IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 7, Issue 1, Ver. I (Jan. - Feb. 2017), PP 38-43
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

An Improved Adaptive Steganographic Method Based on Least Significant Bit Substitution and Pixel-Value Differencing

Varun sangwan
Sangwan.varun@gmail.com

Abstract: *This paper presents a novel technique for improved data embedding in cover images based on least significant bit and pixel-value differencing. The proposed method is based on the properties of human visual system i.e. eyes can tolerate larger changes in edge areas as compared to smooth areas. Therefore, the method utilizes the HVS concept and hides large amount of secret data in edge areas while less amount of data in smooth areas. The results of the proposed method are verified using extensive simulations.*
Keywords: *pixel-value differencing (PVD), imperceptibility, steganography, PSNR, HVS, least significant bit (LSB) substitution.*

I. Introduction

Steganography is not a new concept. Although the term steganography was coined at the end of the 15th century, it is believed that steganography was first practiced during the Golden Age in Greece. In ancient times, messages were hidden on the wax tables, written on the stomachs of rabbits, or tattooed on the messenger's head [1]. Modern steganography makes use of the digital multimedia files such as audio, video, image etc for data hiding. Images are widely used digital media on the Internet, so most steganographic algorithms are implemented on images. The secret information is embedded into the cover image to obtain the stego image, which is then used for transmission via a public channel [2].

This paper focuses on achieving both high embedding capacity of cover image as well as high image quality. This objective is achieved by making use of two techniques: (i) LSB substitution [3], which belongs to category one, and (ii) PVD [4], which belongs to category two.

The remaining sections of the paper are organized as follows. In section 2, the literature review is described. In Section 3, the proposed method is presented. In section 4, several experimental results are presented to demonstrate the performance of proposed scheme. Finally, conclusions are given in Section 5.

II. Literature Review

2.1 PVD method

In 2003, Wu and Tsai used basic property of HVS system and presented a steganography method using PVD [4]. This method hides different amount of secret bits in consecutive non-overlapping pixel pairs by taking the difference value between the pixels of a pixel pair. This method partitions the given cover image into non-overlappings blocks with two consecutive pixels, say p_i and p_{i+1}.Wu and Tsai designed a range table R_j with ranges varying from 0 to 255. The range table R_j has six ranges as R_1=[0,7], R_2=[8,15], R_3=[16,31], R_4=[32,63], R_5=[64,127] and R_6=[128,255]. The lower bound and upper bound value of each range is given by l_j and u_j. Also, the width of each range is given by $|R_j|$=$u_j - l_j + 1$. The method of hiding secret data into the non-overlapping blocks is as follows:

1. Calculate the difference value between the two pixels of each block, $d_i = |p_i - p_{i+1}|$.
2. Find the range to which the above calculated d_i belongs to.
3. Compute how many bits of secret data can be embedded in each block of pixel pair, $t_j = \lfloor log_2 |R_j| \rfloor$.
4. Read t_j bits from the binary secret data stream and covert into a decimal value s_i.
5. Calculate the new difference value, $d_i^{'} = l_j + s_i$.
6. Modify the pixels p_i and p_{i+1} as,

$$(p_i^{'}, p_{i+1}^{'}) = \begin{cases} \left(p_i + \left\lceil \frac{z}{2} \right\rceil, p_{i+1} - \left\lfloor \frac{z}{2} \right\rfloor\right) \; if \; p_i \geq p_{i+1} \; and \; d_i^{'} > d_i \\ \left(p_i - \left\lfloor \frac{z}{2} \right\rfloor, p_{i+1} + \left\lceil \frac{z}{2} \right\rceil\right) \; if \; p_i < p_{i+1} \; and \; d_i^{'} > d_i \\ \left(p_i - \left\lceil \frac{z}{2} \right\rceil, p_{i+1} + \left\lfloor \frac{z}{2} \right\rfloor\right) \; if \; p_i \geq p_{i+1} \; and \; d_i^{'} \leq d_i \\ \left(p_i + \left\lfloor \frac{z}{2} \right\rfloor, p_{i+1} - \left\lceil \frac{z}{2} \right\rceil\right) \; if \; p_i < p_{i+1} \; and \; d_i^{'} \leq d_i \end{cases} \quad (1)$$

where$z = |d_i - d_i^{'}|$. This process is repeated for each of the block to obtain the stego image.

