Iraqi Journal for Computers and Informatics (IJCI)
doi:10.25195/2017/4311
Vol. [43] Issue[1] 2017

Corners-based Image Information Hiding Method

Ahmed Talib [1, 2]

[1] IT Dept., Technical College of Management, Middle Technical University (MTU), Baghdad, IRAQ
dr.ahmed.talib@mtu.edu.iq

[2] Research and Development Dept., Ministry of Higher Education and Scientific Research, Baghdad, IRAQ
ahmedtz@rdd.edu.iq

Abstract: ***The huge explosion of information over World Wide Web forces us to use information security methods to keep it away from intruders. One of these security methods is information hiding method. Advantage of this method over other security methods is hiding existence of data using carrier to hold this data embedding inside it. Image-based information hiding represents one of widely used hiding methods due to the image capability of holding large amount of data as well as its resistance to detectable distortion. In last decades, statistical methods (types of stego-analysis methods) are used to detect existing of hidden data. Therefore, areas that have color variation (edges area) are used to hide data instead of smooth areas. In this paper, Corners points are proposed to hide data instead of edges, this to avoid statistical attacks that are used to expose hidden message. Additionally, this paper proposes clearing least significant bit (CLSB) method to retrieve data from stego-image without sending pixels' map; this will increase security of the proposed corner-based hiding method. Experimental results show that the proposed method is robust against statistical attacks compared with edge- and sequential-based hiding methods. SVM classifier also confirms the outperformance of the proposed method over the previous methods by using Corel-1000 image dataset.***

Keywords: Information Hiding, Corners, Steganography, Edges, SVM Classifier.

1. INTRODUCTION

Generally image information hiding system (also called Image Steganography and Image Watermarking) consists of cover-image (carrier) and hidden message to produce stego-image. An overview of image information hiding system is depicted in Figure 1, where embedding procedure is used to hide message in cover image to generate stego image. Whereas, extracting procedure is utilized to extract hidden message from stego-image [1].

Secure messages transmission over the Internet is one of the most urgent operations in recent days. It should make sure that no one can detect the secret message through communication process between the sender and the receiver. To achieve such secrecy, the message must hide in cover media in a way that avoid any metrics that measures possibility hiding message in this cover. Embedding process forces distortion in the cover media. The distortion of cover has two forms visually and/or statistically. This may lead to increase of possibility of detecting the hidden message by attacker. Therefore, the objective of any information hiding technique is to preserve the visual and statistic distortion of the cover media as minimum as possible [2, 3].

Images are considered as an ideal media for information hiding techniques due to its visual flexibility and its suitable size to be sent over the web. Security of information hiding techniques based on the places of embedding. Noisy area (pixels) (area of high-variation colors) is good choice for embedding because they are hard to identify compared with smooth area. Edges pixels are considered as noisy pixels because their color values are different than their neighboring pixels. Consequently, edges are best choice to hide secret message than any other image's areas. Where in smooth areas, any small changes will be noticed by attacker [4, 5]. This research proposes an Information Hiding (IH) technique to hide secret data in the Corner Pixels of cover image. Corner pixels have high variation in their colors. Thus, the proposed IH technique can overcomes stego-analysis methods that can detect any statistical variation of colors in sequential- and edge-based methods. Additionally, hiding pixel map that must send from sender to receiver will be ignored in this proposal IH technique by using clearing LSB. This will increase effectiveness and security of the proposed method.

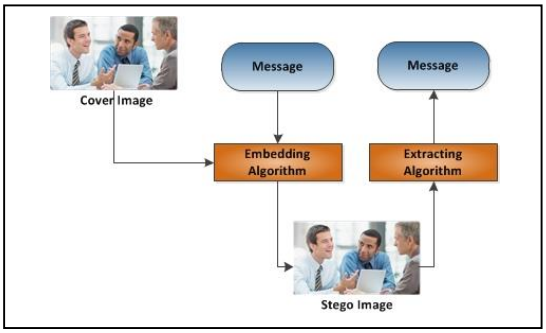


Figure 1: Overview of Image-based Information Hiding System

To evaluate image information hiding system, several factors are used [6-8]. Firstly, Capacity; how much data can embed in cover image. Secondly, Distortion; how much visual quality is degraded after data embedding in cover image. Thirdly, Computation Complexity; how much the computational cost of embedding and extracting procedures. The proposed method outperformed the state of art methods in second and third factors but failed in first factor (capacity) because any image normally has few corner pixels to be used in hiding process.

An organization of this paper is listed as follows. Section II

discusses some information hiding techniques (watermarking and steganography techniques). In Section III, proposed corner-based information hiding is detailed. Section IV shows and discusses the results of experiments. Finally, Section V presents the paper conclusion.

