Australian Journal of Basic and Applied Sciences, 8(3) March 2014, Pages: 161-167

AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Adaptive Color Image Steganography Using Intra Color Pixel Value Differencing

[1]C. Prema and [2]Dr.D. Manimegalai

[1]Assistant Professor/HOD of CSE, JACSI College of Engineering, C. Prema, 628619, Nazareth, Tamil Nadu, India.
[2]Prof/Head of IT , National Engineering College, Dr. D. Manimegali, Kovilpatti, Tamil Nadu, India.

ARTICLE INFO

Article history:
Received 12 January 2014
Received in revised form 20 March 2014
Accepted 25 March 2014
Available online 2 April 2014

Keywords:
Steganography, Data hiding, RGB color image, intra color pixel value differencing, Stego-image, Steganalysis

ABSTRACT

Background: Steganography, which refers to the process of imperceptibility, embedding a secret message into a cover/host media so as to conceal the content of the message data. It has been widely regarded as a promising solution to multimedia security and privacy. The major objective of the steganography is to prevent some unintended observer from stealing or destroying the confidential information. **Objective:** A novel color image steganographic method using intra color pixel value differencing (ICPVD) is proposed in this paper. Every steganography method must have a tradeoff between capacity and imperceptibility to human vision and capacity and detectability. To embed secret data, each color components of rgb color image is partitioned into non-overlapping blocks of two consecutive pixels. The secret data is embedded into the color differences between (r,g),(g,b) and (b,r) pairs. By the use of all the three components of the cover image, hiding capacity is increased further. **Results:** Detectability of the proposed method is verified by using histogram and statistical chi-squared methods. Adaptive approach is also applied to reduce the stego image distortion. Experimental results show that the proposed method not only achieving better image quality but also provides high embedding capacity. **Conclusion:** The hiding capacity of the image depends on the difference between these intra color pixel differences. Less in difference is considered as smooth area in which less data can be hidden. On the reverse, more in difference means edge area in which more data can be hidden. So, the tradeoff between capacity and imperceptibility is achieved in this proposed method. Moreover, the proposed method provides nearly lossless extractions at the receiving side. Cover image knowledge is not needed to extract the secret data.

To Cite This Article: C. Prema and Dr.D. Manimegalai., Adaptive Color Image Steganography Using Intra Color Pixel Value Differencing, ***Aust. J. Basic & Appl. Sci.,*** *8(3): 161-167, 2014*

INTRODUCTION

As the use of intranet increases, we provide security to the information from unauthorized access, use, disruption, modification, recording or destruction. Generally two methods such as cryptography and steganography are used to provide security to the information. Cryptography is the art of secret writing which is intended to make a message unreadable by the third party but does not hide the existence of the secret communication. Steganography means hiding information in harmless carrier or cover such as text, audio, images, videos, VoIP etc. Anyone else viewing this media will fail to see that it contains hidden or encrypted data. Hiding messages in image files can be categorized into two as Spatial Domain Method and Frequency Domain Method.

A simple and well known spatial domain method is Least Significant Method (LSB). In LSB, the message is embedded into the LSB of each image pixel. The two major goals of image steganography is high hiding capacity and high imperceptibility. By the use of two or more LSBs of cover image (Feng J.B., Lin, I.C., Tsai, C.S., Chu, Y.P 2006 and Katzenbeisser, S., Petitcolas 2000) results in high hiding capacity with acceptable image quality. Maximum of three LSBs scheme is producing merely acceptable stego image (Nan-I Wu1 and Min-Shiang Hwang 2007). The effect of hiding of more data into cover image and robustness are analyzed and summarized by Liao et al (Liao, Z., Huang, Y., Li, C. 2007 and Wu, N.I., Hwang, M.S 2007). To improve the image quality, Chan and Cheng 2004 proposed a method of simple LSB with Optimal Pixel Adjustment (OPA). The experimental result of their method shows the resultant stego image which is visually indistinguishable from cover image. To improve the imperceptibility of stego image in LSB method, Lee and Chen 2000 proposed a variable size LSB with minimum error replacement method. More recently, Soleimanpour 2013 introduced a novel steganographic method based on genetic algorithm which improves the visual quality of the stego image. To achieve high imperceptibility, Wu and Tsai 2003 proposed a Pixel Value Differencing (PVD)

Corresponding Author: C. Prema Jayaraj Annapackiam CSI College of Engineering, CSE Department, C. Prema, 628 202, Nazareth, Tamil Nadu, India.
E-mail:jacsicecse@gmail.com

method, in which the secret message is embedded into the gray value difference of two consecutive pixels of the cover image.