2.2 PVD and LSB replacement method

In 2005, Wu *et al.* proposed a steganographic method inspired by PVD technique [4]. This method partitions the given cover image into non-overlappings blocks with two consecutive pixels, say p_i and p_{i+1}. Here, the range table R_j with ranges varying from 0 to 255 is divided into 'lower level' and 'higher level'. In case of div=15, lower level contains ranges R_1=[0,7] and R_2=[8,15] while higher level contains ranges R_3=[16,31], R_4=[32,63], R_5=[64,127] and R_6=[128,255]. The lower bound and upper bound value of each range is given by l_j and u_j. Also, the width of each range is given by $|R_j|$=$u_j - l_j + 1$. Now, for each block difference value is calculated as, $d_i = |p_i - p_{i+1}|$.

Case I: If the difference value $d_i$falls in the range of lower level, then LSB substitution method is used to embed 6-bits of secret data. The procedure is as follows:

Let the 6-bits secret data is S=$a_1, a_2, a_3, a_4, a_5, a_6$.

1. Replace 3-LSB of p_i with a_1, a_2, a_3 to obtain $p_i^{'}$.
2. Replace 3-LSB of p_{i+1} with a_4, a_5, a_6 to obtain $p_{i+1}^{'}$.
3. Calculate the new difference value $d_i^{'} = |p_i^{'} - p_{i+1}^{'}|$.
4. If the new difference value falls in the higher level, then perform the readjusting operation.

$$(p_i^{'}, p_{i+1}^{'}) = \begin{cases} p_i^{'} - 8, p_{i+1}^{'} + 8 \;\; if \; p_i^{'} \geq p_{i+1}^{'} \\ p_i^{'} + 8, p_{i+1}^{'} - 8 \;\; if \; p_i^{'} < p_{i+1}^{'} \end{cases} \quad (2)$$

Case II: If the difference value d_i falls in the higher level range then PVD method is used to embed secret data bits in pixel pairs.

2.2Adaptive PVD and LSB replacement method

Khodaei and Faez proposed a method for data hiding in 2012 based on optimum pixel adjustment process (OPAP) and PVD [5]. In this method,the cover image is divided into consecutive non-overlapping blocks of size 1×3 in raster scan manner. Each block $B_i$has a centre pixel named as base pixel p_{ic}. The following steps perform data embedding in each block:

1. Consider k-rightmost LSBs of p_{ic} and transform these three LSBs to a decimal value, say LSB_i. Read k-bits from binary secret data in continuation and replace the k LSBs of p_{ic} with these binary secret data bits to obtain $p_{ic}^{'}$. Also, transform these bits to a decimal value, say s_{ic}.
2. Compute the difference value $d$using $d = LSB_i - s_{ic}$.
3. Modify $p_{ic}^{'}$ using OPAP as follows:

$$p_{ic}^{'} = \begin{cases} p_{ic}^{'} + 2^k \; if \; d > 2^{k-1} \; and \; 0 \leq p_{ic}^{'} + 2^k \leq 255 \\ p_{ic}^{'} - 2^k \; if \; d < -2^{k-1} \; and \; 0 \leq p_{ic}^{'} - 2^k \leq 255 \\ p_{ic}^{'} \qquad otherwise \end{cases} \quad (3)$$

4. Compute the absolute difference values between the base pixel and other pixels of the block by using

$$d_{ij} = \left|p_{ij} - p_{ic}^{'}\right| \; ; \; (i,j) \neq (1,2) \quad (4)$$

where$i$ and $j$denotes the location of the pixel in a block.

5. Assign the ranges corresponding to the differences found in Step 4 and obtain the lower bounds too i.e. l_{ij}. Accordingly, calculate t_{ij} which denotes the number of bits to be concealed into first and third pixels of the block.
6. Read t_{ij} bits in continuation from the binary secret message and transform these bit-sequences into decimalvalues, say s_{ij} . Now, compute the new difference values using

$$d_{ij}^{'} = l_{ij} + s_{ij} \quad (5)$$

7. Calculate the two new values of each pixel of a block using

$$p_{ij}^{''} = p_{ic}^{'} - d_{ij}^{'}$$

$$p_{ij}^{'''} = p_{ic}^{'} + d_{ij}^{'} \quad (6)$$

8. Choose the best new value for these pixels from the values obtained in Step 7 using

$$p_{ij}^{'} = \begin{cases} p_{ij}^{''} & if \left|p_{ij} - p_{ij}^{''}\right| < \left|p_{ij} - p_{ij}^{'''}\right| \; and \; 0 \le p_{ij}^{''} \le 255 \\ p_{ij}^{'''} & otherwise \end{cases} \quad (7)$$

Repeat the above procedure for each block B_i of the cover image so as to obtain the final stego image.

