IJCTA, 9(10), 2016, pp. 4493-4500
© International Science Press

Comparative Analysis of Image Steganography Methods

***Mohanjeet Kaur **Mamta Juneja**

Abstract : Steganography is the technique, which can be used for the purpose of hiding the data into similar form or other form of data to create the covert channel among the internet or intranet links to protect the data from the various kinds of masquerading or attacks(reviewer 1 ,comment 2 and 3). Image steganography is one of the leading steagnography classes which deal with data hiding techniques for hiding the data in the images. Text, image or audio data can be embedded in the images by using the various spatial domain or transform domain methods. In this, we will review different types of LSB and PVD and hybrid edge based image steganography techniques. The techniques are compared on the basis of three parameter robustness, imperceptibility and payload capacity and MSE. The main idea in these techniques is that more capacity of embedding data at the edge areas of the cover image rather than smooth areas of the cover image. An attempt has been made to analyze the key issues of various steganography methods in order to identify their suitability for data hiding.

Keywords : LSB substitution, Edge based image steganography, PSNR, Embedding capacity, Random edge pixel embedding, pixel value difference (PVD).

1. INTRODUCTION

Information hiding will play an important role in today's world. It has captured a lot of attention by researchers due to the advancement in the modern communication technology. In the today's modern world, everyone comes across the digital information. Major concern about this digital information is the security of the information as transferring data over the internet is not safe and it suffers from eavesdropping Initially, Cryptography was used for a reliable and safe transmission. However, the encrypted data which have a meaningless message may actually evoke suspicion from illegal attackers. But now, steganography [2-4] is invented to overcome the drawback by embedding confidential data into a cover media without attracting any special attention from hackers. So, steganography is a technique which is used to provide more security to the confidential information.

Steganography is derived from two Greek word stegano and graphy which means "covered writing". Steganography is a part of information security which is used to hide the data or any object from the intruder [1].

Following key terms are used in steganography :

1. **Cover image :** Cover image is used as a carrier for embedding secret information or message to be sent to the receiving party.
2. **Message :** Message is Secret data that the sender wishes to remain confidential. It can be plain text, ciphertext, audio file or video file.
3. **Stego key :** It is a key to integrate the information inside cover medium and extract same information from the stego medium.

* Department of Computer Science & Engineering UIET, Panjab University Chandigarh, India kaur.mohanjeet@gmail.com

** Department of Computer Science & Engineering UIET, Panjab University Chandigarh, India mamtajuneja@pu.ac.in

4. **Stego image :** It is the cover image with a hidden secret data inside it called the Stego image. It is employed at the receiver end to pull out the message hidden in it.

Image steganography uses images as the cover media to hide the secret data. As a lot of redundant information is contained in images so images are taken to be cover media. The redundant bits of an image are those bits that cannot be detected even when they are altered. Image files full fill this requirement so they are very commonly used as a cover media for steganography. The main idea of image steganography is to keep the data safe form the hackers. Image steganography model is shown in the following figure1.

The figure includes the following components:

Message (M) : Important information that is to be hidden in the cover image.

Cover Image (I) : Media used for embedding.

Stego Key (K): Key used for encrypting the message M.

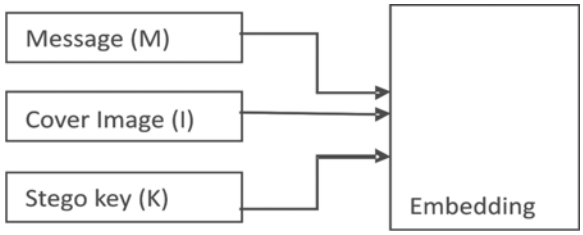

Fig. 1. Steganography Model.

There are basic three requirements used to evaluate the performance of the steganography (reviewer 2 and comment 3):

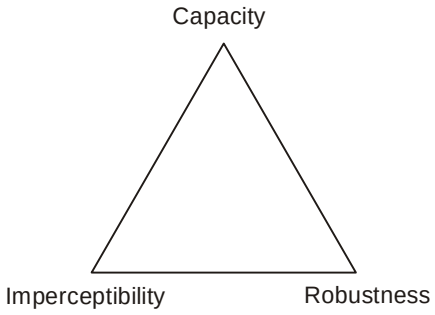

Fig. 2. Basic requirement of image steganography methods.