To reduce the stego image distortion in PVD method, the new values are readjusted into the valid range. Due to readjustment, falling off boundary problems occurred in PVD. If the two pixels are in extreme edges or smooth area, this problem may be worsening the situation. To overcome this problem, C.M.Wang ,Nan-I Wu 2007 a uses PVD and modulus function. In their method, an optimal approach, the message can be embedded into the two pixels by modifying their remainder. To give resistant against PVD histogram analysis, new extension of PVD (EPVD) is proposed by ZaZamin Zaker and Ali Hamzeh, Seraj 2009. To achieve this, histogram's Gaussian step is presented. To increase the hiding capacity, they adapted range overlapping rules in which different values are to be shifted to the left neighbor range.

Major disadvantage of the PVD method is that the hiding capacity is moderate. To increase the hiding capacity of the stego image, Ko-Chin Changa and Chien-Ping Changa 2008 proposed a Tri Way Pixel Value Differencing method (TPVD). Instead of referring only one direction like conventional PVD, three different directional edges are considered. To reduce the image distortion in the stego image, an optimal approach of selecting the reference point and the adaptive rules are presented. R.Sridevi and G. John Babu 2012 proposed TPVD with modulus to produce more hiding capacity than TPVD.

Existing PVD methods even in low hiding capacity, some statistical artifacts will be inevitably introduced. Weiqi Luo and Fangjun Huang 2009 proposed a more secure steganography based on content adaptive scheme in which sharper edge regions are used first for data hiding. Hiding capacity of TPVD is further increased by the method proposed by Xin Liao and Qiao-yan Wena 2011. They proposed a method based on TPVD and modified LSB substitution. The resultant stego image produces acceptable image quality and also provides large hiding capacity.

In all the above mentioned PVD method, only two quantization range variables are used to increase capacity of the cover image and also provide better image quality. Hsien Wen, Tseng and Hui-Shih 2013 proposed a new method in which a new quantitation table is taken based on the perfect square number which is used to decide the payload. J.K.Mandal and Debashis Das 2012 proposed a color image steganography. By the use of three color components, hiding capacity in difference pixel components are usually increased. To provide more security, different number of bits in different components is used. In a color image steganography of J.K.Mandal and Debashis Das 2012 approach, PVD method is applied to each color components separately to embed the secret data. So this approach is similar to conventional PVD method. By the use of this conventional PVD method, considerable amount of distortion occurred by adjusting the consecutive pixels present in the three color components. To reduce this distortion, a novel approach is proposed in this paper. In this proposed method, intra color pixel differences between r-g, g-b, b-g are taken to hide the secret data. For hiding process, PVD method is applied to each intra color differences separately. No secret key is needed to select the color components. These intra color differences are taken in some order. Imperceptibility is improved by the use of PVD method. Security of the proposed method is tested by Histogram analysis and RS steganalysis. PSNR is also calculated to evaluate the stego image quality.

The rest of this paper is organized as follows. In section 2, the proposed method is given both for hiding and extracting algorithm. Experimental results and analysis are discussed in section 3. Conclusion and future work is presented in section 4.

Proposed Method:

In this proposed method, the color image is considered as cover. The intra color differences between the two successive pixels of the color cover image are used to hide the secret data. By the use of all three color components, the capacity of this proposed method is higher than the PVD method.

2.1 Hiding Algorithm:

1. Extract the three color components from the color cover image to get three M*N matrix. Pick two successive pixels from each color components say (R_i, R_{i+1}), (G_i, G_{i+1}), (B_i, B_{i+1}).
2. Calculate the differences d_0, d_1, d_2
3. Locate the suitable range for d_i (i=0, 1, 2) in the designed range table. It is denoted as $R_{j,i}$.
4. Compute the amount of secret bits t_i by using

$$t_i = \lfloor \log_2 w_{i,j} \rfloor \quad (1)$$

where $w_{i,j}$ is the width of the range table.