III. Proposed work

This section presents a method, which utilizes LSB substitution and PVD techniques for data hiding. The method consists of three phases: (i) range division phase, (ii) embedding phase and (iii) extracting phase. These phases are presented in next subsections.

3.1 Range division phase

Prior to embedding the secret message, the grey level range [0,255] is divided into five ranges IR_n $(n = 1, \ldots, 5)$ where $IR_n = [l_n, u_n]$, l_n denotes the lower bound of the range IR_n and u_n denotes the upper bound of the range IR_n. These five ranges can be $IR_1 = [0,7]$, $IR_2 = [8,15]$, $IR_3 = [16,31]$, $IR_4 = [32,63]$ and $IR_5 = [64,255]$. Fig. 1 shows the dividing case i.e. div=15 for the proposed method. It divides the range [0,255] into 'lower level' which consist of ranges $IR_1 = [0,7]$, $IR_2 = [8,15]$ and 'higher level' which include ranges$IR_3 = [16,31]$,$IR_4 = [32,63]$, $IR_5 = [64,255]$. Let t_n are the number of bits to be embedded in the pixels falling under the range R_n. According to HVS, changes in edge areas are less visible than smooth areas and hence, more data can be embedded in edges. In the proposed method, first two ranges (IR_1, IR_2) fall under the category of smooth regions whereas last threeranges (IR_3, IR_4, IR_5) falls in the edge regions. Therefore, we propose to embed 3 bits in the lower level and 4 bits in the higher level.

Lower-level		Higher-level		
IR_1=[0,7]	IR_2=[8,15]	IR_3=[16,31]	IR_4=[32,63]	IR_5=[64,255]

Fig.1 The dividing case (div=15) of the proposed method with 'lower level' and higher level'

3.2 Embedding phase

Initially the cover image is divided into non-overlapping blocks having four consecutive pixels each, in raster scan manner. So, each block consists of four pixels. The data embedding will be performed in second and third pixel first and then in third and fourth pixel. The following steps perform data embedding in each block:

1. The secret data will be embedded into the second and third pixel say, $p_{i2}$and p_{i3}using PVD –LSB method as described in section 2.2. After data embedding we will get new pixels $p_{i2}^{'}$ and $p_{i3}^{'}$.
2. Now , data embedding in remaining pixels of the block will take place using adaptive PVD-LSB replacement method as mentioned in section 2.3. Compute the absolute difference between first pixel $p_{i1}$and $p_{i2}^{'}$say, d_i and the absolute difference between fourth pixelp_{i4} and $p_{i3}^{'}$say, d_{i+1}.
3. Assign the ranges corresponding to the differences found in Step 2 and obtain the lower bounds too i.e. l_i and l_{i+1} Accordingly, calculate $t_i$and t_{i+1}which denotes the number of bits to be concealed.
4. Read $t_i$and t_{i+1} bits in continuation from the binary secret message and transform these bit-sequences into decimalvalues, say $s_i$and s_{i+1} . Now, compute the new difference values using

$$d_i^{'} = l_i + s_i$$
$$d_{i+1}^{'} = l_{i+1} + s_{i+1} \quad (8)$$

5. Calculate the two new values of first and fourth pixel of a block using

$$p_{i1}^{''} = p_{i2}^{'} - d_i^{'}$$
$$p_{i1}^{'''} = p_{i2}^{'} + d_i^{'}$$
$$p_{i4}^{''} = p_{i3}^{'} - d_{i+1}^{'}$$
$$p_{i4}^{'''} = p_{i3}^{'} + d_{i+!}^{'} \quad (9)$$

6. Choose the best new value from step 5 using

$$p_{i1}^{'} = \begin{cases} p_{i1}^{''} & if |p_{i1} - p_{i1}^{''}| < |p_{i1} - p_{i1}^{'''}| \; and \; 0 \le p_{i1}^{''} \le 255 \\ p_{i1}^{'''} & otherwise \end{cases}$$

$$p_{i2}^{'} = \begin{cases} p_{i2}^{''} & if|p_{i2} - p_{i2}^{''}| < |p_{i2} - p_{i2}^{'''}| \; and \; 0 \le p_{i2}^{''} \le 255 \\ p_{i2}^{'''} & otherwise \end{cases} \quad (10)$$

Repeat the above procedure for every block of the cover image so as to obtain the final stego image.

3.3 Extracting phase

In this part the secret data is obtained from the stego image. The stego image is partitioned into non-overlapping block of size 1x4 and then for the complete extraction of the secret message following steps are executed.