1. **Payload capacity :** It is defined as the maximum amount of data that is embedded into the image. Capacity can be measured in terms of bpp which means what number of bits of a pixel of cover image has been utilized by the secret information.
2. **Robustness :** It is the message's ability to persist even after performing the operation like compression, rotation, cropping and filtering etc.
3. **Imperceptibility :** It is defined as the quality of the stego-image. Imperceptibility is also known as invisibility. It means there is no decay in the quality of image before and after embedding the secret information.

(Reviewer 1 and comment 2)Performance measures are used for evaluating the efficiency and time complexity of any steganography system. To evaluate the performance of the steganography using three parameters [19]:

1. PSNR 2. MSE 3. Bpp

PSNR (Peak Signal to Noise Ratio) : It is used to define the quality of image and is measure in decibels (dB). It measures the distortion that occurs during embedding in the image. It is mathematically defined as:

$$PSNR = 10 \log\left(\frac{C_{max}^2}{NSE}\right) \quad ...(14)$$

Where C_{max} represents the maximum pixel value in the image and is either 1or 255.

MSE (Mean Square Error) : This is represented by comparing error in data at received end with sender data before and after processing. It refers to the mean error between image used as cover and the stego-image formed. It is mathematically defined as:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2 \quad ...(14)$$

Where M and N denotes the image dimensions that are the length and breadth and S_{xy} and C_{xy} are the stego image and cover image respectively.

Bpp (bits per pixel) : Bpp is defining the amount of data is embedded into cover image and illustrate the total number of the bits of a single pixel used on an average for embedding the secret file. It is measured in bpp and the MHC (Maximum Hiding Capacity) in percentage.

2. LITERATURE SURVEY

LSB and PVD based steganography techniques: Da-Chun Wu et.al, in 2003 proposed a technique for embedding secret data into a grayscale value cover image. A cover image was split into non-overlapping blocks. Select the two successive pixels in each block and calculate the difference values. To embed data in the block when gray value falls off of the range of 0 through 255.In this, if value zero than smooth block and 255 than shapely edge block. The range intervals of the selection were based on the characteristics of human visual system (HVS) to grayscale value variations from smoothness to contrast. It provides good quality of stego image, but not provides the security against various types of attacks [17].

To improve the embedding capacity of above technique, H. C. Wu et.al, in 2005 proposed a method to use the combination of LSB and PVD approaches of steganography to improve the embedding capacity and the PSNR. This method used the difference between the two consecutive pixel values to hide the data. It used an LSB substitution technique for hiding the data at the smooth area and PVD to hide the data at the edges of image. The splitting between the smooth area and edge areas of range width table used at the sender and receiver end to increase the security level, which made it difficult to guess the area at which the data hiding was done. In this, two pixels were embedded using LSB if difference falls into smooth area of the range width table and pixel embedded by PVD if difference fall into higher level. This method used to increase imperceptibility and embedding capacity at edge pixel was more as compared to the smooth area of image [4].

Further features of image are used to improve imperceptibility So, Santosh Arjun, N. et.al [5], in 2006 proposed a method of filtering based new adaptive steganography technique uses for embedding the message into the cover image. Adaptive steganography was done by using local and global feature of the cover image (reviewer 2 and comment 3). Data embedding was done in the high frequency area of the image rather than the low frequency area of the image. This approach filters the image into a low frequency spatial image (LFSI) and high frequency spatial image (HFSI) and inverse transform was performed on both after embedding the data into the HFSI component. In this embedding at the HFSI depended on the magnitude of the pixel. Greater the magnitude of the pixel, a larger number of bits was inserted into the pixel. The Magnitude of the HFSI had been always greater than the 128 so the embedding capacity also increase up to 1 Bpp and method was used the multi band filter instead of using the HPF (high pass filter). The approach achieved the more embedding capacity and also the confidentiality and controlled the capacity limit trough the filter cutoff frequency. It was less subjected to the attacks and main disadvantage was, small difference in the cutoff frequency and order of the filter at the sender and the receiver end than message decoding was not matched to the original image [5].

