IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 7, Issue 1, Ver. I (Jan. - Feb. 2017), PP 33-37
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

A Hybrid Steganography Technique Based On LSBMR And OPAP

Varun sangwan
Sangwan.varun@gmail.com

Abstract: *This paper presents a steganography technique based on two existing methods of data hiding i.e. LSBMR and OPAP. The proposed method uses the non-overlapping blocks, having three consecutive pixels. The center pixel of this block embeds k- bits of secret data using OPAP and the remaining pixels of the block embed data using LSBMR. The experimental results show that the proposed method provides better embedding capacity while maintaining the good image quality. The improved performance is shown in comparison to other data hiding methods that are investigated in this study.*

Keywords: *steganography, imperceptibility, least-significant-bit matching revisited (LSBMR), Optimal-pixel-adjustment process (OPAP).*

I. Introduction

The Internet has emerged as a powerful tool for communication over the past decade. It has provided an open and connected environment to its users. Communicating over the Internet is fast and hassle-free but there are few risks attached with it, which cannot be ignored. The biggest nightmare that surrounds the Internet today is privacy. Privacy may be compromised whenever some confidential information is transferred from one person to the other over this open network. To resolve this issue there is a need of a technique through which the information can be transferred secretly. Secure communication between two entities is when the information is transferred in a way that is insusceptible to eavesdropping. Various information hiding techniques are available that facilitate two parties to communicate in secret.

Steganography is one such branch of data hiding. The primary goal of steganography is to conceal the message being communicated within some cover media. The digital cover media used for this purpose can be an image, audio, video, text etc [1]. Digital images are widely used in steganography in comparison to other available cover media due to their high abundance on the Internet. In this paper, the cover media used is an image and the secret data used in the form of text.

Steganography can be performed in various domains but the spatial domain techniques are more popular than others due to their simplicity and less time complexity. In this paper, one such spatial time domain technique has been proposed. The spatial domain methods can be divided into three categories: (i) high embedding capacity approaches with acceptable image quality, (ii) high image quality approaches with reasonable hiding capacity and (iii) restricted embedding capacity approaches with a slight distortion in the quality of the image.

First category of spatial domain approaches focuses on increasing the embedding capacity of cover media [2]. Well-known least-significant-bit (LSB) substitution method lies under this category. In this method, k-LSB bits are replaced with secret data bits. Second category of spatial domain approaches consists of adaptive steganographic methods which makes use of the properties of human visual system (HVS) i.e. hiding more data in edge areas and less data in smooth areas.

The third category of spatial domain approaches provides restricted embedding capacity while maintaining high robustness against steganalysis attacks. One such technique is LSBMR that keeps the cover media unchanged and therefore, less susceptible to attacks.

This paper, focuses on second category methods and proposes a new steganographic algorithm that makes use of LSBMR [3] and OPAP [2] to embed secret data into grayscale cover images. This method consists of two stages. In first stage, the cover image is partitioned into blocks of three consecutive pixels. The center pixel is embedded with k-bits of secret data using LSB substitution and is adjusted accordingly by OPAP for data recovery on the other side. The other two pixels are embedded with one bit each using LSBMR. In the second stage, the data is extracted from stego image.

The remaining sections of the paper is organised as follows. In section II, the literature review is described. In Section III, the proposed method is presented. In section IV, several experimental results are presented to demonstrate the performance of proposed scheme. Finally, conclusions are given in Section V.

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,

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

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 [5]. 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.

III. Proposed work

This section describes the proposed steganographic method for greyscale cover images. The method consists of two phases: (i) embedding phase and (ii) extracting phase.

3.1 Embedding phase

First the cover image is partitioned into non-overlapping blocks in raster scan manner. Each block has three consecutive pixels in which the center pixel is named as p_{ic} and the first and third pixels are p_{i1} and p_{i2}. The procedure of embedding data is as follows [6]:

1. Consider the *k*-LSBs of p_{ic} where $k \in \{3,4,5,6\}$ and transform them into a decimal value LSB_i.

2. Read *k*-bits of secret data (i.e. $k \in \{3,4,5,6\}$) and replace the *k*-LSBs of p_{ic} with these *k*-bits of secret data to obtain$p_{ic}^{'}$. Also, covert the k-secret data bits into decimal equivalent, say s_{ic}.
3. Compute the difference value, $d=LSB_i - s_{ic}$.
4. Using OPAP modify the value of $pic^{'}$ as follows:

$$p_{ic}^{'} = \begin{cases} p_{ic}^{'} + 2^k \ \ if\ d > 2^{k-1} \ \ and\ 0 \le p_{ic}^{'} + 2^k \le 255 \\ p_{ic}^{'} - 2^k \ \ if\ d < -2^{k-1} \ \ and\ 0 \le p_{ic}^{'} - 2^k \le 255 \\ p_{ic}^{'} \qquad otherwise \end{cases}$$

