Available online at www.sciencedirect.com

ScienceDirect

IERI Procedia 4 (2013) 17 – 24

Procedia IERI

www.elsevier.com/locate/procedia

2013 International Conference on Electronic Engineering and Computer Science

Color Image Steganography based on Pixel Value Modification Method Using Modulus Function

V.Nagaraj[a], Dr. V. Vijayalakshmi[b] and Dr. G. Zayaraz[c]

[a] *Research scholar, ECE Dept., Pondicherry Engineering College, Puducherry-605014, India*
[b] *Assistant Professor, ECE Dept., Pondicherry Engineering College, Puducherry, India*
[c] *Associate Professor, CSE Dept., Pondicherry Engineering College, Puducherry, India*

Abstract

Steganography is the only answer for secure and secret communication. Existing methods in image steganography focus on increasing embedding capacity of secret data. According to existing methods, the experimental results indicate that two pixels are required for one secret digit embedding. In direction of improve the embedding size of secret data, a novel method of Pixel Value Modification (PVM) by modulus function is proposed. The proposed PVM method can embed one secret digit on one pixel of cover image. Thus, the proposed PVM method gives good quality of stego image. The experimental outputs validate that good visual perception of stego image with more secret data embedding capacity of stego image can be achieved by the proposed method.

Selection and peer review under responsibility of Information Engineering Research Institute

Keywords: Steganography, Pixel Value Modification, Pixel Value Differencing, Tri-Way Pixel Value Differencing, Data Hiding, Embedding Payload.

1. Introduction

Steganography is the knowledge of communicating invisible secret data by embedding it into a multimedia carrier. The idea of steganography is to hide the very existence of the embedded data. Even though the term Steganography has been known for thousands of years, its digital practice came about only lately and research was intensified after the depressing event of Twin towers (11th Sep 2001).

* Corresponding author. Tel.: +91-989418892.
E-mail address: nagarajvaithilingam@gmail.com.

2212-6678
Selection and peer review under responsibility of Information Engineering Research Institute
doi:10.1016/j.ieri.2013.11.004

Steganalysis is art of detecting hidden messages present in stego objects, defeats Steganography algorithms are based on two types they are the spatial domain and the transform domain. Steganography's main objectives are undetectability, robustness and capacity of the secret data. These features are separating it from other relating techniques like watermarking and cryptography.

Least Significant Bit (LSB) steganography method is the common approaches of steganography. Insertion, masking and filtering, and transformations [1] are some of other methods in steganography techniques. LSB insertion method, two or more LSB bits of pixels are replaced with secret bits. Chan and Cheng [2] proposed LSB substitution with an optimal pixel adjustment for data embedding in simple manner. Wu and Tsai[3] proposed a Pixel Value Differencing (PVD) method with outstanding quality of stego image and also hide more data . Thereafter, various PVD based approaches have been proposed [4].

In this steganography paper, an approach of color images, using PVM has been proposed. The color pixel components are separated into three planes namely R, G and B planes. In the proposed method a digital color image are used as a cover image. When compared to Wu-Tsai's PVD method it will provide more security in data hiding and also better stego image quality. The experimental results of proposed method have high capacity than PVD methods.

This paper is prescribed with following sections. Section 2 analyses the PVD and other embedding methods. In Section 3, described with embedding and extracting procedures of the proposed method is given. In Section 4, discussing with the experimental results of proposed method is presented. Finally, Section 5 gives the conclusion of proposed method.

2. Related Work

The PVD method is data hiding scheme based on pixel difference in cover image. [5], in which cover image area are classified into two types one is smoother region and other one is hard regions. In the smoother region pixel are having small differences with their neighbor pixels. These smoother pixels are not suitable for data embedding. So the pixels with large differences with their neighbor pixels are used for data embedding. This method provides good embedding capacity but stego images are statically detectible one.

Modified version of PVD method is Tri-way pixel value differencing (TPVD) method [6], In the TPVD method three direction pixel selections is made for increasing the payload by embedding secret bits in three different directions on cover image. PVD method only uses one direction for data embedding. Whereas TPVD use horizontal, vertical and diagonal edges of image for embeds secret data. Preprocessing phase of cover image into 2x2 pixel blocks is required in TPVD method.

