 2014, 29:375-384.
21. Wang CM, Wu NI, Tsai CS, Hwang MS. A high quality steganographic method with pixel-value differencing and modulus function. Journal of Systems and Software. 2008, 81(1):150–158.
22. Joo JC, Lee HY, Lee HK. Improved steganographic method preserving pixel-value differencing histogram with modulus function. EURASIP Journal on Advances in Signal Processing. 2010, doi:10.1155/2010/249826.
23. Shen SY, Huang LH. A data hiding scheme using pixel value differencing and improving exploiting modification directions. Computers & Security. 2015, 48: 131-141.
24. Khodaei M, Faez K. New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. IET Image processing. 2012, 6(6):677-686.