(3)

5. For data hiding in first and third pixel follow the four cases:

Case I: $LSB(p_{i1}) = s_{i1} \& f(p_{i1}, p_{i2}) = s_{i2}$

$$(p_{i1}^{'}, p_{i2}^{'}) = (p_{i1}, p_{i2})$$

Case II: $LSB(p_{i1}) = s_{i1} \& f(p_{i1}, p_{i2}) \neq s_{i2}$

$$(p_{i1}^{'}, p_{i2}^{'}) = (p_{i1}, p_{i2} \pm 1)$$

Case III: $LSB(p_{i1}) \neq s_{i1} \& f(p_{i1} - 1, p_{i2}) = s_{i2}$

$$(p_{i1}^{'}, p_{i2}^{'}) = (p_{i1} - 1, p_{i2})$$

Case IV: $LSB(p_{i1}) \neq s_{i1} \& f(p_{i1} - 1, p_{i2}) \neq s_{i2}$

$$(p_{i1}^{'}, p_{i2}^{'}) = (p_{i1} + 1, p_{i2})$$

where $f(p_{i1}, p_{i2}) = LSB(\left\lfloor \frac{p_{i1}}{2} \right\rfloor + p_{i2})$ and s_{i1}, s_{i2}denote two secret bits to be embedded. After embedding process new block will have pixels $p_{i1}^{'}, p_{ic}^{'}, p_{i2}^{'}$. The above procedure will be repeated for each block of cover image to obtain the stego image.

3.2 Extracting phase

In this section the embedded data is recovered from stego image. The stego image is partitioned into non-overlapping blocks of three pixels each. Then select the second pixel of the block first and perform the extraction process as follows:

1. Extract the secret data bits from *k*-LSBs of $p_{ic}^{'}$ and call it s_{ic}.
2. Obtain s_{i1} and s_{i2} using the relation,

$$s_{i1} = LSB(p_{i1}^{'})$$
$$s_{i2} = f(p_{i1}^{'}, p_{i2}^{'})$$

Concatenate s_{ic},s_{i1} and s_{i2} to obtain the original secret data bit stream. Apply the above procedure on each block to extract the whole secret data bits.

IV. Experimental Results

This section presents the experimental results of the proposed method and compares the results with the results of PVD method and PVD &LSB replacement method. The test images used for verifying the results are greyscale images of size 512X512, namely 'Lena', 'Peppers', 'Baboon' and 'Boat'. Generally, for performance evaluation of data hiding methods, four criteria are utilized [7]: (i) imperceptibility of stego images, (ii) the embedding capacity, (iii) the complexity and (iv) the robustness of data embedding algorithm. The proposed method tries to satisfy these criteria satisfactorily.

The PSNR value is used to evaluate the distortions of the stego images [8]. It can be computed as

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - Y(i,j))^2 \quad (4)$$

$$PSNR = 10 log_{10} \left(\frac{Max^2}{MSE} \right) \quad (5)$$

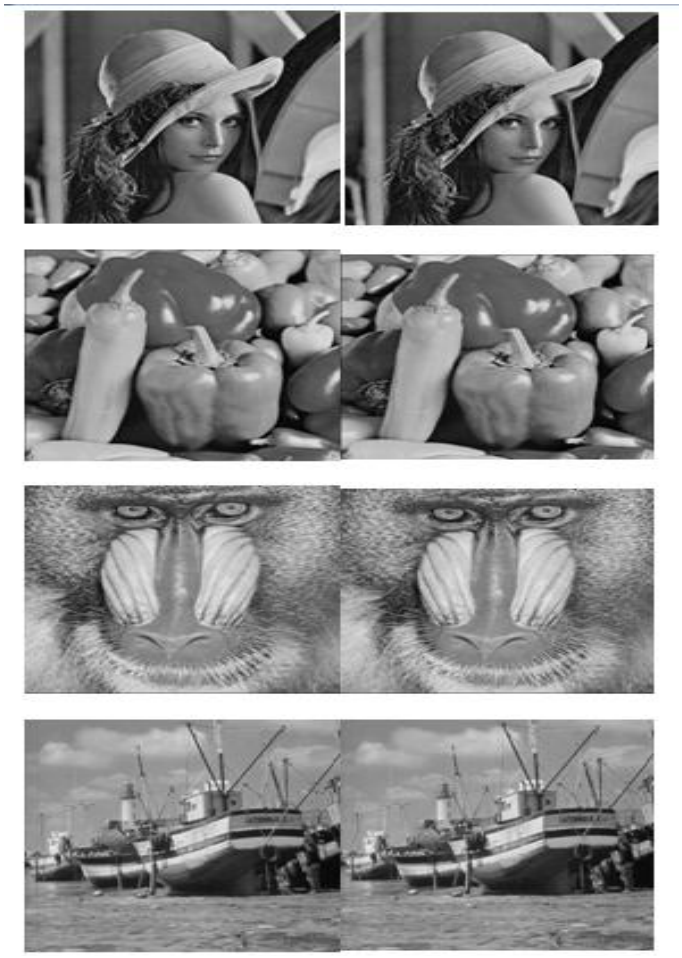
where MxN denotes the size of the cover image I and stego image Y. a high PSNR value means good quality of stego image and is highly imperceptible whereas a low PSNR means the opposite. Fig. 1. shows the similarity between cover images and its corresponding stego images and hence proves the proposed method is highly imperceptible.