Another modified version of PVD is Adaptive pixel value differencing (APVD) method. APVD method is only applied for gray scale images. In gray scale digital image having pixel value ranges from 0 to 255. The stego image of exceeding the range of gray scale will be problem [7]. So the APVD method will solve these problems with modulus function and some conditions. So the pixel values of stego image will not exceed the gray scale range. The hidden capacity of the APVD method will be equal to Wu-Tsai's PVD method with satisfactory stego image quality.

M.Padmaa and Dr.Y.Venkataramani proposed data hiding scheme by using Zig Zag Traversing Scheme (ZZTS) [8]. This scheme is succeeded by taking difference value of three and two neighboring pixels in cover images. In this method zig zag scanning improves security and the quality of stego image with high capacity of concealed information and it also has hamming code for error corrections for reliable secret communication.

In the Improved Exploiting Modification Directions (EMD) method [9] one secret bit are embedded with one pixel of cover image. This EMD method one to one embedding of secret bits is attained so capacity of embedding secret bits in this method very high. The experimental result of this method has shown that

average Peak Signal Noise Ratio (PSNR) values for limited payload can be obtained. Also original EMD method was applied only for gray images.

Color image steganography based on PVD [10] method solves the problem of overflow in pixel values of images. This method gives good security than the PVD used in gray images and also provides better visual stego image.

3. Proposed Pixel Value Modification Method by Modulus 3 Function

The proposed pixel value modification method (PVM) Method divides cover image into three color planes (Red, Green and Blue). Every pixel contains 24 bits (for 8-bit representation) each one as 8 bit components in pixel. In the proposed method, all the three components have been used for data embedding. First, each color component from a pixel is separated and three separate M*N matrix is obtained.

Pixel value modification method for data hiding in each plane in a sequencing manner is carried out. First embedding of bits in 1st pixel of the red component matrix, then in 1st pixel of green component matrix and lastly in blue component matrix is done. Further embedding of different number of bits for different component pixel for increasing security, capacity and also improving the visual quality is carried out.

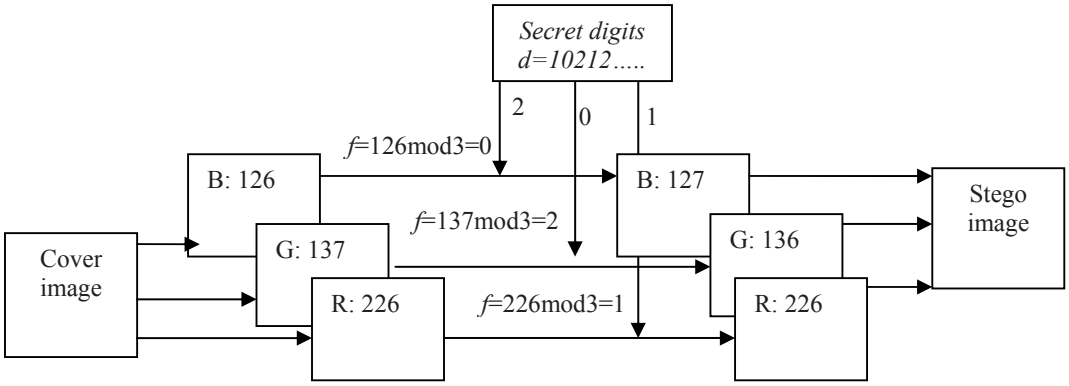


Fig1. An example for the Embedding of PVM method

3.1 Embedding Procedure

Step 1: Separate the color image into three component color matrix and apply the following steps on each of them sequentially i.e. apply following steps on 1st pixel value of Red matrix, then 1st pixel value of Green matrix and finally on Blue matrix continue the same procedure for 2nd pixel value of each plane and so on.

Step 2: Let a secret digits is *d*. secret data are converted into base 3 values of (0, 1, 2). These secret values are embedded into three planes.

Step3: Pixel values of the image matrix are grouped into $g_1, g_2, ..., g_n$. Decimal value of Red pixel is represented by g_{ri} , similarly decimal value of Green and Blue are represented as g_{gi} and g_{bi} where the function f is calculated by Eq. (1) for each planes.

$$f=f(g_1,g_2,g_3,\ldots\ldots g_n)=\sum_{i=1}^{n} g_{ri} \bmod 3 \quad (1)$$

Step4: The appropriate pixel for PVM method to be selected for embedding should fall in the range of $0 \leq g_i \leq 250$ of cover image are appropriate pixels for pixel value modification method. The function *f* has three cases.

