Pixel Value Differencing Steganography Techniques: Analysis and Open Challenge

Mehdi Hussain[1, 2], Ainuddin Wahid Abdul Wahab[1], Nor Badrul Anuar[1], Rosli Salleh[1] and Rafidah Md Noor[1]
[1]*Faculty of Computer Science and Information Technology, University of Malaya, Malaysia*
[2]*School of Electrical Engineering and Computer Science, NUST, Pakistan*

***Abstract*—Steganography is the science of secret data communication using carrier medium, such as images, videos, text, and networks. Image steganography is majorly divided into spatial and frequency domains. Pixel value differencing (PVD) considered as good steganographic algorithm due to its high payload and good visual perception in spatial domain. The purpose of this paper is two folded. First is the critical analysis of current PVD methods using evaluating parameters (payload, visual quality and resistance of attacks) and secondly it highlights the current promising directions on PVD steganographic research.**

INTRODUCTION

In recent years, information hiding has become an essential research area due to the boost of digital communication over Internet. The spatial domain steganography is favorite due to its capability of providing spaces for high payload of secret data[1]. There are several methods of spatial domain steganography available such as least significant bit (LSB), PVD, Histogram shifting, and Pixel Mapping[1]. The PVD scheme uses the difference value between two consecutive pixels to determine how many secret bits can be embedded. PVD performance has shown to provide a high payload, good visual quality and resistance to steganalysis attacks. Human vision has a larger tolerance in edge areas than in smooth areas, that's turn out to be the advantage of PVD philosophy. In PVD, more edges mean more secret data can be embedded. PVD can be classified into basic PVD, PVD with LSB, Multi Directions (MD), Multi-Pixel Differencing (MPD), Side matching, and Modulus Function (MF). This paper presents a current literature review of PVD methods based on general evaluating parameters. It further indicates the direction of PVD steganographic research with respect to the latest techniques.

TABLE I OBSERVATIONS OF PVD METHODS

Ref	High Payload	Visual Quality	Resist Analysis	Type + Observations
[2]	Y	Y	Y	PVD: Basic technique of PVD method
[3]	Y	Y	N	PVD with variable k-bit LSB readjustment [2]
[4]	Y	Y	N	Exploit edge area, PVD k-LSB, Improved [3]
[5]	Y	N	Y	MD-PVD, processed pixels simultaneously,[2]
[6]	Y	Y	Y	LSB, OPAP & MPD, block size 3 pixels, k-bit LSB on center pixel, PVD at 1st and 3rd pixels, capacity & PSNR increased against [3,4]
[7]	Y	Y	N	MPD & LSB, Improve the pixel traversal of [6]
[8]	N	Y	Y	PVD- EMD, Exploiting Modification Direction
[9]	Y	Y	N	MD-MPD, improve [2] Tri-way PVD, Horizontal, Vertical, Diagonal.
[10]	Y	N	Y	PPM Minimize falling off PVD boundaries
[11]	N	N	Y	Capacity improved only in side match PVD, Utilized 4 neighbors pixels with PVD, Good tolerance of Steganalysis attack
[12]	Y	N	Y	MD-MPD :Compress secret image by JPG2000, embedded by Tri-way PVD [9], High computation complexity
[13]	N	N	Y	Security improved by random embedding PVD
[14]	Y	Y	N	Side Match PVD, correlation between neighboring pixels to estimate the smoothness of pixels; Suffers with FIEP problem
[15]	Y	N	N	MPD, Extend the PVD method, use 4 and 8 pixels differencing enhancing [2]
[16]	Y	Y	N	MF MPD, Modulus Function Multi Pixel Differencing up to 8 pixels enhanced capacity
[17]	Y	Y	Y	MF PVD, Adjust the pixels remainder with PVD, Distortion is minimized.
[18]	Y	Y	N	MD PVD : Multi Direction 4, 8 and diagonal directions in PVD
[19]	N	Y	Y	MF PVD modulus function, novel turnover policy used to cater the boundary conditions
[20]	Y	Y	N	PVD LSB Selective Strategy, Improved the smooth area differences pixels with new adjustment of lower level strategy, extending [3]

ANALYSIS AND FUTURE DIRECTION

Generally, investigations on PVD were focused on incrementing the embedding capacity using LSB or a readjusted process, but limited studies were focused on the PVD range table design for same purpose. Besides, it is intuitive to design it using the width of the power of two. Table 1 describes the comparisons of different PVD methods based on evaluating parameters (payload, visual quality and attack resistance levels). In more details, the capacity comparisons graph is shown in Fig. 1, where abscissa and ordinate axes are the reference number of techniques and average payload of secret data over gray scale 512x512 images dataset respectively. It can be seen that methods in [4, 6 and 20] provides a high payload (above 90 KB) with a reasonable (more than 35) PSNR and their tolerance steganalysis attack levels as depicted in Fig. 2.