Manglem Singh et.al [9], in 2007 put forward a technique for hiding the encrypted data in the feature of the image rather than embedding the secret data into the smooth area of the cover image. In this approach, first encrypt the message than detect the edges using edge detection technique and LSB embedding algorithm uses for hiding the encrypted message in non-adjacent and random pixel location on edge of the image. The intruder did not have any suspicion that secret message bits were concealed in the cover image. This approach ensures the security and blind LSB detection technique was not estimate the length of the secure message bits accurately [9].

To embed more data at edge areas of the image, Cheng-Hsing Yang et.al [7], in 2008 the proposed steganography technique based on the new adaptive embedding algorithm LSB data hiding in the non continuous area (edge area) of the image with the spatial domain. Embedding the data into the grayscale image without any distortion and PVD was used to distinguish an area between the continuous and non continuous area in the image. Embedding at the edge pixels of the image used k bit LSB substitution by greater value of the k than the continuous area of the image. In this the range width table includes difference value which was divided into the lower, middle and high level. This approach achieved the imperceptibility, high capacity and PSNR .The relative attack performed on the stego image to detect embedding information, but not provide resistance to the attacks [7].

C.-H. Yang and M.-H. Tsai et.al [8], in 2009 proposed a technique to improve histogram based reversible data hiding by using interleaving prediction for grayscale images. In this approach number of predicted error values as much as the number of pixels in the cover image and then all prediction value was transformed into the histogram to improve the PSNR and embedding capacity of the image. The pixel difference between the cover image and stego image was always within the ±1 [8].

To further improve the robustness of steganography system, Weiqi luo et.al [11], in 2010 proposed a technique of edge adaptive image steganography based on LSB matched revisited. This approach selects the embedding area, according to the size of the message which was embedded into cover image and by PVD in two successive pixels in the original image. It was also preserves the statistical and visual attack feature. It was provides the resistance towards the attacks. Visual quality and security of the stego image was also high using this LSB revisited approach as compared to using the typical LSB substitution [11].

Table 1. Given below shows the comparative analysis of above discusses : (reviewer 1 and comment 3)

Table 1. Comparative analysis of above discusses

Authors	*Approach used*	*Pros*	*Cons*
Da-Chun Wu et.al [17]	1. PVD (pixel value differencing)	1. Embedding capacity: 50960 dB2.PSNR: 41.793.Good quality of stego image	1. Not resists towards the various attacks like: statistical attack analysis , chi-square and RS attacks analysis.
H. C. Wu et.al [4]	1. Fusion of LSB and PVD. 2. An LSB substitution technique for hiding the data in the smooth area.3.PVD to hide the data at the edges of image.	1. Embedding capacity: 95755 dB 2. PSNR:36.16 3. Increase imperceptibility 4. Embedding capacity at edge pixel was more as compared to the smooth area of image	1. Range width table send at the receiver end of extraction of original image ,so more prone to stego attacks
Santosh Arjun,N. et.al [5]	1. Adaptive steganography was proposed, that uses both global features (density, frequency, color and contrast) and local image features(pixel value)	1. Less prone to stego attacks 2. Embedding capacity rate:11.11%	1. Less subjected to the attacks2.small difference in the cutoff frequency and order of the filter at the sender and the receiver end than message decoding was not matching to the original image

Authors	*Approach used*	*Pros*	*Cons*
Manglem Singh et.al [9]	1. Blind LSB detection technique 2. Simplified data encryption standard (S-DES) 3. Pseudo randomnumber generator (PRNG)	1. Ensures the securityembedding data in the feature of the image	1. Low payload capacity2. Stego image quality poor
Cheng-Hsing Yang et.al [7]	1. K Bit LSB and PVD technique for embedding	1. If 4-5 bits used for embedding,then payload capacity:1,076,1092.PSNR: 32.423.MSE:7.86	1. It provides no resistance toward the attacks
C.-H. Yang and M.-H. Tsai et.al [8]	1. Interleaving prediction for gray scale image	1. Payload capacity: 99947 2. PSNR: 48.82 dB 3. Improve histogram based reversible data hiding	1. Sometime problem occurs in not correct obtain of prediction
Weiqi Luo et.al [11]	1. LSB matched revisitedPVD and PRNG	1. High PSNR 2. Resistance towards the attacks 3. Embedding rate was 50% with accuracy 83%	1. Lower embedding rate 2. Poor visual quality

