Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 4; April-June, 2016, pp. 246-249

http://www.krishisanskriti.org/Publication.html

Survey and Analysis of Edge Based Steganographic Techniques

Neha Singla[1] and Khushil Saini[2]

[1,2]Netaji Subhas Institute of Technology, Dwarka
E-mail: [1]nehasingla66@gmail.com, [2]khushil@rediffmail.com

Abstract—*The main goal of steganography is undetectablity. Towards this goal edge based adaptive techniques of steganography are used, due to the fact that edge area is less sensitive to human visual system. In this paper we have presented the prominent techniques for finding edges and their advantages and disadvantages. Exhaustive literature survey has been done to find which technique is better in terms of embedding rate and Steganalysis, what are the drawbacks of these techniques. This paper concludes with some recommendations and advocates for constructing an edge adaptive technique and presenting results.*

1. INTRODUCTION

As a consequence of the fact, transmitting data has been fast and easy these days due to the development of the Internet. Security is the major matter for these communications and steganography is the art of hiding and transmitting secret messages through carriers without being exposed i.e. 'covered writing' is done , in which text, audio, video or any digital media can be cover in which secret message can be hidden. In the field of information hiding there are two more techniques: cryptography and watermarking. The difference between these three is shown in Table 1.1 [1]. Steganography hierarchy is shown in Fig. 1.1, our main concern will be steganography in digital images. Images are preferred because of high redundancy and more accurate display.

Audio steganography – In this audio signal is modified to carry the secret information. Although audio steganography has nearly equal potential as in hiding data in images but due to larger size this is not preferred.

Video Steganography – In this the carrier medium of secret message is video. It overcomes the payload capacity limitation of image and moreover it is more secure as it is difficult for attackers to find message in a large number of frames.

Text Steganography – In this message is hidden behind the text file. Breaking the stegaonographic system is impractical as no one can even guess that message is hidden behind a webpage.

Image Steganography – In this image is used as carrier medium. Images are preferred due to data redundancy but they have restricted payload capacity as compared to video.

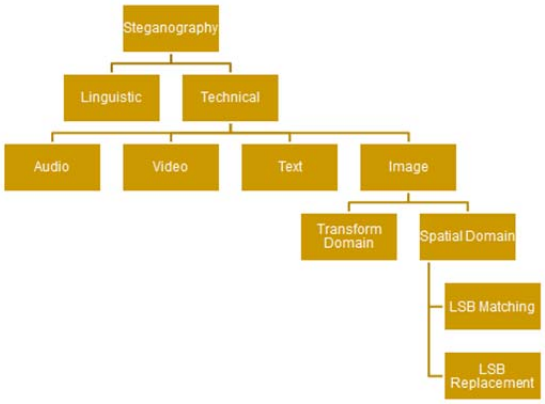

Fig. 1.1: Hierarchy of steganography

Table 1.1 Comparison of various information hiding schemes

Criterion/ method	Steganography	Watermarking	Encryption
Carrier	Any digital media	Mostly image/audio files	Usually text based, with some extensions to image files
Secret data	Payload	Watermark	Plain text
Key	Optional		Necessary
Input files	At least two unless in self-embedding		One
Detection	Blind	Usually informative (i.e., original cover or watermark is needed for recovery)	Blind
Authentication	Full retrieval of data	Usually achieved by cross correlation	Full retrieval of data
Objective	Secrete communication	Copyright preserving	Data protection
Result	Stego-file	Watermarked-file	Cipher-text
Concern	Delectability/ capacity	Robustness	Robustness
Type of attacks	Steganalysis	Image processing	Cryptanalysis
Visibility	Never	Sometimes	Always
Fails when	It is detected	It is removed/replaced	De-ciphered
Relation to cover	Not necessarily related to the cover. The message is more important than the cover	Usually becomes an attribute of the cover image. The cover is more important than the message	N/A
Flexibility	Free to choose any suitable cover	Cover choice is restricted	N/A
History	Very ancient except its digital version	Modern era	Modern era

Image steganography can be classified in two categories: Spatial domain and Transform domain. In Spatial domain, the message is directly embedded in the pixels of the image without converting the image. Spatial domain consists of LSB replacement and LSB matching algorithms. In transform domain, embedding is done by modifying the LSB of non-zero DCT coefficients of a cover image. In place of DCT discrete wavelet transform (DWT), Fourier transform or any other

representation of images could be used. Main features of both domains are shown in Table 1.2.

Edges are the region where difference in value of adjacent pixels is large. If we modify the edge pixels then it is difficult for human visual system (HVS) to detect the change. In this paper we have presented various edge based adaptive techniques and their pros and cons.

2. EDGE FINDING TECHNIQUES

Most of the research in the field of image steganography has been done using edge adaptive techniques. Edge detection can be performed in many ways but mainly they are divided into two categories: Gradient and Laplacian. In Gradient method, edge detection is done by looking the maximum and minimum in the first derivative of the image. The Laplacian method searches for the zero crossings in the second derivative of the image to find edges. Robert, sobel and prewitt methods are based on gradient method. Gradient approximation is used in sobel edge detection but it is sensitive to noise and data extraction is sometimes incorrect.