2. RELATED WORKS

There are several IH methods to embed a message securely in a carrier media and also there are other methods to detect the presence of secret message in this carrier. Any IH technique contains embedding and extracting processes. Image-based IH techniques are categorized into two types: spatial domain and frequency (transform) domain [4].

The normal IH technique depends on the least significant bit (LSB) of carrier pixels. In spatial domain type, LSB replacement technique is used. In LSB replacement method [2, 3], LSB of pixel in the cover is replaced by bit from secret message. As result of replacing LSB in the cover, an increasing the pixel value by 1 or decreasing the pixel value by 1 or unchanging the pixel value in the cover image.

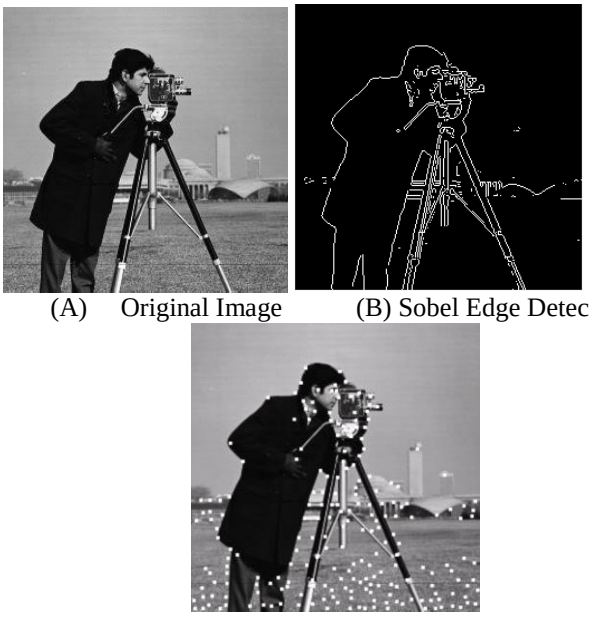
In frequency domain, the LSB-based hiding is achieved by modifying the LSB of non-zero coefficients of certain transform in a cover image. There are different ways to hide data in transform domain as mentioned in [1, 9].

In stego-analysis techniques, the distortion (that is caused by the process of data embedding) is tracked to identify the existence of the hidden message in an image. These techniques are categorized into visual and statistical attacks [8, 9]. Visual attacks are used to detect distortion that is visible to human visual system. Statistical attacks are used to detect any irregularity of data statistics that is caused by steganography. Statistical detectors such as histogram attack [10], sample pair analysis (SPA) [11], RS method [12] and Weighted Stego Analysis (WSA)[13] can reliably detect presence of stego-data and even estimate message length. Some researches such as [3, 4, 6] use edges to hide information in image to avoid such statistical detectors.

3. THE PROPOSED CORNERS-BASED IMAGE INFORMATION HIDING METHOD

Generally, data hiding techniques use edges and non-edges (smooth) area of cover image to save secret information. Although, these techniques have less human visual distortion (that measure by Peak-Signal-to-Noise-Ratio (PSNR) and it depends on secret message size), but it has much statistical distortion. Statistical distortion can be measured by statistical analysis method to stego image only (such as WSA and SPA). Therefore, to reduce statistical distortion, edge pixels are used for information hiding. But in some case edges-based hiding can be detected by stego-analysis methods (SPA and WSA). In order to increase security of hidden message and make it undetectable by stego-analysis methods, Corners pixels instead edges pixels are used.

Information hiding in edges or corner pixels is very hard to detect, where the edge or corner pixels are measured as noisy pixels during embedding process. Figure 2, shows the edges and corner of an example "camera-man" image. These pixels have different colors from their neighbor pixels, that's mean that area has high color variations. In case of hiding secret message in these areas, the possibility of detecting hidden message is very weak. Therefore, a technique is proposed to hide message in corners-based areas. A comparison is made to compare between corner- and edge-based method in terms of visual distortion measure (PSNR) and stego-analysis detection (statistical distortion) measure (WSA and SPA analysis). This is to find the best method in terms of the inability of detecting hidden message.



(A) Original Image (B) Sobel Edge Detector

(C) Susan Corner Detector

Figure 2: Edge and Corner Detection for Camera-Man image

Information hiding process in the proposed corner- based information hiding method (also it can be applied on edge-based method) consists of two phases: Embedding phase and Extracting phase.

