International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 22 (2015) pp 42877-42880

A Steganographic Method Based on Modified Pixel-Value Differencing

Azhar Ahmad Jaini

Researcher, UTM-IRDA Digital Media Centre (MaGIC-X), Faculty of Computing, Universiti Teknologi Malaysia, 81310 Skudai, Johor Bahru, Malaysia azharahmadjaini@yahoo.com

Ghazali Sulong,

Professor, UTM-IRDA Digital Media Centre (MaGIC-X), Faculty of Computing, Universiti Teknologi Malaysia, 81310 Skudai, Johor Bahru, Malaysia ghazali@spaceutm.edu.my

Abstract
This study proposes a new steganographic scheme using the Modified Pixel-Value-Differencing (PVD) technique that considers the pixel value difference between a pixel with all its surrounding pixels. The proposed PVD takes into account only at the first three MSBs to generate a Bit-Length-Matrix (BLM), which keeps the length of bit string embedded on each pixel. The BLM is generated from both Cover and Stego Image-there is no need for a Quantization Table to be sent to the receiver. Experiment result using standard dataset shows that the proposed technique achieved high capacity of more than 3.59 bpp with acceptable imperceptibility.

Keywords: steganography, Pixel-Value-Differencing, Bit-Length Matrix

Introduction

Steganography is a field of embedding secret messages within another files. Many researchers [1][2][3] embedded the secret messages to the LSBs as this will normally yield a good noise value. The challenge is to select the best set of pixels that are to be embedded. The pixel-value differencing (PVD) [4][5][6] in steganography is a method of detecting pixels with high value difference as compared with their neighbours. The embedding of message bits is more at the pixels with more difference value. The scanning block for PVD generally varies in two manners, the value difference and the block size. The PVD technique provides quantization table that represent the payloads at each pixel. Several studies have been proposed to improve the PVD methods.

This work proposes a new approach to decide the number of bits to be embedded. In other earlier works, there are many ways to embed the secret message. One of them is by determining the smooth and noise area where more bits embedded at noise areas than the smooth areas. Some use the quantization table to map the location of the pixels that are to be embedded. These location information are either sent to receiver in the form of table or embedded in the stego image. Both either increase the payload of data transfer or reduce the capacity. This work provides a common result in determining the smooth and noise area using either the cover image or the stego image. So, the location information is regenerated at the receivers' end without having to embed them at the stego image.

The remainder of this paper is organized as follows. Section 2 briefly describes the related earlier works. Section 3 describes our proposed scheme. This include the message preparation using Insignificant Bit Exclusion, the PVD approach, embedding and extraction procedure. Section 4 describes the experiment results. The final section, Section 5 concludes this paper.

Related Works

Pixel Value Differencing in steganography was introduced to make used of the value difference between two pixels of greyscale image [4][5][6]. To achieve this, Wu and Tsai first partition the image into non-overlapping couple of pixels [4]. So, an image sized $n \times n$ or n^2 pixels is partitioned into $(n^2)/2$ couples. The difference value of each couple is calculated with the understanding that low value difference represent smooth area and high value difference represent sharp edge area.

There are a few other studies related to scanning and measuring the value difference of greyscale pixels. Wu et al. [7] used pixel-value differencing and LSB replacement methods. Yang and Weng [8] used multi-pixel differencing in a four-pixel block to determine how many secret bits should be embedded. Jung et al. [9] proposed another multi-pixel differencing and LSB substitution methods. Liu and Shih [10] proposed the generalizations of pixel-value differencing with the block-based approach and Haar-based approach. Liao et al.'s [11] proposed another four-pixel differencing and modified LSB substitution. Yang et al.'s [12] proposed a blocked type PVD. Tseng et al. [13] proposed a new quantization range table based on the perfect square number.

Proposed Scheme

In this study we execute PVD in the first 3-bits (3-MSBs) to avoid fake edges.