5. Read t_i bits from the secret data and convert into their equivalent decimal value b_i
6. Calculate the new difference by

$$d_i' = l_{j,i} + b_i \quad if\ d_i \geq 0$$
$$d_i' = -(l_{j,i} + b_i) \quad if\ d_i < 0 \quad (2)$$

where $l_{j,i}$ is the lower level in the selected range in which d_i is located.

Australian Journal of Basic and Applied Sciences, 8(3) March 2014, Pages: 161-167

7. Modify the values of (R_i, R_{i+1}), (G_i, G_{i+1}), (B_i, B_{i+1}).

$$P_0(1,2) = (R_i', G_{i+1}') = R_i - \lceil m_0/2 \rceil, G_{i+1} + \lfloor m_0/2 \rfloor$$
$$P_1(1,2) = (G_i', B_{i+1}') = G_i - \lceil m_1/2 \rceil, B_{i+1} + \lfloor m_1/2 \rfloor$$
$$P_2(1,2) = (B_i', R_{i+1}') = B_i - \lceil m_2/2 \rceil, R_{i+1} + \lfloor m_2/2 \rfloor \quad (3)$$

where $m_i = d_i - d_i'$

8. Steps 1 to 7 are repeated until all the secret bit streams are embedded.
9. To avoid falling-off boundary problems, the following two situations are considered.

Case 1: If $P_0 \cong 0, P_1 \cong 0, P_2 \cong 0$ and $P_0 < 0$ or $P_1 < 0$ or $P_2 < 0$, readjust P_0, P_1, P_2 by

$$P_0'(1,2) = P_0(1) + (2^{t_i})/2, P_0(2) + (2^{t_i})/2$$
$$P_1'(1,2) = P_1(1) + (2^{t_i})/2, P_1(2) + (2^{t_i})/2$$
$$P_2'(1,2) = P_2(1) + (2^{t_i})/2, P_2(2) + (2^{t_i})/2 \quad (4)$$

Case 2: If $P_0 \cong 255, P_1 \cong 255, P_2 \cong 255$ and $P_0 > 255$ or $P_1 > 255$ or $P_2 > 255$, readjust P_0, P_1, P_2 by

$$P_0'(1,2) = P_0(1) - (2^{t_i})/2, P_0(2) - (2^{t_i})/2$$
$$P_1'(1,2) = P_1(1) - (2^{t_i})/2, P_1(2) - (2^{t_i})/2$$
$$P_2'(1,2) = P_2(1) - (2^{t_i})/2, P_2(2) - (2^{t_i})/2 \quad (5)$$

The proposed hiding process as given in figure 4 is illustrated by one example.

2.2 Extraction Algorithm:

1. Extract the three color components R, G, B from the given stego image.
2. Calculate the intra color differences between the color components as in hiding process.

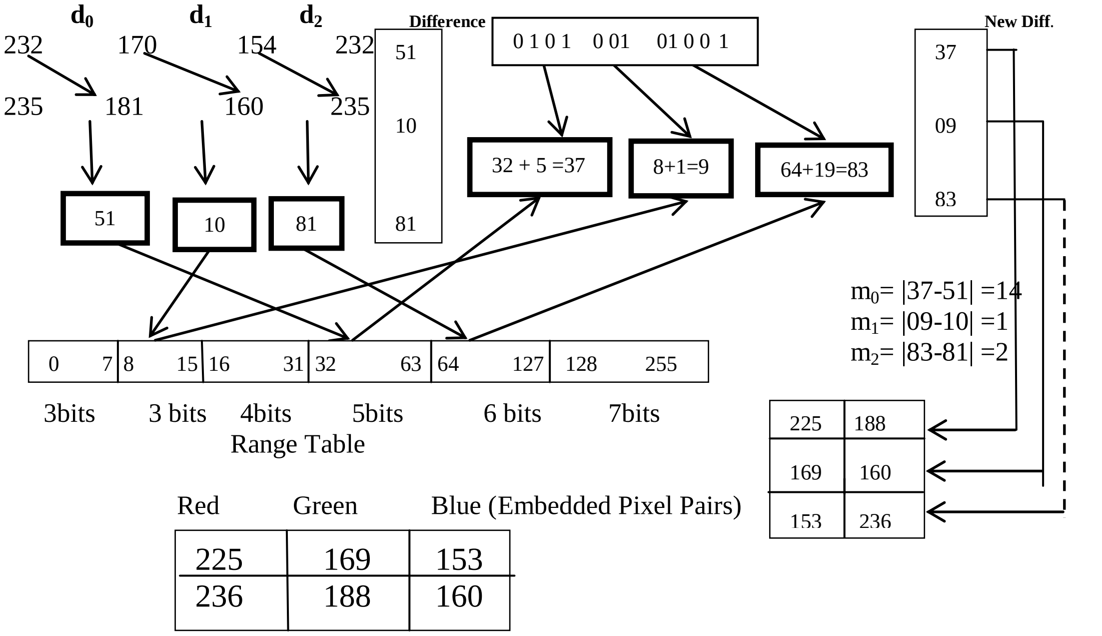
$$d_0' = R_i' - G_{i+1}'$$
$$d_1' = G_i' - B_{i+1}'$$
$$d_2' = B_i' - R_{i+1}' \quad (6)$$