Case 1: If $f = d$, then

Modification is not needed, directly g_{ri} is taken as new pixel value g_{ri}'

Case 2: If $f \neq d$ and $f < d$, then

Increase the value of g_{ri} by 1, $g_{ri}' = (g_{ri} + 1)$ then new modified pixel value is obtained.

Case 3: If $f \neq d$ and $f > d$, then

The value of g_{ri} is decreased by 1, $g_{ri}' = (g_{ri} - 1)$ then new modified pixel value is obtained.

Step 5: Similarly repeat the step 3 and 4 for pixel value modification in green and blue matrix of cover image.

Step 6: After modification of pixel value with secret data in RGB planes combination these RGB planes gives stego image the resultant stego image.

3.2 Extracting Procedure

Step 1: Divide the stego image into three component planes Red, Green and Blue. Now, in the received the stego image will select the pixel value which is falls in between $0 \leq g_i \leq 253$ in RGB plane.

Step 2: Pixel values of the Red plane are extracted and Eq. (2) will gives a secret digit d.

$$d = g_{ri}' \ mod3 \qquad (2)$$

Step 3: Similarly secret digits of green and blue planes are also extracted by same way starting from 2nd pixel value of each plane and so on. Finally secret digits of base 3 are obtained which is converted into original secret data.

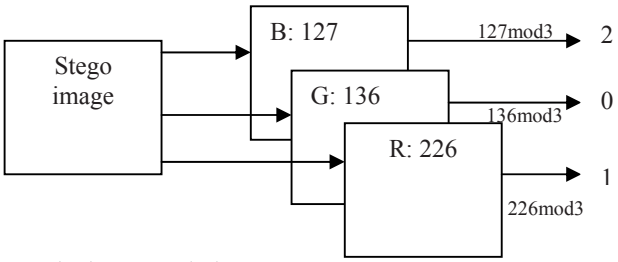


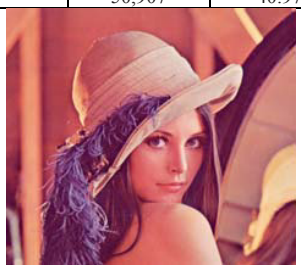
Fig2. An example for the Extracting in PVM method

4. Experimental Results

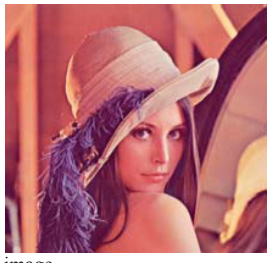
The proposed PVM method hides secret data into RGB planes of cover color image. The problem of overshooting 0~ 255 ranges for each component pixels, which is in the existing PVD method has been removed here. This PVM method results better visual quality of the stego image. Fig.3. show the cover images and their Stego images. The test images chosen are Lena, Airplane, Baboon and Pepper images. The comparison results, of message payload and PSNR value, between PVM method and PVD methods is shown in Table 1. The histogram analysis was performed on the cover image and stego image. Fig.3 shows the minimum changes in the histogram of stego images when compared to the cover images histogram. This shows that a steganalyst will not be able to find out the hidden message easily. The proposed method histogram was found to be almost alike to the cover image. This PVM method results in less distortion of the pixels in stego image. Also it provides more security because different number of bits has been hidden in different planes of an image pixel, so it has hard to trace how many bits are hidden within a pixel. As a result the distortion of the pixel value in the stego image will be less and it has no remarkable effects in histogram and also in visual quality of color images.