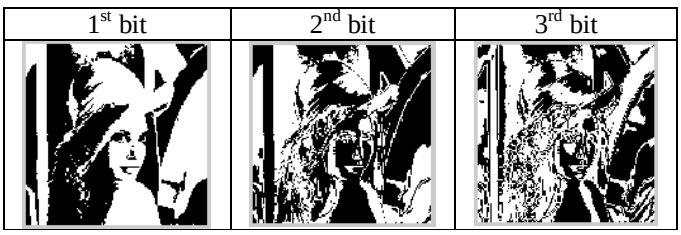

Fig 2: Bit Slice image of 'lena'

This modified PVD processes bit-sliced images that consist only 1s and 0s. It does not involve threshold or range value as normally conducted. Each bit-sliced image is filtered by a 3x3 block. The procedure is as follow.

Input. Cover image or stego image
Output. The Bit Length Matrix (BLM) representing the noise area (or edge)
Step1. Scan bit-slice image using a 3X3 block
Step 2. Filter the block using the convolution matrix F^{PVD} below where the average difference value is calculated.

$$F^{PVD} = \frac{1}{8}\begin{bmatrix}1 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 1\end{bmatrix} \qquad \dots(1)$$

$$Pixel_{ij} = \begin{cases} Noise\ area, & if\ \left(CB_{ij} \times F_{ij}^{PVD}\right) = C_{ij} \\ Smooth\ area, & if\ \left(CB_{ij} \times F_{ij}^{PVD}\right) \neq C_{ij} \end{cases}$$

Where,
CB_{ij} = 3 × 3 block matrix centered at pixel (i,j)
C_{ij} = Greyscale value of pixel (i,j)

Step 3. Noise areas are embedded with longer bit length and smooth areas are embedded with shorter bit length. For example BLM(3,4) represents 3 bit embedded at smooth area and 4 bits at noise area.

Example:

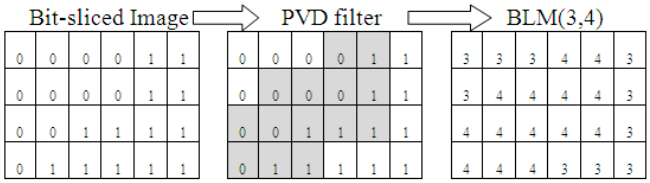

Fig 3: From Bit-Sliced Image to Bit Length Matrix

Step 4. Repeat step 1 to 3 to get BLMs for all three bit-slice images.
Step 5. Merge all three BLMs from each bit-slice image by choosing the highest value

$$BLM_{ij}^{F} = \max\left(BLM_{ij}^{1}, BLM_{ij}^{2}, BLM_{ij}^{3}\right) \qquad \dots(2)$$

Where,
(i , j) = location of the pixel
BLM^1 = BLM value of bit-sliced image of the first bit
BLM^2 = BLM value of bit-sliced image of the second bit
BLM^3 = BLM value of bit-sliced image of the third bit
BLM^F = final BLM value

Embedding Procedure

The secret message is in the form of long bit-string-tape is cut according to the length stated in the matching BLM. The embedding procedure is as follow.

Input. Cover image (C), Secret message bit string (M), BLM^F
Output. Stego image (S)
Step 1. Read the BLM value for pixel (i,j), i.e, BLM_{ij}
Step 2. Read the greyscale value of cover image at pixel (i,j), i.e, C_{ij}
Step 3. Convert C_{ij} value from decimal to binary.
Step 4. Substitute the LSBs of C_{ij} according of the length stated at BLM_{ij} with the same length of bits taken from the secret message bit string.
Step 5. Convert C_{ij} back to decimal and keep as stego pixel, S_{ij}
Step 6. Repeat step 1 to 5 until finish
Step 7. Save stego image, S