3. Identify the suitable ranges for d_0', d_1', d_2' in the range table which is used in hiding process.
4. Calculate the amount of secret bits t_i by $t_i = \lfloor \log_2 w_{j,i} \rfloor$
5. The lower limit $l_{j,i}$ is subtracted from d_i to obtain b_i
6. Finally b_i' is converted to its corresponding decimal value for b_i data bits.

The extraction of secret data from the above illustrated example is explained here.

$$d_0' = |225 - 188| = 37$$
$$d_1' = |169 - 160| = 09$$
$$d_2' = |153 - 236| = 83 \quad (7)$$

Subtracting these values from the lower limits 32, 8, 64, we get the binary values as 5,1,19. The corresponding binary values 0101,001,010011 with length of 4, 3, and 6. So, the secret bit stream is 0101000110011 as we used in hiding process.



Red	Green	Blue
225	169	153
236	188	160

Fig. 4: Proposed Method for Hiding Process (Illustrative Example).

7. Experimental Results and Discussion:

To demonstrate the performance of the proposed approach, different experiments have been done for nine test images used by existing methods. Experimental result shows that the proposed method can perform better than PVD method (Wu, D.C., Tsai, W.H 2003), Chung-Ming Wang 2007 method and TPVD method 2008. The range table R has six sub ranges such as R_1 [0-7], R_2 [8-15], R_3 [16-31], R_4[32-63], R_5[64-127], R_6 [128-255]. The width of these ranges are 8, 8,16,32,64,128 respectively. To evaluate the stego image quality, the Signal to Noise ratio (PSNR) was calculated for stego images. It is defined as

$$PSNR = 10\log_{10}(255^2/MSE) \text{ dB} \quad (8)$$

$$MSE = \frac{1}{MXN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(\alpha_{i,j} - \beta_{i,j}\right)^2 \quad (9)$$

where $\alpha_{i,j}$ the pixel of the cover image and $\beta_{i,j}$ is the pixel of the stego image.

For color image the MSE is calculated for each color components separately. The average (mean) of these three values gives the MSE of the color image.

MSE (color image)=(mseR + mseG + mseB)/3 (10)

For larger PSNR value, imperceptibility of the stego image is good. For easy comparison, the color stego image is converted into gray scale image. The results in a, d of figure 5 are the stego images of the proposed method and in b, e and c, f are the images by Wu &Tsai method and Chung Ming Wange method respectively. The PSNR obtained from this proposed method is better than the other two methods.