Khodaei *et. al* [6] divides pixels in 3 non-overlapping blocks. Apply k-bit LSB with OPAP on 2nd pixel and PVD on 1st and 3rd pixels respectively. Due to modification of 2nd pixel by LSB, PVD has to works on drifted pixels for differencing with neighbor pixels which reduce the PSNR. In addition there is also an issue related to boundary overflow/underflow conditions. Considering possibility of increasing the PSNR, exploit the R1 (range level) of both type1 and type2 range tables of PVD as depicted in Fig-3. If difference value between 1st with 2nd or 3rd with 2nd pixels occurs in R1 of range table1/table2, then direct 3-bit LSB mode could be

978-1-4799-8745-0/15/$31.00©2015 IEEE

applied with secret data bits instead of PVD. Because PVD in R1 range accommodate the difference value with equivalent of 3 bit decimal secret data of $1^{st}/3^{rd}$ pixel with 2^{nd} pixel. In above process only $1^{st}/3^{rd}$ pixel value is shifted to accommodate the secret data. It causes distortion due to $1^{st}/3^{rd}$ pixel is drifting on the basis of 2^{nd} (already LSB altered) pixel. In contrast, LSB hide the secret bits in actual pixels instead of already drifted value. Generally PVD always modify the both pixels to accommodate secret data equally and it's more useful on edge pixels not for smooth area pixels (small ranges differences).

Similarly in [20], Yang *et. al.* introduced a lower level strategy, which enhances the capacity and PSNR against Wu *et. al.* [3]. This method targeted to refine embedding method in smooth area pixels. For edge area simple PVD is applied but there is no analysis of histogram attack. Modulus function with turnover policy can overcome this histogram analysis issue as in Joo *et. al.*[19]. For higher level area (heavy texture area), the use of MPD instead of PVD would increase hidden capacity, because MPD involves multiple pixels to find the edge areas.

Yang *et. al* [20] also investigated that generally 90% of pixels are belongs to smooth areas, where PVD performance strength based only on edge areas. So, combination of PVD with LSB is required for enhancing the capacity. As noticed and proved that all above good methods [4, 6, and 20] utilized LSB with PVD for good capacity and PSNR.

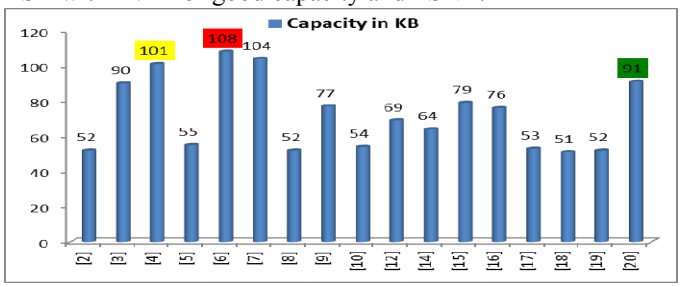

Fig. 1. Capacity comparisons graph

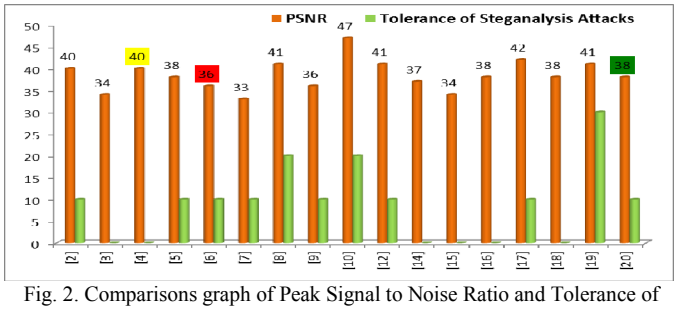

Fig. 2. Comparisons graph of Peak Signal to Noise Ratio and Tolerance of Steganalysis Attacks Level, 0: No, 10: RS / Histogram, 20: RS + Histogram 30: RS + Histogram + LSB Matching