1. The data is extracted from the second and third pixel of the block first. Compute the difference between the two pixel values say $d_i^{'}$. If the difference lies in lower level of the range table then read three LSB bits from both pixels and concatenate the data bits and call it s_{ic}.
2. If the difference lies in the higher level then find out the difference between the lower bound of corresponding range and $d_i^{'}$, call it *b.* Find out *t* i.e. number of concealed bits and covert *b* into *t* number of bits. This string of bits is say, s_{ic}.
3. Calculate the absolute difference valuesbetween the 1st& 2nd pixel and 3rd&4th pixels of a block and find the range to which these difference values belong to. Then, obtain the lower bound $l_i$and $l_{i+1}$of the corresponding range and also determine the number of bits $t_i$and $t_{i+1}$to be extracted from each pixel.
4. Obtain the secret data sub-streams as $s_{i1}$and $s_{i2}$by taking the difference between above calculated difference values and respective lower bounds. Transform $s_{i1}$and s_{i2} to binary strings with length equivalent to$t_i$and t_{i+1}.

Finally, concatenate s_{ic} ,$s_{i1}$and $s_{i2}$to obtain the original bit sequence of the secret message.

IV. Experimental Results

This section presents the experimental results of the proposed method. The test images used for verifying the results are greyscale images of size 512X512, namely 'Lena', 'Baboon', 'Boat' and 'Peppers'. For the performance evaluation of any steganography method, the three main criteria can be used:

(i) *Capacity*: Capacity is defined as the maximum amount of secret message that can be stored in a cover image [6].

(ii) *Imperceptibility*: It defines the similarity between the cover image and the stego image. The value of PSNR is used to define imperceptibility and is given by:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - Y(i,j))^2 \quad (11)$$

$$PSNR = 10log_{10}\left(\frac{Max^2}{MSE}\right) \quad (12)$$

where MxN denotes the size of the cover image I and stego image Y. A high PSNR value means good quality of stego image whereas a low PSNR means the opposite[7] [8][9].

(iii) *Robustness*: Robustness is the property that provides the resistance against elimination of secret information from the stego image. It can be examined through steganalysis. Various steganalytic methods have been developed to detect the hidden message from the cover media [10][11][12][13].

Fig. 2 shows the changes are unobservable even after large data embedding in the cover image. Hence, the proposed method provides good image quality. Imperceptibility of the proposed method is governed by Table 1, which shows the good PSNR value in comparison to PVD-LSB method. Also, the embedding capacity is higher as compared to PVD-LSB method.The graph in Fig 3.shows the changes that occur in histogram due to data embedding [9]. It is clear from the fig. 3 that proposed method induces less uncompensated change in the histogram and therefore is more secure than PVD-LSB method.

(a) **(b)**

Fig. 2. (a) standard cover images (b) stego images embedded with data using proposed method.

Cover images	Method	Embedding capacity (bits)	PSNR (db)	Robustness
Lena	PVD-LSB	766,040	36.16	Less
	Proposed	777,255	36.5076	More
Peppers	PVD-LSB	770,248	35.34	Less
	Proposed	77,8591	35.2305	More
Baboon	PVD-LSB	717,848	32.63	Less
	Proposed	768,538	33.1523	More
Boat	PVD-LSB	756,768	33.62	Less
	Proposed	776,904	33.9226	More

Table 1. Comparison of the results between PVD-LSB and proposed method.

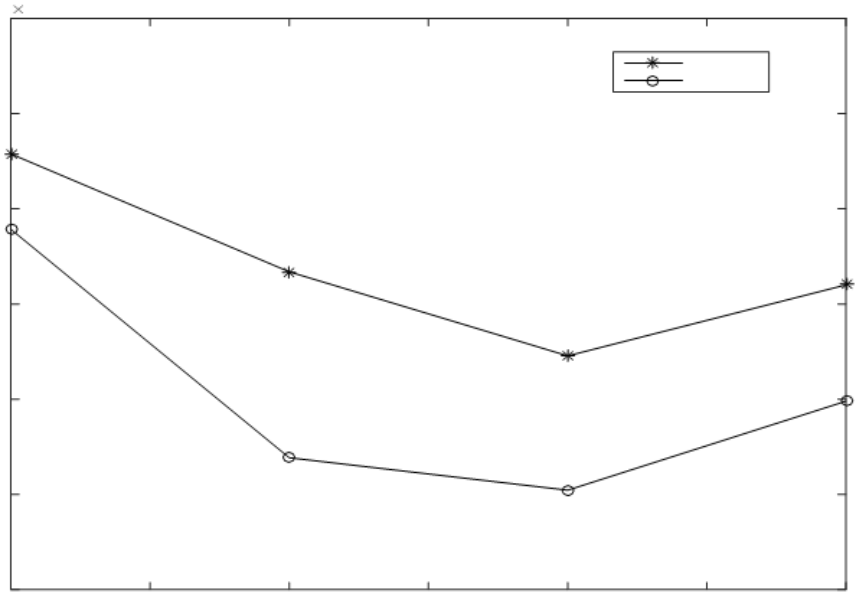

Fig. 3. Uncompensated changes in histogram after embedding via proposed method and PVD- LSB method.