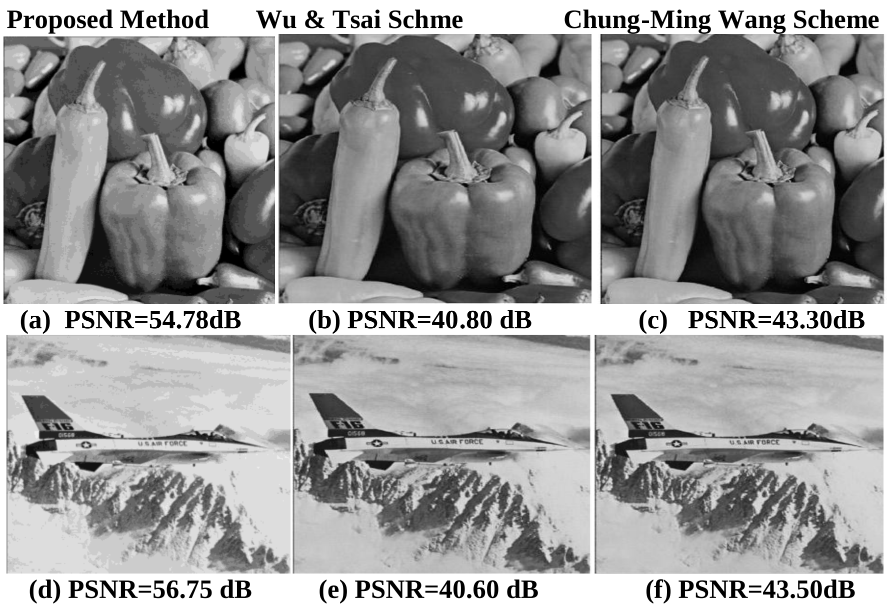


Fig. 5: Size of the image 256X256 (a), (d)- stego images of the proposed method (b),(e)and (c),(f) are the images by Wu &Tsai method and Chung Ming Wange method respectively.

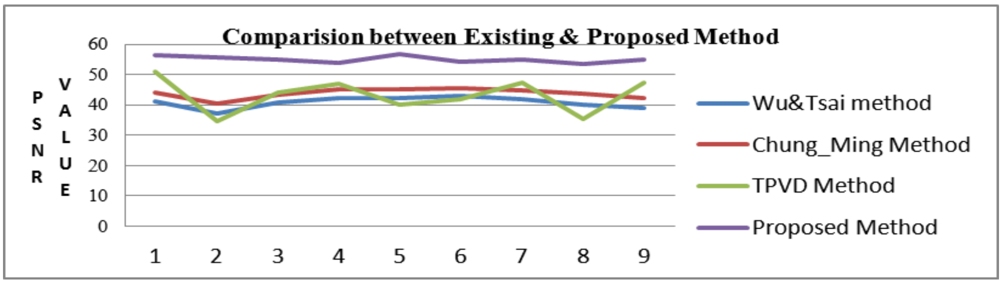


Fig. 6: Comparisons between Existing & Proposed Method.

The comparison chart in figure 6 is provided for the proposed and existing methods between the PSNR values and the images taken for analysis. It proves the goodness of the proposed method. In table 1, the PSNR values of the proposed method and the other two methods are given. It is increased by 3 to 14dB, because the distortion in edges is reduced by adaptive adjustment. In figure 7, the color cover image and stego images are given. No visible difference was seen between these two. So the imperceptibility of the proposed method is good. Finally the proposed method is also compared with TPVD. PSNR values in table 2 shows the improvement of the proposed method. Capacity and Computational time of the two methods are also given. The proposed method has high hiding capacity with small increase in time.

Table 1: PSNR values comparison between the proposed and existing methods.

S. No	Image Name	Wu & Tsai Method		Chung-Ming Wang Method		Proposed Method	
		Capacity (Bytes)	PSNR (dB)	Capacity (Bytes)	PSNR (dB)	Capacity (Bytes)	PSNR (dB)
1.	Lena	51,219	41.1	51,219	44.1	202569	56.48
2.	Babbon	57,146	37	57,146	40.3	181720	55.74
3.	Peppers	50,907	40.8	50,907	43.3	203549	54.78
4.	Tank	50,449	42.4	50,449	45.3	180766	53.87
5.	Airplane	49,739	42.2	49,739	45.2	161778	56.75
6.	Truck	50,065	42.9	50,065	45.6	172735	54.38
7.	Elaine	51,074	41.9	51,074	44.8	172896	55.04
8.	Couple	51,603	40.2	51,603	43.5	186792	53.45
9.	Boat	52,635	38.9	52,635	42.1	190869	54.83

