ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Image Steganography Methods Based on Pixel Value Differencing: Review and Proposal for Enhancing the Security of Five Pixel Pair Algorithm

Nayana Kolhe[1], Harish Barapatre[2]

M.E. Student, Department of Computer Engineering, Y.T.I.E.T, Bhivpuri Road, Maharashtra, India[1]

Assistant Professor, Department of Computer Engineering, Y.T.I.E.T, Bhivpuri Road, Maharashtra, India[2]

ABSTRACT: Now a days, message transmission has become rapid and convenient using Internet as the communication channel. Since Internet is an open channel of communication, there is always a threat of stealing the information. This is why security of information is regarded as one of the most important factors of information and communication technology. Steganography is a technique which hides secret information into a cover media or carrier for transmitting secret data to the desired destination stealthily. The pixel-value differencing (PVD) method is a spatial domain steganographic method that provides higher embedding capacity and produces good quality stego images. The PVD approach groups two consecutive pixels either in vertical or horizontal direction to form a pixel pair. The difference of pixl values in the pair is used to hide the secret information.

KEYWORDS: Internet, PVD, Steganography, LSB substitution

I. INTRODUCTION

Steganography is generally used in secret communication between acknowledged parties. It uses unsuspected multimedia object to hide the secret information. A Steganography uses the bits of the cover object, such as a graphic or an audio file, to hide the secret data. The unused or insignificant bits of the cover media are replaced with the secret data.

The PVD approach of image steganography improves the data hiding capacity of cover the images and produces good quality of stego images. In pixel value differencing approach, the difference value between two consecutive pixels is regarded as a feature for recording the secret message. When the original difference value is unequal to the secret message, the values of two consecutive pixels are directly adjusted so that their difference value stands for the secret data.

II. RELATED WORK

In pixel value differencing approach, the difference value between two consecutive pixels is regarded as a feature for recording the secret message. When the original difference value is unequal to the secret message, the values of two consecutive pixels are directly adjusted so that their difference value stands for the secret data.

In the PVD method, a gray-valued cover image is partitioned into non-overlapping blocks composed with twoconsecutive pixels,PB_{iB} and PB_{i+1B}. For each block, a difference value dB_{iB} is calculated by subtracting PB_{iB} from PB_{i+1B}. Since the pixel values ranges from 0 to 255, the set of all difference values also ranges from -255 to 255. Therefore, $|dB_{iB}|$ ranges from 0 to 255. A range table with n contiguous ranges (RB_{kB} where k = 1,2,3,…..,n) is designed with table range from 0 to 255. It is necessary to use the same range table for hiding the secret data in the cover image and extract the secret data from the stego image. The lower and upper boundary of the range RB_{kB} are

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

denoted by lB_{kB} and uB_{kB}, respectively, then $RB_{kB} \in [lB_{kB}, uB_{kB}]$. The width wB_{kB} of RB_{kB} is calculated as $wB_{kB} = uB_{kB} - lB_{kB} + 1$. The width wB_{kB} is used to decide the number of secret information bits to be hidden in the block. The difference value $|d_i|$is used to locate the range R_k from the range table. The width w_k is used to estimate number of secret information bits (t_i) to be hidden in the block where $t_i = \lfloor \log_2 w_k \rfloor$.Then t_i bits are read from the binary secret data and transformed into a decimal value b. The new difference value $d'_i$is calculated as $d'_i = l_i + b$. The two pixel values are modified so that the difference is d'_i. The process is repeated until all the secret data is hidden in the cover image. The stego image is then constructed with the modified pixel values.

For extracting the secret information, the stego image is partitioned into pixel blocks using the same approach used in the embedding process. Then the difference value $d'_i$for each block of two consecutive pixels $P_i$and P_{i+1} in the stego-image is calculated. Then $|d'_i|$ is used to locate the suitable range R_k. Subtract l_i from d'_i to obtain b'. b' represents the secret data in decimal form. Therefore, b' is transformed into a binary sequence with t_i bits. This binary sequence stands for the original secret data. This process is repeated until all the secret data hidden in the stego image is extracted. [1,2].