Hybrid Edge detection based Steganography techniques : To use more edges of images for embedding, Chen et al. [10], in 2010 suggested a method of high payload steganography, by using hybrid edge detection. In this method LSB substitution technique was combined with canny edge detection and fuzzy logic edge detection. It was not only achieved higher payload capacity, but also improved the stego image quality. Any image or object edge boundary achieved by this hybrid edge detector was more precise than using a single edge detector either fuzzy logic edge detector or canny edge detector. It was implemented for grayscale images, not tested for color images. It was achieved higher payload capacity that was 2.66bpp which was also used to achieve the highest quality of stego image. It was also resisting the stegoanalysis system that was based on the statistical attack analysis [10].

To further improve PSNR, Hussain, M. et.al [13], in 2011 put forward a method of embedding data in the edge boundaries of the cover image with high PSNR.This paper was targeted on low capacity of data embedded with high PSNR and high level of imperceptibility. Data more hidden at the boundaries of image rather than embedding more data at the smooth area of an image with high PSNR and with low computational complexity and also used the stego image as the native image for the object segmentation and feature extraction of objects. Canny edge detection with their default threshold parameter was used to detect the edge boundaries. In this horizontal edge pixel was used for data embedding and difference of horizontal edge pixel with the upper boundary pixel should be larger than the edge difference threshold. It was used for high PSNR but having the disadvantage of low embedding capacity and also used only for horizontal edge detection pixel boundaries [13].

To improve the Chen et.al [10] payload capacity and PSNR, Anastasia Ioannidou et.al [12], in 2012 proposed a method based on high embedding capacity and hybrid edge detection for color image steganography. In this approach edge area and feature of image like density, frequency was used to hide the wide range of data. In this proposed scheme hybrid edge detection was used to find the greater set of edges. It was achieved good peak to signal ratio (PSNR) and high payload capacity. It was exploited for color images. In this paper number of bits which was embedded in each RGB color was increased from 1 to 6 bits , So embedding bits in edge pixel also increase and quality of the stego image remain same but relation between neighbor pixel was does not Used [12].

To improve PSNR and capacity, Mamta Juneja et.al[14], in 2013 suggested a method to improve the PSNR and embedding capacity new adaptive based LSB technique for data hiding. To provide, the more

security, advanced encryption standard (AES) was used to encrypt the message which was embedded in to cover image. Rather than using the feature of smooth area, feature of edge areas like density, frequency, color and contrast was also used because of edge pixel changes were more tolerated than any changes in smooth areas of the image. In this fusion of canny edge detection and advanced Hough transforms used for edge pixel detection. The approach was provided more imperceptibility, high payload capacity and also high robustness. It was more resistance to steganalysis attack like chi-square, histogram and RS attacks. It provided more PSNR and high embedding capacity [14].

Table 2. Given below shows the comparative analysis of above discusses approaches: (reviewer 1 and comment 3)

Authors	*Approach used*	*Pros*	*Cons*
Chen, W.J. et.al [10]	1. LSB substitution technique 2. Fusion of canny edge detection and fuzzy logic edge detection	1. Payload capacity : 0.65 bpp 2. PSNR : 47.1 3. highest quality of stego image 4. resisting toward statistical attack analysis	1. Applied only at grey scale images
Hussain, M. et.al [13]	1. Canny edge detection with their default threshold parameter	1. If Threshold value :16 then PSNR value was 88.23 2. Low computational complexity3.MSE:9.76	1. Low embedding capacity and used only for horizontal edge detection pixel boundaries
Anastasia Ioannidou et. al [12]	1. Hybrid edge detection and utilized 6 bits of RGB color image for embedding	1. PSNR: 46.88 dB 2. Payload capacity: 1.26 (bpp) 3. Quality of the stego image remain same	1. PSNR Slightly reduced as compared to Weiqi luo et. al, 2010
Mamta Juneja et.al [14]	1. Adaptive based LSB technique for embedding at non edge pixel 2. Advanced encryption standard (AES) 3. Fusion of canny edge detection and advanced Hough transforms used for edge pixel detection	1. More resistance to steganalysis attack like chi-square , histogram and RS attacks2.Embedding capacity was 60 % for edge area and 50% for smooth areas3.Utilized 12 bits of RGB color image for embedding	
Hsien-Wen Tseng et. al [15]	1. Canny and fuzzy block based algorithm 2. non-edge pixels based on the least-significant-bit	1. PSNR: 38.18 dB 2. Payload capacity: 2.41(bpp) 3. increase imperceptibility	1. Some distortion at receiver end when extract cover image form stego image 2. Grey scale images only used
Deepali Singla et. al [16]	1. fusion of canny edge detection and fuzzy edge detection 2. 1-4-8 LSB embedding 3. Advanced encryption standard (AES)	1. PSNR: 46.68dB 2. MSE: 12.453. pay load capacity: 10.26bpp	1. more data was embedded in contrast areas rather than at brighter areas of the image