Table1. The Results of Comparison of the proposed method with Existing PVD methods

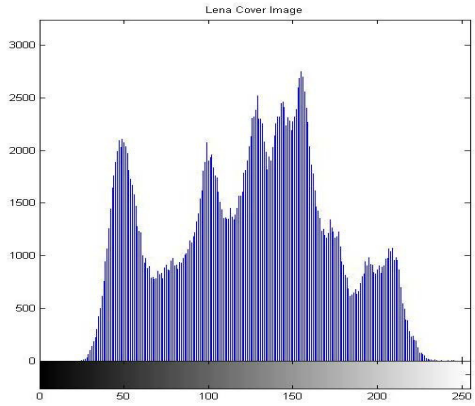
Cover image	Wu and Tsai`s method (PVD)		Tri way PVD method (TPVD)		Proposed method (PVM)	
	Payload (bytes)	PSNR	Payload (bytes)	PSNR	Payload (bytes)	PSNR
Lena	51,219	41.79	75,836	38.89	83,654	45.0926
Baboon	57,146	37.90	82,407	33.93	91,286	39.0633
Airplane	51,224	40.60	76,352	38.70	81,851	43.9345
Pepper	50,907	40.97	75,579	38.50	78,612	42.0500

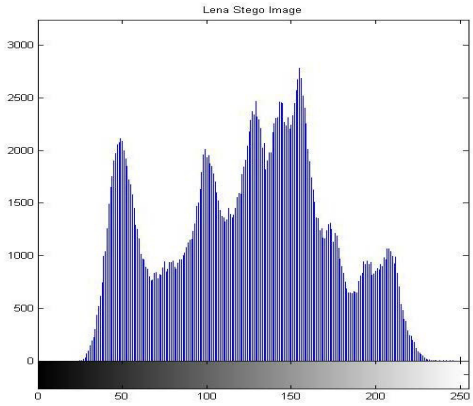


(a) Lena image



(b) Stego Lena image



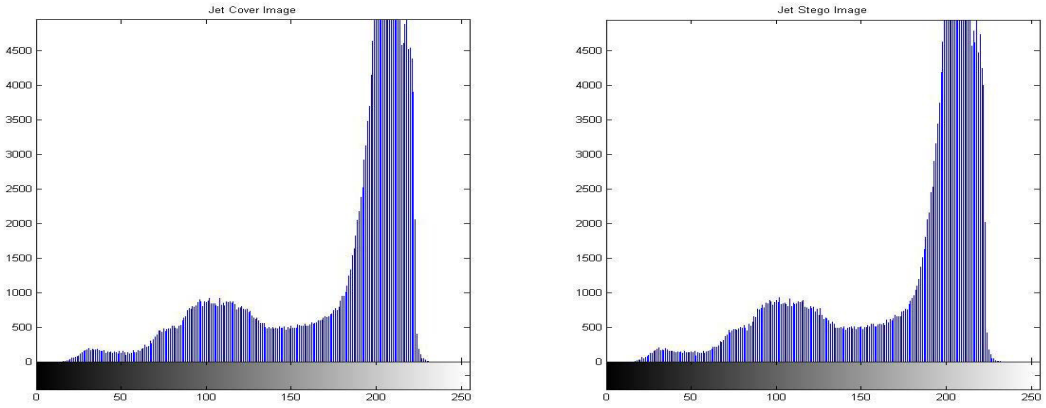


(i) Histogram of Cover Lena and Stego Lena image

Figure 3(a)

(a)Airplane image

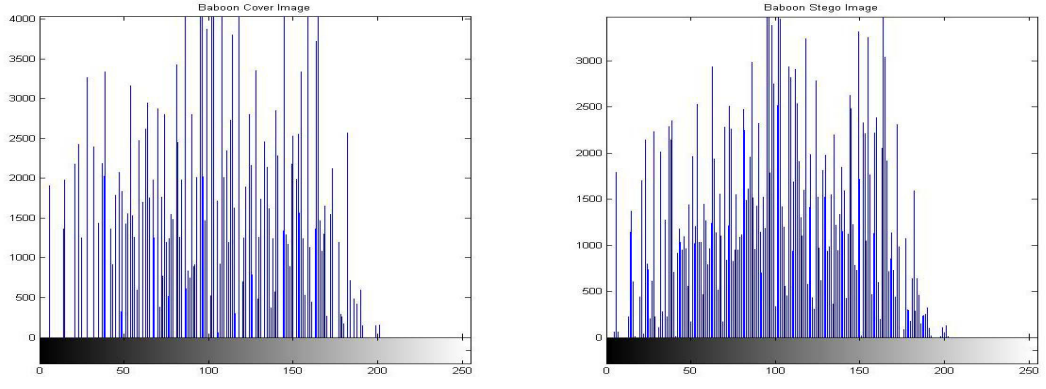
(b) Stego Airplane image



(ii) Histogram of Cover Airplane and Stego Airplane

Figure3 (b)