A. *Methods with PVD and LSB substitution*

A steganographic method based on least-significant-bit (LSB) replacement and pixel-value differencing (PVD) method is presented by Wu et.al [2]. The range table is divided into lower level (smooth area) and higher level (edged area). In the smooth areas, 6 bits of the secret data is hidden into the cover image by LSB method while in the edged area, secret data is hidden using the PVD method. Ki-Jong Kim et. al. [3] has proposed a high capacity data hiding method with PVD and LSB substitution. The method differentiates the difference between two consecutive pixels as smooth area or edged area. M. Khodaei et.al. [4] has presented a new adaptive data-hiding method based on least-significant-bit (LSB) substitution and pixel value differencing (PVD) for gray-scale images. In the embedding process, the division Div between lower level and higher level is assumed. AwadKh. Al-Asmari et.al. [5],Xin Liao et.al. [6], M.B. OuldMedeniet al.[7,8] has also presented steganography methods based on PVD and LSB substitution.

B. *Methods with PVD and modulus function*

Chung Ming Wang et. al. [9] has proposed a high quality steganographic method with pixel-value differencing and modulus function. PVD technique is used to calculate the difference between two consecutive pixels. The remainder of two consecutive pixels is calculated by modulus operation. The remainder is modified to hide the secret data in two consecutive pixels. Fen Pang et al. [10] has proposed a method that uses modulus function in horizontal direction and PVD method in vertical direction to hide the secret information. Jeong-Chun Joo et. al. [11], Manjunath Gadiparthi et. al. [12] and Min-Yen Chiu et. al. [13] has proposed PVD based steganography methods with use of modulus function

C. *Method with PVD and chaotic map*

El-Sayed M. El-Alfy et.al. [14] has proposed a method based on PVD and chaotic map. The method increases security against the histogram analysis and adds another level of challenge for extracting the secret message by the steganalyzer

D. *Tri Pixel Value Difference Method*

In this method, data can be hidden in vertical and diagonal edges along with the horizontal edges. [15,17] The cover image is divided into non-overlapping blocks of 2 × 2 pixels to form 4 pixel pairs. But changing of pixel values for the fourth pixel pair affects the first and the second pairs, the fourth pair is useless and is discarded. Therefore, only three pairs are used to embed the secret data. P. Mohan Kumar Uet.al.U [18] has proposed a secure image steganographic system using TPVD adaptive LSB matching revisited algorithm for maximizing the embedding rate.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

E. *Five pixel pair differencing*

Gulve et. al. [19] has proposed the steganography method with five pixel pair differencing approach. The objective of the method is to increase the hiding capacity of the cover image and provide security to the hidden secret information. The cover image is partitioned into blocks of 2 x 3 pixels. The five pixel pairs are formed as (P(x,y),P(x,y+1)), (P(x,y+2),P(x,y+1)), (P(x+1,y),P(x,y+1)), (P(x+1,y+1),P(x,y+1)) (P(x+1,y+2),P(x,y+1)).

PX_0 $P_{(x,y)}$	PX_1 $P_{(x,y+1)}$	PX_2 $P_{(x,y+2)}$
PX_3 $P_{(x+1,y)}$	PX_4 $P_{(x+1,y+1)}$	PX_5 $P_{(x+1,y+2)}$

Fig.1. Pixel box

The whole cover image is divided into number of such blocks and for all the blocks the same approach is used for forming the pixel pairs. As shown in figure 1, pixel P(x,y+1) is used as the common pixel.