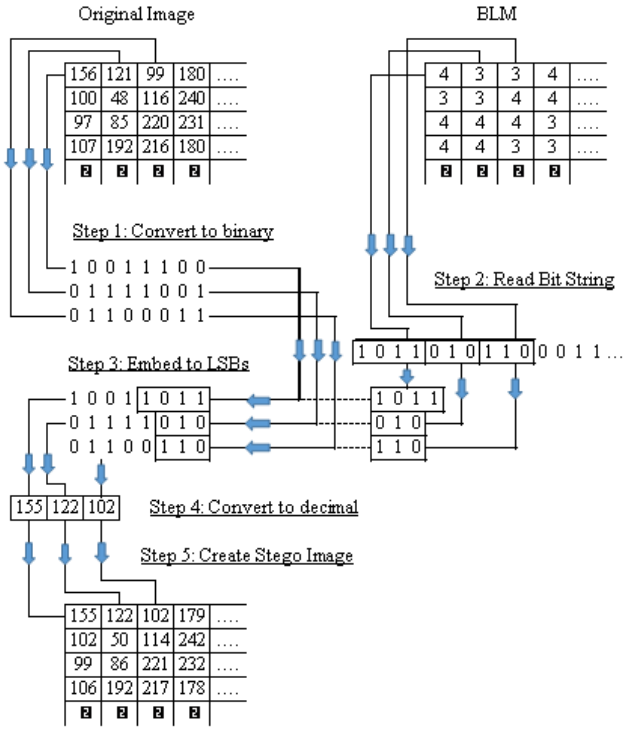

Fig 4: Example of embedding process

Extraction Procedure

The embedding of secret message in this study is at most up to the fifth LSBs. The first three MSBs are not used to embed secret message. So, the bit-slice images of the 3-MSBs for both cover and stego image are exactly similar. Hence, by having this similarity, the Bit Length Matrix, BLM used to embed the secret message is regenerated using only the stego image at the receiver's end without losing any bit. The procedure to extract the message is as follow.

Input. Stego image, S
Output. Secret Text, T
Step 1. Read the BLM value at pixel (i,j), i.e, BLM_{ij} from S using the procedure stated at 3.1
Step 2. Read the greyscale value of stego image at pixel (i,j), i.e, S_{ij}
Step 3. Convert S_{ij} value from decimal to binary.
Step 4. Extract the correct length of bit string from S_{ij} based on the value of BLM_{ij}

Step 5. Concatenate the extracted bit string
Step 6. Repeat step 1 to 5 until finish
Step 7. Divide bit string to every byte and convert back to decimal. That decimal values are the ASCII values of the characters from the secret message

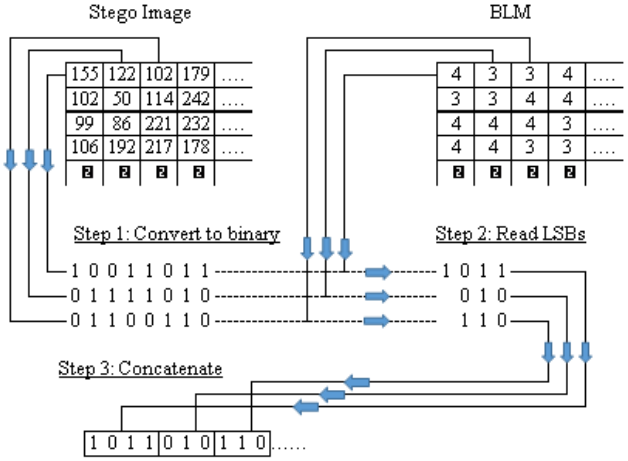

Fig 5: Extraction procedure

Experiment Results

This study uses House, Tiffany, Baboon, Lena, Airplane and Pepper as standard dataset or cover images and the multi-lingual 'lorem ipsum' standard text as secret message.

The images this experiment is pre-processed to 128 pixels X 128 pixels greyscale images. Figure 4 shows the cover images and stego images after the embedding of the 'lorem ipsum' standard text.

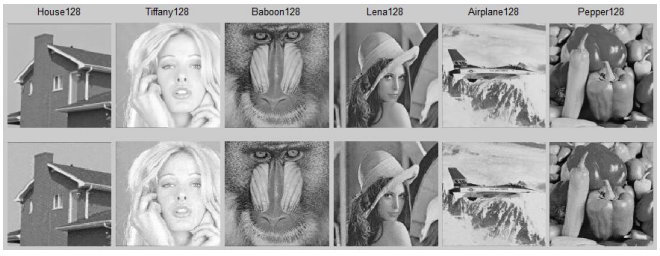

Fig 5: Original Cover images (top row) and Stego Images using BLM(3,4) (bottom row)

By having the ability to re-generate the BLM at the receiver's end, there is no needs to include the location information in the stego image, hence, increase the capacity significantly. This is shown in table 1 below.