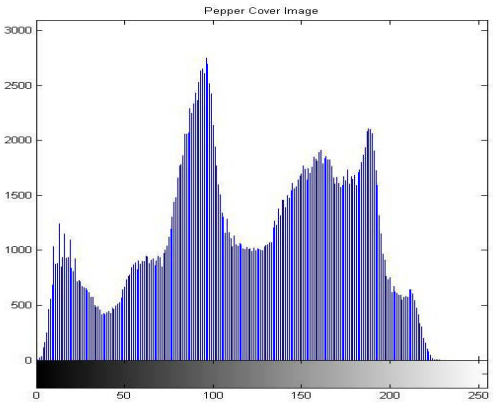
(a)Baboon image (b) Stego Baboon image

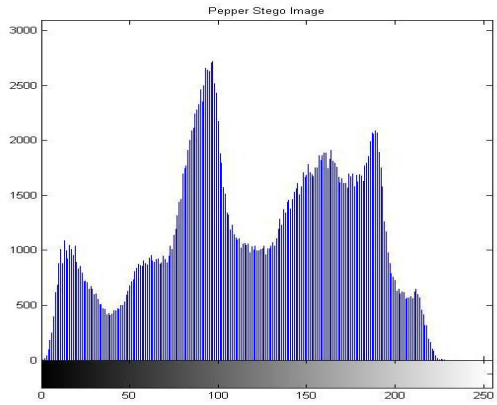


(iii) Histogram of Cover Baboon and Stego Baboon

Figure 3 (c)

(a) Pepper image (b) Stego Pepper image





(iv) Histogram of Cover Pepper and Stego Pepper image

Figure 3 (d)

Fig.3. Cover images, Stego image and their corresponding histogram of Cover images and Stego images

5. Conclusions

In this paper, proposed PVM steganography method for data hiding by using pixel value modification with modulus function in color images was done. This method also guarantees that no pixel value will exceed the range 0 to 255 in stego image. In the existing PVD embedding methods, only one secret digit was embedded for two consecutive pixels, but the proposed PVM method, embeds one secret digit in only one pixel. Proposed method on color images gives more capacity and security than the PVD methods. It also provides better visual quality of stego image. Moreover, proposed method extracts the hidden secret message efficiently without using the range tables.

References

[1] R. J. Anderson and F. A. P. Petitcolas, “On the limits of steganography”. IEEE Journal on Selected Areas in Communications, pages 474–481, 1998.
[2] C.K. Chan, L.M. Cheng,” Hiding data in images by simple LSB substitution”, pattern recognition vol. 37, Issue 3,pp. 469-474, 2004.

[3] D.C. Wu, and W.H. Tsai, “A Steganographic method for images by pixel-value differencing”, Pattern Recognition Letters, Vol. 24, pp. 1613-1626, 2003.
[4] 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,” IEE Proceedings on Vision, Image and Signal Processing, Vol. 152, No. 5, pp. 611-615, 2005.
[5] C.M. Wang, N.I. Wu, C.S. Tsai, M.S. Hwang, “A high quality steganography method with pixel-value differencing and modulus function”, Journal of System Software, Vol.81, No.1, pp.150–158, 2008.
[6] K.C. Chang, C.P Chang, P.S. Huang, and T.M. Tu, “A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing,” Journal of Multimedia, Vol. 3, No. 2, pp.37-44, June 2008.
[7] J.K. Mandal, Debashis Das “Steganography Using Adaptive Pixel Value Differencing (APVD) for Gray Images through Exclusion of Underflow/Overflow ”, Computer Science & Information Series, ISBN : 978-1-921987-03-8, pp. 93-102, 2012.
[8] M. Padmaa and Dr. Y. Venkataramani, “ZIG-ZAG PVD – A Nontraditional Approach,” International Journal of Computer Applications, Vol. 5, No. 7, pp. 5-10, August 2010.
[9] Ki-Hyun Jung and Kee-Young Yoo, “Improved Exploiting Modification Direction Method by Modulus Operation,” International Journal of Signal Processing, Image Processing and Pattern, Vol. 2, No.1, March, 2009.
[10] J. K. Mandal and Debashis Das, “Color Image Steganography Based on Pixel Value Differencing in Spatial Domain,” International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.