The embedding process begins with hiding 3 secret message bits in the common pixel using simple LSB substitution method. The three rightmost bits of common pixel are replaced with 3 bits of binary sequence of secret message. The common pixel with its modified value is used to form five pixel pairs with remaining five pixels in the block. The secret data is hidden in the five pairs using the PVD approach. At the end a new block is constructed with new values assigned to all the pixels. The new value assigned to the common pixel may be different than assigned to it after embedding 3 secret message bits into it using LSB substitution method. Accordingly, two-step pixel value adjustment process is carried out and the difference d'_i is maintained for all the pixel pairs PB_{iB}'s in the block. During extraction, the secret data is first extracted from the common pixel and then the PVD approach is used for extracting secret data from the five pairs in the block.

III. COMPARISON OF RESULTS

The results of various image steganography methods based on pixel value differencing are compared. For the purpose of comparison, the three standard images, Lenna, Baboon and Pepper are used. The resolution of the test images is 512 x 512 pixels.

Cover image	PVD Method		TPVD Method		FPPD method LSB sub		FPPD method Grey code	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Lena	50960	41.79	75836	38.89	97558	41.57	81631	42.46
Baboon	56291	37.90	82407	33.93	98017	41.03	82115	41.69
Peppers	50685	41.73	75579	38.50	97576	41.53	81650	42.38

Table 1. Comparison of hiding capacity in bytes

IV. PROPOSED SYSTEM

The proposed system enhances the stenographic algorithm proposed by Gulve et. al. [19] by making it more secure in following ways –

The selection of the common pixel is randomized based on a random number generated from pseudo random number generator function.

The secret message is first scrambled by XORing it with a number generated through pseudo random number generator function. The scrambled message is then embedded in the cover image.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

