Secured Information Hiding Using Variable Pixel Block Size of PVD Steganographic Techniques

Dinesh D. Patil & S. M. Bansode

Department of Computer Science and Engineering
Government College of Engineering, Aurangabad (MS), India
E-mail : dineshonly@gmail.com, kandharess11@gmail.com

***Abstract* – In this paper we propose a steganography method for hiding secret information within the spatial domain of the gray scale & color image. The proposed approach works on pixel value differencing (PVD), the cover image is divided into blocks of equal sizes and then embeds the message using the difference values d of pixel obtained in each block. In a color image every pixel value composed of red, green and blue component and each of which ranges from 0 to 255 in case of 8-bit representation. The embedded message changes the characteristics and the properties of the image in which it is hidden ($p'_0 - p'_1$) and it is needed that these changes are difficult to be identified. In this paper to enlarge the hiding capacity of secret information and quality of stego-image that cannot be perceived by human eyes we extend block based PVD from two pixel block to the four and eight pixel block size for embedding data. The proposed method not only has an acceptable image quality but also provides a large embedding capacity. Our results are compared with the PVD method with four and eight pixels and the values obtained are better than the PVD method.**

Keywords: Embedding capacity, PVD method, Peak signal to noise ratio (PSNR), Steganography

I. INTRODUCTION

Stegnography is an art of sending a secrete message under the camouflage of a carrier content. The carrier content appears to have totally different but normal meanings. The goal of stegnography is to mask the very presence of communication, making the true message not discernible to the observer [1]. The carrier image in stegnographic is called the "cover image" and the image which has the embedded data is called the "stego image". On the other hand, steganalysis is the set of techniques that aim to distinguish between cover-objects and stego objects [2]-[3].

There are two kinds of image stegnographic techniques: spatial-domain and transform domain based methods. Spatial domain based methods embed messages directly in the intensity of pixels of images [2]-[6]. For transform domain based ones, images are first transformed to another domain (such as frequency domain), and messages are then embedded in transform coefficients [7]-[10]. Fridrich et al, present a new, reliable and extremely accurate steganalytic method that can be applied to 24-bit color images as well as to 8-bit grayscale (or color) images with randomly scattered message bits embedded in the LSBs of colors or pointers to the palette [4]-[5]. Zhang et al, [7], proposed a steganalysis method which is based on a physical quantity derived from the transition coefficients between difference histograms of an image and its processed version produced by setting all bits in the LSB plane to zero. This quantity is claimed to be a good measure of the weak correlation between successive bit planes and can be used to discriminate stego-images from cover images. They also indicate that there exists a functional relationship between this quantity and the embedded message length. The pixel-value differencing (PVD) method proposed by Wu and Tsai [6] can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. Wu and Tsai [6] presented a stegnographic method based on Pixel Value Differencing (PVD). They divide the cover image into a number of non-overlapping two pixel blocks. Each block is categorized according to the difference of the gray values of the two pixels in the block. A small difference value indicates that the block is in a smooth area and a large one indicates that it is in an edged area. The pixels in edged areas may tolerate larger changes of pixel values than those in the smooth areas. Therefore, it is possible to embed more data in edged areas than in the smooth areas [8]-[9]. All possible difference values are classified into a number of ranges and the number of bits which can be embedded in a pixel pair is decided by the width of the range that the difference value belongs to. It is claimed that the changes in the resulting stego-image are unnoticeable [11]. In this paper, a novel stegnographic approach using four and eight pixel-value differencing is proposed. To increase the hiding capacity of original PVD method is extend to four pixel and eight

pixel differencing scheme. Also, to reduce the quality distortion of the stego-image brought from setting larger embedding capacity, an optimal problem is formulated and solved. This can maintain the stego-image at an acceptable and satisfied quality.

II. PROPOSED SYSTEM

In this proposed system gray scale & color image is used as cover image, every pixel in a color image composed of three colors (channels) i.e. Red, Green and Blue. So, every pixel contains 24 bits (for 8-bit representation) where 8 bits for red component, 8 bits for green and 8 bits for blue component in a pixel, all the three components have been used for data embedding. First, separated each color Component from a pixel then we get three separate M*N matrix for each color

Now, apply pixel value differencing method for data hiding in each matrix separately, but in a sequencing manner. First embed bits in 1st pixel block of the red component matrix, then in 1st block of green component matrix and lastly in blue component matrix, then again 2nd block of red matrix and soon. In Extracting steps Divide the stego image into three component matrix RED, GREEN and BLUE and execute the following steps for each pixel block, consist of two consecutive non-overlapping pixels, of RED, GREEN, and BLUE respectively i.e. extract bits from one stego pixel at a time. Then same procedure explain for data hiding and data extractions for gray scale and color image.