Hsien-Wen Tseng et al.[15], in 2014 image steganography has been done using high embedding capacity block based data hiding with minimum distortion using hybrid edge detection. This method was used canny and fuzzy block based algorithm to embed the more covert data at the edge area pixels rather than embedding at smooth area pixels of the image. It was achieved the high embedding capacity by using fuzzy block based algorithm and achieved the minimum distortion by using edge pixel of each 4*4 block with minimum MSR and select the proper edge and non edges and also increase the imperceptibility [15].

Deepali Singla et al. [16], in 2015 proposed a method for image steganography for color image was done using hybrid edge detection. In this approach, more data were embedded in contrast areas rather than doing embedding at brighter areas of the image. In this hybrid edge detection was a fusion of canny edge detection and fuzzy edge detection to discover the edges and the adaptive LSB substitution was done by using 1-4-8 LSB technique. To provide, the more security to the stego image, advanced encryption standard (AES) was used to encode the message either any text or image which is embedded into cover image.

Table 3. Above existing techniques apply to Lena image (512 × 512) with secret image (128 × 128) for evaluating payload capacity and PSNR Value (Reviewer 1 and comment 1 for image Lena parameter value)

Author Name	*PSNR(dB)*	*Payload Capacity*
Da-Chun Wu et al. ,[17]	41.79	50960
H. C. Wu et. al.,[4]	36.16	95755
Cheng-Hsing Yanget.al[7]	37.93	102119
C.-H. Yang et al.,[8]	48.82	99947
Chen et.al[10]	47.1	0.65 (bpp)
Anastasia Ioannidou et.al[12]	46.88	1.26 (bpp)
Hsien-Wen Tsenget.al[15]	38.18	2.41(bpp)
Deepali Singlaet.al[16]	46.68	10.26(bpp)

3. CONCLUSION

In this review paper, we will review so many steganographic techniques and issues arising during embedding are also identified(reviewer 1 and comment 4). Initially, LSB techniques were used for the steganography, but these techniques are not resists towards the various types of statistical attack analysis, chi-square and RS attack analysis. To increase the payload capacity hybrid edge detection steganography technique used. For embedding many hybrid approaches used for steganography like a combination of LSB technique and PVD (pixel value difference) method and edge detection method. For the better performance of the edge detection, Hybrid edge detection like a fusion of canny edge detection and fuzzy logic edge detection and fusion of Hough transform and canny was used for edge embedding.

Various types of techniques have been used to achieve better PSNR, embedding payload and imperceptibility. More improvement can be done on the basis of new hybrid edge detection technique to target on better achievement of high imperceptibility, robustness and embedding capacity and other new encryption technique is also used to provide more security. To improve the payload capacity, dynamic fuzzifier can be used for the robust image embedding. The dynamic fuzzifier module is responsible for the segmentation, selection and fuzzy weight calculation among the input cover and secret image to improve robustness and imperceptibility (reviewer 1 and comment 2).