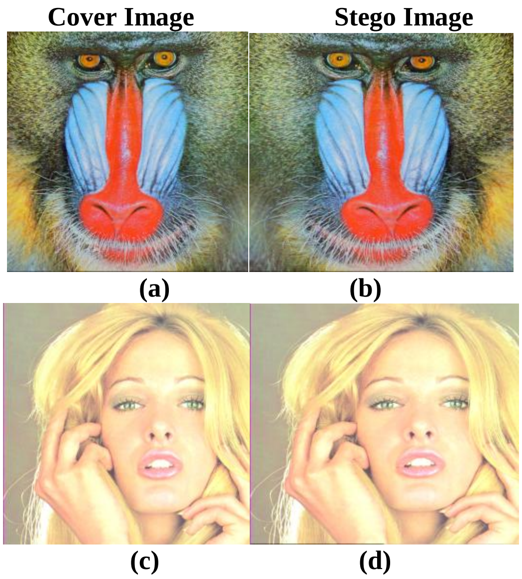


Fig. 7: (a) & (b) cover and stego image of baboon and (c) & (d) Cover and stego image of Elaine

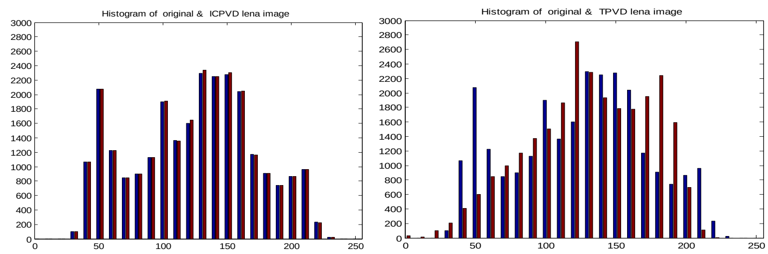


Fig. 8: (a) Histogram of proposed method (b) Histogram of TPVD method.

Table 2: Comparison between the proposed and TPVD method.

S. No	Image Name	TPVD Method			Proposed Method		
		Capacity (Bytes)	PSNR (dB)	Elapsed Time (sec)	Capacity (Bytes)	PSNR (dB)	Elapsed Time (sec)
1.	Lena	76162	50.83	11.43	202569	56.48	14.9
2.	Babbon	83814	34.63	8	181720	55.74	15.93
3.	Peppers	76000	43.88	10.1	203549	54.78	18.85
4.	Tank	75351	46.83	12.37	180766	53.87	14.7
5.	Airplane	59731	40.21	11.26	161778	56.75	14.28
6.	Truck	76581	41.97	9.98	172735	54.38	14.8
7.	Elaine	76657	47.36	10.76	172896	55.04	18.41
8.	Couple	77654	35.23	9.46	186792	53.45	15.34
9.	Boat	78031	47.17	10.91	190869	54.83	15.3

For analysis purpose, the histogram between the original cover image and stego image of Lena image is taken. Figure 8, (a) shows the histogram of the proposed method and (b) is the histogram of the TPVD method.

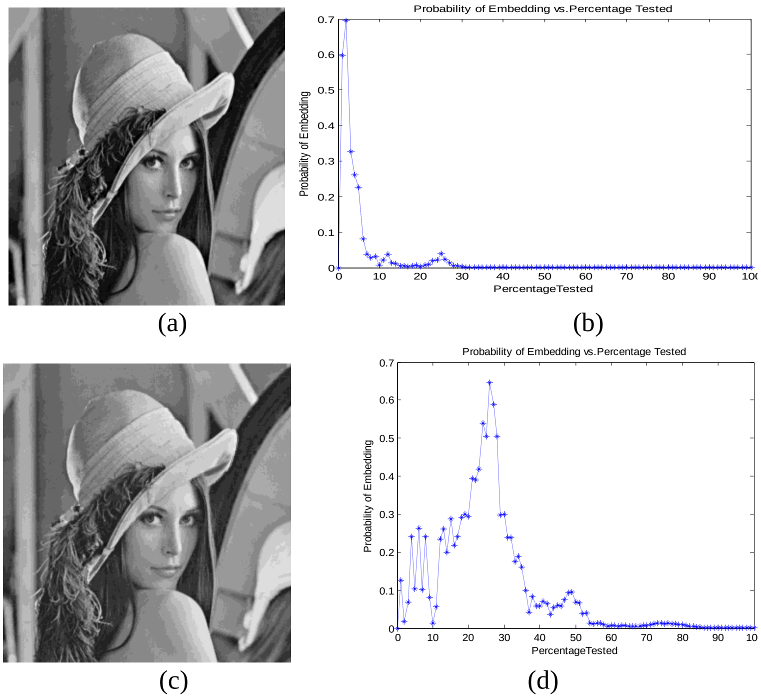


Fig. 9: (a) Lena stego image (b) Chi-Squared attack output of proposed method and (c) Lena stego image (d) Chi-Squared attack output TPVD method