A. *Data Hiding*

In our proposed system blocks of 2 (PVD), 4 and 8 pixels size are used to embed data in images. In PVD scheme, the cover image is divided into non-overlapping blocks, where each block consists of two consecutive pixels in row order Shown in I.

The data hiding procedure is independent in each block. Let the pixel pair in one block of cover image be (P_0, P_1). The difference d in "(1)"is calculated from the adjacent pixel as

$$d = P_1 - P_0 \qquad (1)$$

with $|d| \in [0, 255]$. The data embedding procedure replaces w least significant bits of the absolute difference $|d|$ with the secret bits. As stated previously, the number of secret bits to embed depends on the smoothness of the block, or the strength of the pixel-value difference in the block.

I. Pixel difference value

Block Size (Pixels)	**Difference *d* (of consecutive pixels)**
PVD	*d* 1 = abs(f(i,j) -f(i,j+1));

4 Pixels	*d* 1 = abs(f(i,j) -f(i,j+1));
	d 2 = abs(f(i,j+1)-f(i,j+2));
	d 3 = abs(f(i,j+2)-f(i,j+3));

8 Pixels	*d* 1 = abs(f(i,j)-f(i,j+1));
	d 2 = abs(f(i,j+1)-f(i,j+2));
	d 3 = abs(f(i,j+2)-f(i,j+3));
	d 4 = abs(f(i,j+3)-f(i,j+4));
	d 5 = abs(f(i,j+4)-f(i,j+5));
	d 6 = abs(f(i,j+5)-f(i,j+6));
	d 7 = abs(f(i,j+6)-f(i,j+7));

To decide w, $|d|$ is classified according to a set of continuous ranges R. The choice of R in this system is taken as in "(2)" i.e. the width of each range is taken to be a power of 2

$$R = \{R_k\text{-}[l_k, u_k]\} \qquad (2)$$

The number of secret bits to be embedded in each range is as given in equation "(3)".

$$\{w_k = log_2 (u_k - l_k)\} = \{3,3,4,5,6,7\} \qquad (3)$$

If d is in R_k, then w_k secret bits are taken and convert to a decimal value b, then the new difference value d' is calculated by using (4) and (5).

$$d' = l_k + b \quad \text{if } d \geq 0, \qquad (4)$$

$$d' = -(l_k + b) \text{ if } d < 0. \qquad (5)$$

The Pixel values are updated (modified pixel) by (6) to complete the embedding procedure.

$$(p'_0, p'_1) = \begin{cases} P_0 - \text{ceil}[(d' - d)/2],\ P_1 + \text{floor}[(d' - d)/2] & \text{, if } d \text{ is odd} \\ P_0 - \text{floor}[(d' - d)/2],\ P_1 + \text{ceil}[(d' - d)/2] & \text{, if } d \text{ is even} \end{cases} \qquad (6)$$

If the new pixel pair (p'_0 - p'_1) is out of the range [0, 255] i.e. the new pixel value is out of the acceptable intensity value, then the block is labeled as unusable and restores its original pixel values $P_1 - P_0$.

B. *Data Extraction*

In data extraction, the stego-image is divided into the same non-overlapping blocks as in the embedding procedure. Calculate the difference value d' for each block of two consecutive pixels p'_0 and p'_1 in the stego-image Shown in "(7)" & II.

$d' = - (p'_0 - p'_1)$ (7)

Find the optimal R_k of the d', such that

$R = \min (u_i - k)$ (8)

II. Pixel difference value

Block Size (Pixels)	Difference d' (of consecutive pixels)
PVD	$d'1$ = f_ex(i,j+1)-f_ex(i,j);
4 Pixels	$d'1$ = f_ex(i,j+1)-f_ex(i,j); $d'2$ = f_ex(i,j+2)-f_ex(i,j+1); $d'3$ = f_ex(i,j+3)-f_ex(i,j+2);
8 Pixels	$d'1$ = f_ex(i,j+1)-f_ex(i,j); $d'2$= f_ex(i,j+2)-f_ex(i,j+1); $d'3$= f_ex(i,j+3)-f_ex(i,j+2); $d'4$=f_ex(i,j+4)-f_ex(i,j+3); $d'5$=f_ex(i,j+5)-f_ex(i,j+4); $d'6$=f_ex(i,j+6)-f_ex(i,j+5); $d'7$=f_ex(i,j+7)-f_ex(i,j+6);

Where, $u_i \geq k$, $k = |d'|$ and $R_k \in [l_k, u_k]$.

After R is located then obtain b' by subtracting l_k from d' in "(9)".