An improved version [2] of sobel edge detection was introduced in which the original limitation of noise in image was tried to overcome. In this the sobel edge detection is combined with soft-threshold wavelet de-noising to do edge detection, which leads to good quality edge detection in case of noise.

Table 1.2: Main features of spatial and transform domain.

Method	Description
Spatial domain	• Large payload but often offset the statistical properties of the image. • Not robust against lossy compression and Image filters. • Not robust against rotation, cropping and translation. • Not robust against noise. • Many work only on the BMP format.
DCT based domain	• Less prone to attacks than the former methods at the expense of capacity. • Breach of second order statistics. • Breach of DCT coefficient distribution. • Work only on the JPEG format. • Double compression of the file. • Not robust against rotation, cropping and translation. • Not robust against noise. • Modification of quantization table.

Prewitt operator [3] is similar to sobel operator as it uses same equation as sobel. Difference is in value of constant only. The prewitt operator is limited in 8 orientations and experience shows that the result obtained are not much accurate. Roberts cross operator computes 2-D spatial gradient measurement on an image and which is very quick and simple. The high frequency region generally corresponds to edges. Canny edge detection [4] is an approach based on Gaussian filter. The Smoothing concept is used in Gaussian operation, therefore finding errors is effective with the help of probability. The second benefit is improved signal with respect to the noise ratio and this is done by Nonmaxima suppression method. The next advantage is improved detection of edges in case of noise state. The major drawback is Time consumption because of thorny calculation. Pixel value differencing is another way of finding edges by calculating the difference between the intensity of edge pixels. More is the difference more the number of message bits can be introduced. Table 1.3 shows the advantages and disadvantages of basic edge operators. The disadvantages of these operators are overcome by specific techniques.

3. STEGANOGRAPHIC TECHNIQUE

PVD (Pixel Value Differencing) method was introduced by [5], which exploit the fact that Human visual system (HVS) is less sensitive to edge area as compared to smooth area. The edge pixels have intensity either higher or lower than the neighboring pixels. [6] Combined LSB substitution method with pixel value. The combination leads to enhanced quality image as compared to PVD alone. In their approach, secret message is hidden in edge area using PVD while embedding in smooth area is done using LSB substitution. Data hiding done using PVD is not detectable by human visual system but it has a loophole. The unusual pattern in the histogram of pixel differences uncovers the existence of embedded data. To enhance security, [7] proposed a technique that shuns the occurrence of the unusual steps in the pixel difference histogram while preserving the advantage of low visual distortion of the PVD.

Table 1.3: Comparison of edge operators

Edge Operator	Advantage	Disadvantage
PVD	• Simplicity. • High Embedding Capacity.	• Increase the possibility of detecting the message by tracing pixels in every block.
Sobel Method	• Simplicity.	• Does not guarantee a high embedding rate. • Sensitivity to noise. • Data Extraction is sometimes incorrect.
LOG	• It is easier to find the correct position edges.	• Reduces accuracy at corners and curves.
Prewitt	• Results are more accurate than Sobel.	• Sensitivity to noise. • Inaccuracy as gradient magnitude of edge decreases.
Canny	• Better edge detection in presence of noise. • Improving SNR. • Randomization.	• Time Consuming.

[8] Proposed a steganography technique that increases the capacity of the hidden message and stego image is imperceptible to human visual system. The largest pixel intensity difference between the three pixels close to the target pixel is used to determine the amount of embedding data in the target pixel. If the difference is more than more number of bits can be embedded. This had numerous problems like boundary problem for edge pixels, stronger area might left while weaker areas are used, Poor in resistance to steganalysis.

The main goals of steganography are undetectablity and embedding capacity, to accomplish these goals tri-way pixel-value differencing (TPVD) is introduced in [9]. In tri-way pixel- value differencing, three different directions are considered as compared to single direction in original PVD. This helps to improve the embedding capacity, the distortion is optimal and moreover security of message is improved using this method.

Octa (STAR) PVD method introduced by [10] eliminates the histogram attack as in PVD and TPVD. In this 3*3 pixels are considered as compared to 2*2 pixels in TPVD.

Further improvement in this area is done by [11], This uses four-pixel differencing along with least significant bit (LSB) substitution. In this blocks of four pixels are formed and average difference in block is used to classify block as smooth area or edge area. K- Bit LSB substitution method is used to hide the data. In this technique, compromise with security is done to achieve quality.