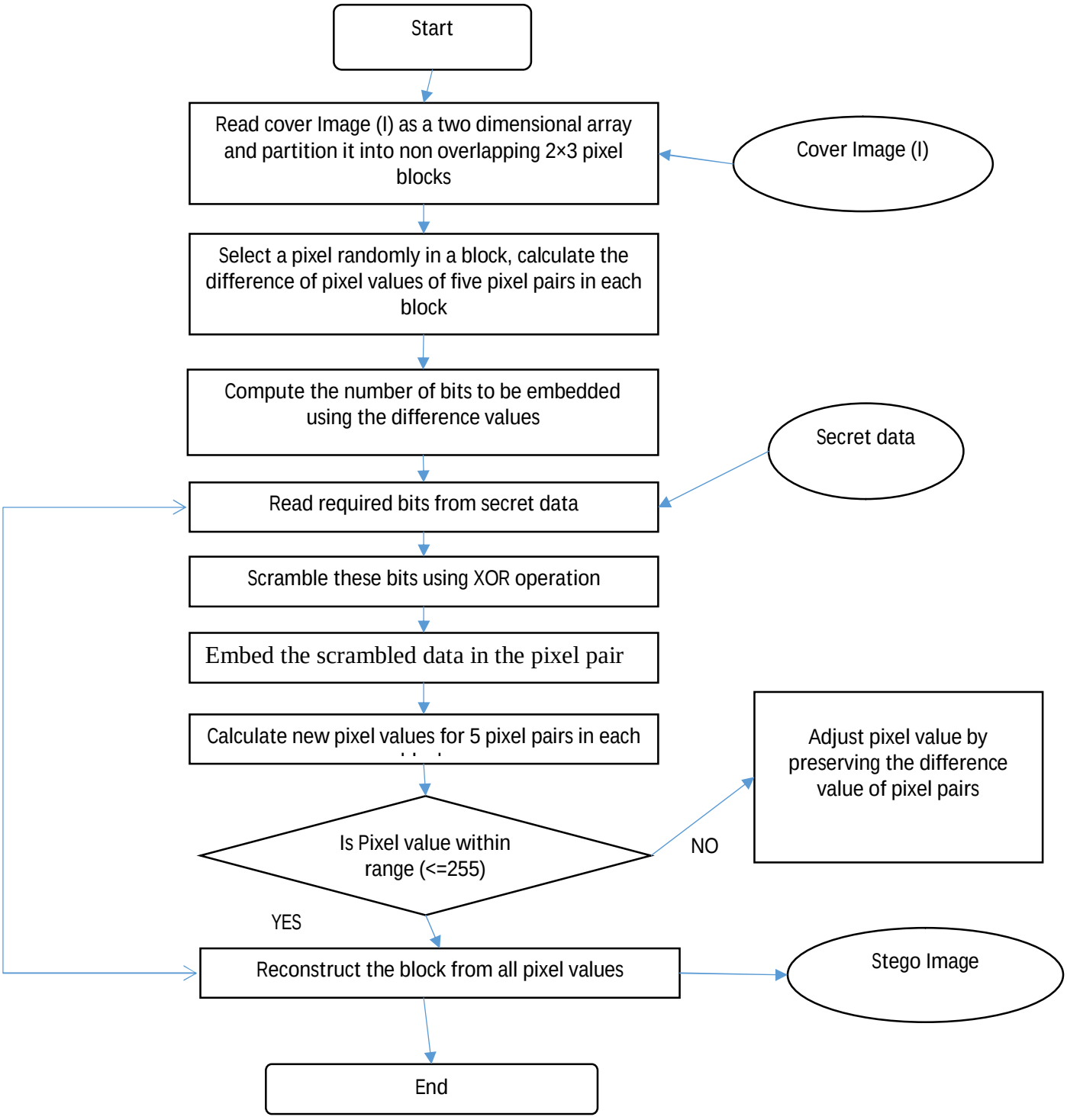

Fig.2. Proposed embedding process

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

The extraction process is reverse of embedding process with the stego image as inputs and the resultant is the secret data.

V. CONCLUSION

PVD approach of image steganography uses the difference between two pixel values to hide the secret information. The hiding capacity (payload) of the cover image is dependent on the number of pixel pairs that can be formed for the given cover image. It is seen that the hiding capacity increases as the block size increase since the number of pairs increases as the block size increases. For a block of 2 x 1 pixels, only 1 pair can be formed whereas for a block of 2 x 2 pixels, 3 pairs can be formed and for a block of 2 x 3 pixels, 5 pairs can be formed. But as the hiding capacity increase, the quality of the stego images may degrade. The PVD stenography methods reviewed in this paper provides acceptable quality of stego images. It is very difficult to develop a steganography method that can resist all the steganalysis attack. Hence there is always a need to develop new steganography methods. It is necessary to increase the security levels for the secret data embedded in the image so that even in case of failure of the steganography method, the intruder should find it difficult to retrieve the hidden secret data. This paper discusses one of the approach to enhance the security of stenographic algorithm by random pixel selection and scrambling the secret data before embedding.