$b' = d' - l_k$ (9)

The b' value represents the value of the secret data in decimal. Convert b' into binary then find the number of bits refer to "(10)"i.e. t from the secret data where

$t = log_2 w_i$. (10)

Convert the binary data stream into decimal values. Obtain the embedded data by converting decimal values into character.

III. RESULT, COMPARISION AND ANALYSIS

In this section result for the proposed technique, the block-based PVD extends from 2-pixel block to the 4 and 8-pixel block sizes are used to embed data in images. For testing three different standard gray images namely Lena, Baboon, F-16, Pepper and House each of size 512 × 512 .For experimental results refers III-V. Results shows that PVD method for gray scale Baboon image are outperforming in case of data embedding capacity with the cost of low PSNR value as compared to the other methods. The PVD method for Baboon gives good quality stego-image with acceptable PSNR i.e. 38.6477. Our proposed method produces the high capacity of embedding and security in terms of PSNR.

III. Results in terms of Capacity and PSNR of PVD method on Baboon image.

Method	Capacity (bits)	PSNR (db)
PVD	425132	38.6232
4-pixel	606217	37.9169
8-pixel	707229	35.5732

IV. Results in terms of Capacity and PSNR of PVD methods on Lena image.

Method	Capacity	PSNR
PVD	376399	40.7641
4-pixel	507032	39.6475
8-pixel	591509	32.3424

V. Results in terms of Capacity, PSNR of PVD methods on F-16 image.

Method	Capacity (bits)	PSNR (db)
PVD	364665	40.6596
4-pixel	545118	34.1963
8-pixel	553846	33.3288

IV. CONCLUSION

The paper proposed modified approach termed as Block based PVD extends from 2-pixel block to 4 and 8-pixel block differencing where large amount of information can be embedded. Difference of two pixels is calculated as shown in table no.1and modified value of two pixels is calculated in (6). This paper shows that the proposed technique improve security of the data to be hidden with increasing embedding capacity. The proposed technique obtained better visibility with better PSNR ratio.

The block-based PVD extends from 2-pixel block to the 4 and 8-pixel block size for embedding data. To reconstruct the pixel values from the embedded pixel-value differences in a block, an optimization problem is formulated and solved. A larger block size will provide a higher capacity at the cost of stego-image quality; a high contrast region can be used to hide more bits without notice. Using this technique, more data can he inserted into areas where differences in the adjacent pixel values is large, as pixels in these areas can tolerate

more changes and this leads to good imperceptibility and a high embedding rate.

V. REFERENCES

[1] F. Hartung and M. Kutter, "Multimedia watermarking Techniques", Proceedings of IEEE, vol. 87, pp. 1079–1107.

[2] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp "Perceptual watermarks for digital images and video". Proceedings of IEEE, vol.87, pp 1108-1126, 1999.

[3] J. Fridrich, "Image watermarking for tamper detection", Proceeding of IEEE International Conf. on Image Processing , Chicago, IL, pp. 404-408, 1998 .

[4] J. Fridrich, M. Goljan, and R. Du, "Stegnography in grayscale and color images", Proceeding of IEEE Multimedia, pp. 22-28, 2001.

[5] J. Fridrich and M. Goljan, "Practical steganalysis of digital image-state of the art", Proceedings of SPIE Conf. on security and watermarking of Multimedia Contents, Portland, Oregon, USA, pp. 1-13,2002.

[6] D.C. Wu and W.H. Tsai, "A stegnographic method for images by pixel- value differencing", Pattern Recognition Letters,vol.24,pp 1613-1626, 2003.

[7] X. Zhang and S. Wang, "Vulnerability of pixel-value differencing stegnography to histogram analysis and modification for enhanced security", Pattern Recognition Letters, Vol. 25, pp. 331-339, 2004.

[8] V. Sabeti, S. Samavi, M. Mahdavi, "Steganalysis of Pixel-Value Differencing stegnographic method", Proceeding of Communications, Computers and Signal, Conference, IEEE Pacific Rim conference, Canada, 2007.

[9] Jiun-Jian Liaw, Wen-Sheng Wang and Min-Yen Chiu, "A Data Hiding Method Using Secret Data Division and Pixel Value Differencing" IEEE , ICGEC ,pp 650-653, 2010.

[10] M.B. Ould MEDENI, El Mamoun SOUIDI, "A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution", IEEE ICMCS, pp 1-4, 2011.

[11] Cheng-Hsing Yang, Chi-Yao Weng, Hao-Kuan Tso, Shiuh-Jeng Wang," A data hiding scheme using the varieties of pixel-value differencing in Multimedia images", The Journal of Systems and Software 84, pp 679-678Elsevier Inc.,2011.

◈◈◈