Cover images	PVD		PVD and LSB replacement		Proposed method	
	Capacity, bit	PSNR, dB	Capacity, bit	PSNR, dB	Capacity, bit	PSNR, dB
Lena	409,752	38.94	766,040	36.16	524,287	38.42
Peppers	407,256	37.07	770,248	35.34	524,287	38.42
Baboon	457,168	33.43	717,848	32.63	524,287	38.43
Boat	421,080	34.89	756,768	33.62	524,287	38.59

Table 1. Comparisons of the results between PVD, PVD & LSB replacement and the Proposed method.

The embedding capacity of the proposed method increases as the k value increases whereas the PSNR value decreases. The distortions occurred due to increase in embedding capacity are slight and indistinguishable. Table 1 shows the comparison of PSNR values and embedding capacity of the proposed method with the PVD and PVD&LSB replacement methods. Here, the proposed method performs better than the PVD method in both criteria whereas its better than second method in PSNR value and not in terms of embedding capacity.

Generally, the methods designed in spatial domain have a low time complexity. The proposed method falls under spatial domain and also, in this method there is no requirement of readjusting phase or knowledge of any range table as required by PVD and PVD &LSB replacement methods. Thus, the time complexity of the proposed method is low.



(a) **(b)**

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

Besides providing large data hiding capacity and good quality of stego image, a steganographic method needs to be resistant against various steganalytic attacks [9],[10]. Mostly the steganalysers are based on image histogram, therefore, if the histogram characteristics are preserved properly then there is possibility of achieving high resistance against the well-known detectors. The proposed method maintains less changes in histogram as the PSNR value is good and the stego image is imperceptible.

V. Conclusions

This paper has presented a hybrid steganographic technique based on LSMR and OPAP. 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.. The efficacy of the proposed method is verified via several experimental results that yielded better performance in comparison with PVD and PVD-LSB replacement method.

References

[1] F. Petitcolas, R. Anderson, and M. Kuhn, "Information hiding- a survey," *Proc. IEEE*, vol. 87, iss. 7, pp. 1062-1078, 1999.
[2] C.K. Chan, L.M. Cheng, "Hiding data in image by simple LSB substitution", pattern recognition, vol. 37, no. 3, 2004, pp. 469-474.
[3] J. Mielikainen, "LSB matching revisited," IEEE Signal Process. Lett., vol. 13, no. 5, 2006, pp. 285-287.
[4] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value-differencing," *Pattern Recognit. Lett.*, vol. 24, no. 9-10, pp. 1613-1626, 2003.
[5] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value-differencing and LSB replacement methods," *Proc. Inst. Elect. Eng.,Vis. Images Signal Process.*, vol. 152, no. 5, pp. 611-615, 2005.
[6] C. M. Wang, N. I. Wu, C. S. Tsai, and M. S. Hwang, " A high quality steganographic method with pixel value differencing and modulus function," *The Journal of Sys.and Soft.*, vol.81, pp. 150-158, 2008.
[7] C.-H. Yang, C.-Y. Weng, S.-J. Wang and H.-M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Trans. Inf. Forensics Sec.*, vol. 3, no. 3, pp. 488-497, 2008.
[8] M. Khodaei and K. Faez, "New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing," *IET Image Processing*, vol. 6, iss. 6, pp. 677-686, 2012.
[9] J. Fridrich, M. Goljan, and R. Du, "Relaiable detection of LSB steganography in color and grayscale images," *Proc. ACM Workshop on Multi. And Sec.*, pp. 61-75, 2000.
[10] A. Westfeld, A. Pfitzmann, "Attacks on stegographic systems", Lecture Notes in Computer Science, vol. 1768, 2000, pp. 61-75.
[11] The USC-SIPI Image Database, http://sipi.usc.edu/database.
[12] 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.
[13] 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.