REFERENCES

1. Da-Chun Wu , Wen-Hsiang Tsai , “A steganographic method for images by pixel-value differencing”, Pattern Recognition Letters, vol. 24, pp. 1613–1626 , 2003.
2. 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.
3. Ki-Jong Kim, Ki-Hyun Jung, Kee-Young Yoo, “A High Capacity Data Hiding Method using PVD and LSB”, IEEE International conference on Computer Science and Software Engineering, Wuhan, Hubei, China, pp. 876-879, December 12-14, 2008.
4. M. Khodaei, K. Faez, “New adaptive steganographic method using least significant bit substitution and pixel-value differencing”, IET Image Processing, vol. 6, no. 6, pp. 677–686, 2012.
5. AwadKh. Al-Asmari And Owayed A. Al-Ghamdi, “High Capacity Data Hiding Using Semi-Hexagonal Pixels Value Difference”, TInternational Conference on High Performance Computing, Networking and Communication Systems (HPCNCS-09) ,TOrlando, Florida, USA, pp. 14-17, July 13-16, 2009.
6. Xin Liao, Qiao-yan Wen, Jie Zhang, “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, 2011.
7. M.B. Ould MEDENI, El Mamoun SOUIDI, “A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution”, IEEE International conference on Multimedia Computing and Systems (ICMCS), Ouarzazate, Morocco, pp. 1-4, April 7-9, 2011.
8. M.B. Ould MEDENI, El Mamoun SOUIDI, “A Generalization of the PVD Steganographic Method”, International Journal of Computer Science and Information Security(IJCSIS), vol. 8, no. 8, p.p.156-159, November 2010.
9. Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang, “A high quality steganographic method with pixel-value differencing and modulus function”, The Journal of Systems and Software, vol. 81, no. 1, pp. 150-158, January 2008.
10. Feng Pan, Jun Li, Xiaoyuan Yang, “Image Steganography Method Based on PVD and Modulus Function”, IEEE International conference on Electronics, Communications and Controls (ICECC), Ningbo, China, pp.282-284, September 9-11, 2011.
11. Jeong-Chun Joo, Hae-Yeoun Lee,and Heung-Kyu Lee, “Improved Steganographic Method Preserving Pixel-Value Differencing Histogram with Modulus Function”, EURASIP Journal on Advances in Signal Processing, vol. 2010, pp. 1-13, 2010.
12. Manjunath Gadiparthi, Keshav Sagar, DivyaSahukari, Rakesh Chowdary, “A High Capacity Steganographic Technique based on LSB and PVD Modulus Methods”, International Journal of Computer Applications, vol. 22, no.5, pp.8-11, 2011.
13. Min-Yen Chiu, Yu-Sheng Liao, Jiun-Jian Liaw, “Improved Steganographic Technique for the Image Quality of PVD”, International Conference on Advanced Information Technologies (AIT), Taichung County, Taiwan, April 23-24, 2010.
14. El-Sayed M. El-Alfy ,Azzat A. Al-Sadi, “Improved Pixel Value Differencing Steganography Using Logistic Chaotic Maps”, IEEE International Conference on Innovations in Information Technology (IIT), Abu Dhabi, pp.129-133, 2012.
15. Ko-Chin Chang, Ping S. Huang, Te-Ming Tu, and Chien-Ping Chang, “Adaptive Image Steganographic Scheme Based on Tri-way Pixel-Value Differencing”, IEEE International conference on Systems, Man and Cybernetics (ISIC), Montreal, pp. 1165-1168, October 7-10, 2007.
16. Ko-Chin Chang, Chien-Ping Chang, Ping S. Huang, and Te-Ming Tu , “A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing”, Journal of Multimedia, vol. 3, no. 2, pp. 37-44, 2008.
17. Ko-Chin Chang, Ping S. Huang, T-M Tu, and Chien-Ping Chang, “Image Steganographic Scheme Using Tri-way Pixel-Value Differencing and Adaptive Rules”, IEEE international conference on Intelligent Information Hiding and Multimedia Signal Processing, Kaohsiung, Taiwan, pp. 449-452, December 26-28, 2007.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

18. P. Mohan Kumarand K. L. Shanmuganathan, “Developing a Secure Image Steganographic System Using TPVD Adaptive LSB Matching Revisited Algorithm for Maximizing the Embedding Rate”, Journal of Telecommunications and Information Technology, vol. 2, pp. 61-66, 2011.
19. Gulve A. K. and Joshi M.S., "A High Capacity Secured Image Steganography Method with Five Pixel Pair Differencing and LSB Substitution", International Journal of Image, Graphics and Signal Processing (IJIGSP), vol.7, no.5, pp. 66-74, 2015.
20. Gulve A. K. and Joshi M.S., “An Image Steganography Algorithm with Five Pixel Pair Differencing and Grey Code”, International Journal of Image, Graphics and Signal Processing (IJIGSP), vol. 6 no. 3, pp. 12-20, 2014