5. Conclusion:

By the perfect utilization of three color components, the hiding capacity of the proposed method is increased than TPVD method. Adaptive adjustment of pixels after hiding reduces the image distortion significantly. Experimental results show the imperceptibility of the stego image while compared with the cover image. Also the detectability of this proposed method is very less for large capacity. So the two trade-off of steganography is achieved by this proposed method. In future work, variable range table may be taken to increase its robustness against steganalysis. Besides random selection of color components by secret key may also be taken in future work to get high robustness. Also the extraction of embedded data can work well without the knowledge of cover image in this proposed method. In future, this proposed method may be applied in object oriented image steganography to increase its robustness.

REFERENCES

Chan, C.K., L.M. Cheng, 2004. ‘Hiding data in images by simple LSB substitution,’ *Pattern Recognition*, 37(3): 469-474.

Chung-Ming Wang a, Nan-I Wu a, Chwei-Shyong Tsai b, Min-Shiang Hwang, 2007. ‘A high quality steganographic method with pixel-value differencing and modulus function’ *The Journal of Systems and Software* xxx.

Feng, J.B., I.C. Lin, C.S. Tsai, Y.P. Chu, 2006. ‘Reversible watermarking: current status and key issues’, *International Journal of Network Security* 2: 161-170.

Hsien-Wen Tseng and Hui-Shih, 2013. ‘A steganographic method based on pixel-value differencing and the perfect square number’ *Journal of Applied Mathematics*, Article ID 189706, 8 pages.

Katzenbeisser, S., F.A.P. Petitcolas, 2000. ‘Information Hiding Techniques for Steganography and Digital Watermarking.’ *Artech House Inc*., Boston.

Ko-Chin Changa, Chien-Ping Changa, Ping S. Huangb and Te-Ming Tu, 2008. ‘A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing’ *journal of multimedia*, 3(2).

Lee, Y.K., L.H. Chen, 2000. ‘High capacity image steganographic model,’ *IEE Proceedings on Vision, Image and Signal Processing*, 147(3): 288-294.

Liao, Z., Y. Huang, C. Li, 2007. ‘Research on data hiding capacity’, *International Journal of Network Security 5* September, 140-144.

Mandal, J.K. and Debashis Das, 2012. ’Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain’ *International Journal of Information Sciences and Techniques* (IJIST), 2(4).

Nan-I Wu1 and Min-Shiang Hwang, 2007. ‘Data Hiding: Current Status and Key Issues’ *International Journal of Network Security*, 4(1): 1-9.

Nazanin Zaker, Ali Hamzeh, Seraj Dean Katebi, Shadrokh Samavi, 2009. ’Improving Security of Pixel Value Differencing Steganographic Method’ *IEEE-*.

Soleimanpour, M., S. Talebi and H. Azadi-Motlagh, 2013. ‘A Novel Technique for Steganography Method Based on Improved Genetic Algorithm Optimization in Spatial Domain’ *Iranian Journal of Electrical & Electronic Engineering*, 9(2).

Sridevi, R. and G. John Babu, 2012. ‘Multi pixel Steganography’, (IJCSIS*) International Journal of Computer Science and Information Security*, 10(6): 61-66.

Weiqi Luo, Fangjun Huang, Jiwu Huang, 2009. ‘A more secure steganography based on adaptive pixel-value differencing scheme’ *Springer Science+Business Media*, LLC.

Wu, D.C., W.H. Tsai, 2003. ‘A steganographic method for images by pixel-value differencing’, *Pattern Recognition Letters*, 24: 1613-1626.

Wu, N.I., M.S. Hwang, 2007. ‘Data hiding: current status and key issues’, *International Journal of Network Security*, 4: 1-9.

Xin Liao and Qiao-yan Wena, Jie Zhang, 2011. ‘A steganographic method for digital images with four-pixel differencing and modified LSB substitution’ *Vis. Commun. Image R*., 22: 1-8.