In [12] base decomposition scheme is used along with PVD. This method offers the advantage of high embedding rate along with maintaining the consistency of image characteristics. The base decomposition scheme is introduced which defines a base pair for each degree in order to construct a two-base notational system. This scheme generates much smaller pixel variations and expected mean square error while giving a higher PSNR but has overflow and underflow problem. This paper [13] uses multi-base notational system with diamond encoding to overcome the problem of overflow and underflow and to maintain divisional consistency. Pixel pairs having large variations are inserted with digits in larger base than those pixel pairs with smaller differences. According to author this technique gives better image quality in techniques using PVD technique. This technique is little bit complicated to use.

[14] Introduced a technique in which a coding method is combined with PVD. To develop efficient technique to embed message in image a coding method is required to minimize the distortion caused. So, different coding techniques can help to produce efficient technique with reduced distortion in image. In this paper coding method used is XOR coding. It gives better result than PVD and TPVD.

This [15] technique is the recent approach using PVD. It enhances the edge adaptive by integrating Tree based parity check. The incorporation of TBPC minimizes the modifications of the cover image, as it changes no more than two bits out of seven pixel bits when embedding four secret bits. TBPC reduces the distortion to be caused but the drawback of this is high computational cost.

4. CONCLUSION

PVD methods are popular methods in the field of edge adaptive techniques. It follows the principle that human visual system is less sensitive to edge area as compared to smooth area. A lot of work has been done using PVD and in which embedding rate is acceptable, but the work lacks security. The majorly required assessment criteria “for a good steganographic technique are Robustness, Undetectablity and embedding capacity. But, there is no technique so far, which has addressed these criteria simultaneously.

So, there is a need of technique which would provide good embedding rate, high PSNR value and will be robust to steganalysis.

Moreover, there are some principles for constructing an edge adaptive technique: edges obtained while encoding and decoding should be same, stronger edges should get favor over weak edges. In PVD even if one pixel in image changes then the edges in stego image may not match with the edges in cover image. Hence, leading to incorrect results. The techniques we studied till now, none of them guarantee same edges in cover image and stego image.

The results given in all techniques depend on the message taken into consideration, we can’t compare with other techniques until we know the message others had taken into consideration. So, there should be some standard messages for which result should be evaluated.

REFERENCES

[1] Cheddad, Abbas, et al., "Digital image steganography: Survey and analysis of current methods", *Signal processing* 90.3, 2010, pp, 727-752.

[2] Gao, Wenshuo, et al., "An improved Sobel edge detection ", *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*. Vol. 5., 2010.

[3] Seif, A.,et.al., “A hardware architecture of Prewitt edge detection”, *Sustainable Utilization and Development in Engineering and Technology (STUDENT), 2010 IEEE Conference, Malaysia*, 20-21 Nov. 2010, pp. 99 – 101.

[4] Canny, J., “A Computational Approach to Edge Detection”, *IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 8,* November 1986, pp. 679-714.

[5] Wu, Da-Chun, and Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing", *Pattern Recognition Letters* 24.9 ,2003, pp, 1613-1626.

[6] Wu, H.C., Wu, N.I., Tsai, C.-S., Hwang, M.S, “Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods”, *IEEE Proceedings-Vision, Image and Signal Processing, Vol. 152, No. 5,*2005, pp. 611-615.

[7] Zhang, Xinpeng, and Shuozhong Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and

modification for enhanced security" ,*Pattern Recognition Letters* 25.3 ,2004, 331-339.
[8] Zhang, Hanling, Guangzhi Geng, and Caiqiong Xiong, "Image steganography using pixel-value differencing " ,*Electronic Commerce and Security, 2009. ISECS'09. Second International Symposium on*. Vol. 2. IEEE, 2009.
[9] Chang, Ko-Chin, et al., "A novel image steganographic method using tri-way pixel-value differencing", *Journal of multimedia* 3.2,2008, pp. 37-44.
[10] Thanekar, Sachin A., and Soudamini S. Pawar, "OCTA (STAR) PVD: A different approach of image steganopgraphy" , *Computational Intelligence and Computing Research (ICCIC)*, IEEE, 2013.
[11] Liao, Xin, Qiao-yan Wen, and Jie Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution" , *Journal of Visual Communication and Image Representation* 22.1,2011, pp. 1-8.
[12] Wu, Nan-I., Kuo-Chen Wu, and Chung-Ming Wang, "Exploring pixel-value differencing and base decomposition for low distortion data embedding" , *Applied Soft Computing* 12.2 ,2012, pp. 942-960.
[13] Hong, Wien, Tung-Shou Chen, and Chih-Wei Luo, "Data embedding using pixel value differencing and diamond encoding with multiple-base notational system" , *Journal of Systems and Software* 85.5 ,2012, pp. 1166-1175.
[14] Al-Dmour, Hayat, and Ahmed Al-Ani, "A steganography embedding method based on edge identification and XOR coding" ,*Expert Systems with Applications* 46, 2016, pp. 293-306.
[15] Al-Dmour, Hayat, Noman Ali, and Ahmed Al-Ani, "An efficient hybrid steganography method based on edge adaptive and tree based parity check" , *MultiMedia Modeling Springer International Publishing*, 2015.