V. Conclusions

In this paper, a histogram preserving data hiding method is presented which is based on LSB substitution and PVD. This method can hide large amount of secret data as well as provide an imperceptible stego image quality while compensating for the dissimilarity between the histograms of the cover and stego images. This advantage of keeping the change in image histogram within permissible limit helps the proposed method to show better resistance against histogram based steganalysers.

References

[1]. F. Petitcolas, R. Anderson, M. Kuhn, "Information hiding - a survey", Proc. IEEE, vol. 87, iss. 7, pp. 1062-1078,1999.
[2]. A.A.J. Altaay, S. bin Sahib, M. zamani, "An introduction to image steganography techniques," Int. Conf. Advanced Computer Science Applications and Technologies, pp. 122-126, 2012.
[3]. C.K.Chan, L.M. Cheng, " Hiding data in image by simple LSB substitution", pattern recognition, vol. 37, no. 3, pp. 469-474, 2004.
[4]. M. Khodaei, K. Faez, "New adaptive steganographic method using least-significant- bit substitution and pixel value differencing," IET Image Process.,vol.6, iss.6, pp. 677-686, 2012.
[5]. H.C. Wu, N.I. Wu, C.S. Tsai, M.S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEE Proc.Vis. Image SignalProcess., vol. 152, no. 5, pp. 611-615, 2005.
[6]. C.M. Wang, N.I. Wu, C.S. Tsai, M.S. Hwang, "A high quality steganographic method with pixel- value differencing and modulus function", The Journal of Systems and Software, vol.81,pp. 150-158, 2008.
[7]. A.D.Kher, "Improved detection of LSBsteganography in grayscale images", Lecture Notes in Computer Science, vol. 3200, pp. 583-592, 2005.
[8]. J.Mielikainen, "LSB matching revisited", IEEE Signal Process. Lett.,vol. 13, no. 5, pp. 285- 287, 2006.
[9]. S. Sarreshtedari, M. A. Akhaee, " One-third probability embedding: a new ±histogram Compensating image LSB steganography scheme", IET Image Process., vol. 8, iss.2, pp. 78-89, 2014.
[10]. N. Akhtar, P. Johri, S. Khan, "Enhancing the security and quality of LSB based image steganography," 5th Int. Conf. Computational Intelligence and Communication Networks, pp. 385-390, 2013.
[11]. A. Westfeld, A. Pfitzmann, "Attacks on Steganographic Systems," Lecture Notes in Computer Science, Springer-Verlag, vol. 1768, pp. 61-75, 2000.
[12]. J. Fridrich, M. Goljan, R. Du, "Reliable detection of LSB steganography in color and grayscale images", Proc. ACM workshop on Multimedia and Security, pp.27-30, 2001.
[13]. A.D. Kher, "Steganalysis of LSB Matching in grayscale images", IEEE Signal Process. Lett., vol. 12,No. 6, pp. 441-444, 2005.
[14]. R.C. Gonzalez, R.E. Woods, "Digital image processing", Third edition, New Jersey,Pearson, 2011.
[15]. J.C. Russ, "The image processing handbook", Sixth Edition, USA, Taylor and Francis Group, 2011.
[16]. Tel Aviv University, " Image Database", http://www.math.tau.ac.il/~turkel/image.html.
[17]. The USC-SIPI Image Database,http://sipi.usc.edu/database.
[18]. Amit bhanwala, Mayank kumar, yogendra Kumar," FPGA based Design of Low Power Reconfigurable Router for Network on Chip (NoC)", ISBN:978-1-4799-8890 ©2015 IEEE,International Conference on Computing, Communication and Automation (ICCCA2015), pp- 1320 - 1326, DOI: 10.1109/CCAA.2015.7148581.
[19]. Mayank kumar, Kishore kumar, sanjiv kumar gupta, yogendra Kumar," FPGA based Design of Area efficient router Architecture for Network on Chip (NoC)", IEEE,International Conference on Computing, Communication and Automation (ICCCA2016), pp-1600 - 1605, DOI: 10.1109/CCAA.2016.7813980.