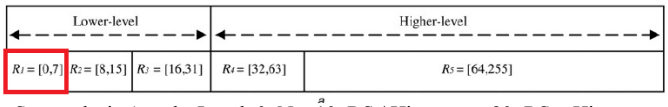

Fig. 3. PVD range table

CONCLUSION

In this paper, we reviewed and discussed various PVD steganographic methods for hiding secret data in digital images. We also compared their performance in terms of the embedding capacity, visual quality and tolerance of steganalysis attacks. PVD with LSB methods proved good results in terms of capacity and PSNR. However, further study on different combinations of PVD (MD, MPD) with adaptive LSB would be the best area for research in improving hiding capacity and PSNR. In addition a detailed comparison of the methods against different attacks (i.e. steganalysis) is another potential area for future work.

REFERENCE

1. Hussain, M. and M. Hussain, *A Survey of Image Steganography Techniques.* International Journal of Advanced Science and Technology, 2013. **54**: p. 12.
2. Wu, D.-C. and W.-H. Tsai, *A steganographic method for images by pixel-value differencing.* Pattern Recognition Letters, 2003. **24**(9): p. 1613-1626.
3. Wu, H.-C., et al., *Image steganographic scheme based on pixel-value differencing and LSB replacement methods.* IEE Proceedings-Vision, Image and Signal Processing, 2005. **152**(5): p. 611-615.
4. Yang, C.-H., et al., *Adaptive data hiding in edge areas of images with spatial LSB domain systems.* Information Forensics and Security, IEEE Transactions on, 2008. **3**(3): p. 488-497.
5. Yang, C.-H., et al., *A data hiding scheme using the varieties of pixel-value differencing in multimedia images.* Journal of Systems and Software, 2011. **84**(4): p. 669-678.
6. Khodaei, M. and K. Faez, *New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing.* IET Image processing, 2012. **6**(6): p. 677-686.
7. Tsai, Y.-Y., J.-T. Chen, and C.-S. Chan, *Exploring LSB Substitution and Pixel-value Differencing for Block-based Adaptive Data Hiding.* 2014.
8. Shen, S.-Y. and L.-H. Huang, *A data hiding scheme using pixel value differencing and improving exploiting modification directions.* Computers & Security, 2015. **48**: p. 131-141.
9. Chang, K.-C., et al., *A novel image steganographic method using tri-way pixel-value differencing.* Journal of multimedia, 2008. **3**(2): p. 37-44.
10. Chen, J., *A PVD-based data hiding method with histogram preserving using pixel pair matching.* Signal Processing: Image Communication, 2014. **29**(3): p. 375-384.
11. Swain, G., *Steganography in Digital Images Using Maximum Difference of Neighboring Pixel Values.* International Journal of Security & Its Applications, 2013. **7**(6).
12. Lee, Y.-P., et al., *High-payload image hiding with quality recovery using tri-way pixel-value differencing.* Information Sciences, 2012. **191**: p. 214-225.
13. Mandal, J. and D. Das, *Colour image steganography based on pixel value differencing in spatial domain.* International journal of information sciences and techniques, 2012. **2**(4).
14. Chang, C.-C. and H.-W. Tseng, *A steganographic method for digital images using side match.* Pattern Recognition Letters, 2004. **25**(12): p. 1431-1437.
15. Patil, D.D. and S. Bansode, *Secured Information Hiding Using Variable Pixel Block Size of PVD Steganographic Techniques.* International Journal on Advanced Computer Theory and Engineering, 2013. **2**(3):p. 4.
16. Liao, X., et al., *A novel steganographic method with four-pixel differencing and modulus function.* Fundamenta Informaticae, 2012. **118**(3): p. 281-289.
17. Wang, C.-M., et al., *A high quality steganographic method with pixel-value differencing and modulus function.* Journal of Systems and Software, 2008. **81**(1): p. 150-158.
18. Hossain, M., S. Al Haque, and F. Sharmin. *Variable rate steganography in gray scale digital images using neighborhood pixel information*. in *Computers and Information Technology, 2009. ICCIT'09. 12th International Conference on*. 2009. IEEE.
19. Joo, J.-C., H.-Y. Lee, and H.-K. Lee, *Improved steganographic method preserving pixel-value differencing histogram with modulus function.* EURASIP Journal on Advances in Signal Processing, 2010. **2010**: p. 26.
20. Yang, C.-H., et al., *Varied PVD+ LSB evading detection programs to spatial domain in data embedding systems.* Journal of Systems and Software, 2010. **83**(10): p. 1635-1643.