REFERENCES

1. Artz, D.: 'Digital steganographic: hiding data within data', IEEE Int. Comput., 2001,5, (3), pp. 75–80
2. Lee, Y.K., Chen, L.H.: 'High capacity image steganography model', Proc. of IEE onVision, Image and Signal Process., vol. 147, no. 3, pp. 288–294, 2000.
3. Benlcouiri, Y., Ismaili, M., Azizi, A., and Benabdellah, M.,"Securing images by secret key steganography," Applied Mathematical Sciences, vol. 6, no. 111, pp. 5513–5523, 2012.
4. H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing andLSB replacement methods," Proceedings of 2005 InstrumentElectric Engineering, Vis. Images Signal Process, vol. 152, no. 5pp. 611–615, 2005.
5. Santosh Arjun, N. and Atul Negi, "A Filtering Based Approach to Adaptive Steganography," 10th Conference,TENCON 2006, IEEE, pp. 1-4, Nov 2006.

6. Cheddad, A., Condell, J., Curran, K., and Mc Kevitt, P., "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.
7. Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Hung-Min Sun , "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems". IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3,pp. 488-497, 2008.
8. C.-H. Yang and M.-H. Tsai, "Improving Histogram-based Reversible Data Hiding by Interleaving Predictions", IET Image Processing, Vol.4. Iss. 4 pp. 223-234,2010.
9. Manglem Singh, Birendra Singh, Shyam Sundar Singh ,"Hiding Encrypted Message in the Features of Images", IJCSNS, VOL. 7, No.4. April, 2007
10. Chen, W.-J., Chang, C.-C., and Le, T., "High payload steganography mechanism using hybrid edge detector," Expert Systems with Applications, vol. 37, no. 4, pp. 3292–3301, 2010.
11. Weiqi luo, member, ieee, fangjun huang, member, ieee et al., ''edge adaptive image steganography based on lsb matching revisited'', ieee transactions on information forensics and security, vol. 5, no. 2, june 2010.
12. Anastasia Ioannidou , Spyros T. Halkidis , George Stephanides b, " A novel technique for image steganography based on a high payload method and edge detection " , Expert Systems with Applications , Vol. 39, pp. 11517–11524, 2012
13. Hussain, M. and Hussain, "Embedding data in edge boundaries with high PSNR", Proceedings of 7th International Conference on Emerging Technologies (ICET 2011), pp.1-6, Sept 2011
14. Mamta Juneja and Parvinder S. Sandhu, "A New Approach for Information Security using an Improved Steganography Technique," J Inf Process Syst, vol. 9, no. 4, 2013.
15. Hsien-Wen Tseng, Hui-Shih Leng , "high-payload block-based data hiding scheme using hybrid edge detector with minimal distortion" , IET Image Process, Vol. 8, Iss. 11, pp. 647–654,2014
16. Deepali Singla and Mamta Juneja, ''Hybrid Edge Detection-Based Image Steganography Technique for Color Images",Intelligent Computing, Communi-cation and Devices, Advances in Intelligent Systems and Computing ,Springer India, 2015.
17. Wu, D.C., and Tsai, W.H.: 'A steganographic method for images by pixel-value differencing', Pattern Recognit. Lett., 2003, 24, (9-10), pp. 1613–1626.
18. Youssef Bassil, "Image Steganography Based on a Parameterized Canny Edge Detection Algorithm," International Journal of Computer Applications (0975 – 8887), vol. 60, no. 4 ,2012.
19. R. Popa, "An analysis of steganographic techniques" The Politehnica University of Timisoara, Department of Computer Science and Software Engineering, 1998
20. A. Kumar and S. Khurana, "Steganalysis Technique on Gray scale Image by Varying Message Length using Adaptive Histogram Equalization Attack", International Journal of Computer Applications, Vol. 90, No. 14, pp. 33-36,2014.
21. C. Stanley, "Pairs of Values and the Chi-squared Attack", Master's thesis, Department of Mathematics, Iowa State University, 2005
22. J. Canny, "A Computational Approach to Edge Detection," IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 8, pp. 679-687, 1986.
23. TALAI Zoubir, TALAI Abdelouaheb, "A Fast Edge Detection Using Fuzzy Rules," International conference on CCCA, pp. 1-5, 2011.
24. T. Chaira and A.K. Ray, "A new measure using intuitionistic fuzzy set theory and its application to edge detection", Applied Soft Computing, Vol. 8, No. 2, pp. 919-927, 2008.