Table 2: The experiment results

Cover Image	BLM(3,4)		BLM(2,3)	
	Payload (bpp)	PSNR (dB)	Payload (bpp)	PSNR (dB)
House	3.59	34.27	2.53	40.32
Tiffany	3.61	34.08	2.55	40.32
Baboon	3.97	32.60	2.91	38.67
Lena	3.71	33.47	2.65	39.66
Airplane	3.64	34.06	2.58	40.16
Pepper	3.73	33.51	2.67	39.69
Average	3.71	33.67	2.65	39.80

The result shows that the proposed scheme has significantly improve the payload values from to average payload of 3.71 bpp with average imperceptibility of 33.67 dB.

Conclusions

This study proposes a technique of embedding secret message of different bit length at noise and smooth area of an image without embedding the location information of the embedded bits. The location or Bit Location Matrix, BLM contains information of the location and length of the secret bits. The receiver of the stego image regenerates the BLM to locate the exact same location of noise and smooth areas. The extraction and concatenation of LSBs in each pixel form the message bit string. The division of the bit string to bytes represents characters of the secret message.

The experiments shows that this method has not violated the basic concept of HVS (Human Visual System) by having high PSNR values or good image quality. The results clearly show that the proposed scheme provides large capacity and high imperceptibility.

References

[1] Reband Jamil Hassan, Ghazali Sulong, 2014, "A new Colour Image Steganography using LSB Approach with Halftoning Determination", International Journal of Scientific & Engineering Research, Vol. 5, Issue 4, pp. 285-291.

[2] Morteza Bashardoost, Ghazali Bin Sulong and Parisa Gerami, 2013, "Enhanced LSB image steganography method by using Knight Tour algorithm, Vigenere encryption and LZW compression", IJCSI International Journal of Computer Issues, Vol. 10, Issue 2, No. 1, pp. 221-227.

[3] Morteza Bashardoost, Ghazali Bin Sulong and Parisa Gerami, 2013, "Enhanced LSB image steganography method by using Knight Tour algorithm, Vigenere encryption and LZW compression", IJCSI International Journal of Computer Issues, Vol. 10, Issue 2, No. 1,pp. 221-227.

[4] D.-C. Wu and W.-H. Tsai, 2003, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613-1626.

[5] C. H. Yang, S. J. Wang, C. Y. Weng, and H. M. Sun, 2008, "Information hiding technique based on blocked PVD," Journal of Information Management, vol. 15, no. 3, pp. 29-48.

[6] R. M. Samant and S. Agrawal, 2011, "Data hiding in gray-scale images using pixel value differencing," ICWET '11, Proceedings of the International Conference & Workshop on Emerging Trends in Technology, pp. 587-592

[7] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Huang, 2005, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," IEE Proceedings Vision Image and Signal Processing, vol. 152, no. 5, pp. 611-615.

[8] C. H. Yang and C. Y. Weng, 2006, "A steganographic method for digital images by multi-pixel differencing," in Proceedings of International Computer Symposium, Taipei, Taiwan, pp. 831-836.

[9] K.-H. Jung, K.-J. Ha, and K.-Y. Yoo, 2008, "Image data hiding method based on multi-pixel differencing and LSB substitution methods," in Proceedings of International Conference on Convergence and Hybrid Information Technology (ICHIT '08), pp. 355-358.

[10] J.-C. Liu and M.-H. Shih, 2008, "Generalizations of pixel-value differencing steganography for data hiding in images," Fundamenta Informaticae, vol. 83, no. 3, pp. 319-335.

[11] X. Liao, Q.-Y. Wen, and J. Zhang, 2011, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," Journal of Visual Communication and Image Representation, vol. 22, no. 1, pp. 1-8.

[12] C.-H. Yang, C.-Y. Weng, H.-K. Tso, and S.-J. Wang, 2011, "A data hiding scheme using the varieties of pixel-value differencing in multimedia images," Journal of Systems and Software, vol. 84, no. 4, pp. 669-678.

[13] Hsien-Wen Tseng and Hui-Shih Leng, 2013, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number," Journal of Applied Mathematics, Volume 2013, Article ID 189706