Embedding phase includes the following steps, (it can be described as the following algorithm):

EMBEDDING MESSAGE IN IMAGE ALGORITHM
Input: Cover Image, Secret message, Filter (*Filter* represents Type of Edge/Corner detection filter)
Output: Stego-Image
Step 1: { Clearing LSB of Cover Image} CleanedCoverImage ← Clearing (CoverImage)
Step 2: { Apply Edge/Corner detection filter on Cleaned Cover Image to produce Filtered Image that its points represent Hiding map } Hiding Map ← DoFilter (CleanedCoverImage, Filter)
Step 3: { prepare secret message for hiding } BinaryMsg ← Convert2Binary(Secret message)
Step 4: {Embed Binary message in Cover Image depending on Hiding map } Stego-Image ← Embed (CoverImage, BinaryMsg, Hiding Map)
Step 5: Return

In embedding process, it will depend on edge/corner map to hide secret message in cover image. This edge/corner map can be extracted by applying edge filter (such as Sobel, Prewitt, Canny or any other filter) or corner filter (such as

Harris, Förstner, Susan corner detector or any other detectors). The points that resulted from these edge/corner detection are represented as hiding map (the hiding positions in cover image).
Extracting phase can be summarized in following algorithm:

EXTRACTING MESSAGE FROM IMAGE ALGORITHM
Input: Stego-Image, Filter (*Filter* represents Type of Edge/Corner detection filter)
Output: Secret message
Step 1: { Clearing LSB of Stego Image} CleanedStegoImage ← Clearing (StegoImage)
Step 2: { Apply Edge/Corner detection filter on Cleaned Stego Image to produce Filtered Image that its points represent Hiding map } Hiding Map ← DoFilter (CleanedStegoImage, Filter)
Step 3: Extract Binary message from Stego-Img depending on hiding map BinaryMsg←Extract (Stego-Img, Filter)
Step 4: Convert Binary message to Character secret message Secret message ← Binary2Char**(**BinaryMsg**)**
Step 5: Return

In extracting phase, also the edge/corner filter on stego-image is applied to find hiding locations (hiding map) to extract secret message from stego-image. There is one big problem, that is hiding map in embedding phase is different from that in extracting phase. This is because, when embedding bits of secret message in cover image (depending on hiding map) to produce stego-image. Stego-image will be different from cover image; thus hiding map also will be different. Consequently, secret message cannot be extracted.

To overcome this problem, cleaning LSB of cover and stego images before finding hiding map is performed. This will remove the dependence on LSB in producing hiding map. Therefore, the hiding map that extracted from cover image will be equal to this that extracted from stego-image. According to this feature, there is no need to send hiding map from sender to receiver to extract message, just specify the type of filter that is used to find hiding map. This will increase the security of image-based information hiding process, where hiding map will not be exposed; it will be extracted by receiver. Cleaning LSB for image is detailed in the following algorithm:

CLEANING LSB FOR IMAGE ALGORITHM
Input: Img (that is the image to be cleaned)
Output: Cleaned Img
Step 1: {pass to all pixel in image } For i← 0 to Img Width-1 For j ← 0 to Img Height -1
Step 2: {read pixel value from image} Pixel ← Img.getpixel (i, j)
Step 3: { clear LSB from this pixel} NewPixel ← Pixel & FEh
Step 4: { put cleaned pixel on new image} CleanedImg.putpixel(i, j, NewPixel**)**
Step 5: { Repeat until cleaning all pixels in image} Next j
Next i
Step 6: {return resulted Image} Return (CleanedImg)

4. RESULTS AND DISCUSSION

4.1 Experimental Settings

In case of data, Corel dataset that contains 1000 color images of different sizes are used for testing in the experiments. Hidden messages are also chosen of different sizes to show the effect of size on performance, as shown in Table 1. Replacing least significant bit (LSB) method is used in this paper as hiding method where three color channels will be participated in the process. Additionally, WSA and SPA stego-analysis methods are used to measure statistical distortion to test reliability of proposed corner-based hiding method. As visual distortion, Peak-signal-to-noise-ratio (PSNR) metric is used to measure this distortion. As Edge detector, the Sobel edge detector is used whereas Susan Corner detector is used as Corner detector.

Table 1: Different messages' sizes which are used in this work.

Message Name	Length
Msg512	512 Bytes
Msg1K	1-Kilo Bytes
Msg2K	2-Kilo Bytes
Msg4K	4-Kilo Bytes

4.2 Results of Statistical Experiments

The result of Table 2, shows the visual distortion is unnoticeable because PSNR is larger than 30 in all cases. That is mean, there is no noticeable distortion can be detect by human visual system where large PSNR value is better than small value. Additionally, PSNR in the proposed corner-based hiding method is better than edge-based method because the hiding process is spread along the image rather than it focused on small region. Also, PSNR in edge-based method is better than that in sequential hiding for the same reason. Also, corner-based method is not allowed with hiding of large message because of limitation of number of corner points. That mean, it does not allow high distortion.

Table 2: Average PSNR value for all dataset images when using Sequential, Edge and Corner-based Hiding.

Hidden Message Size	PSNR value of original image compared with stego-image in-		
	Sequential hiding	Edge-based hiding	Corner-based hiding
Msg512	83	87	92
Msg1K	66	72	78
Msg2K	60	64	69
Msg4K	55	60	Not applied

As statistical distortion, the Sample Pair Analysis (SPA) [11] and Weighted-Stego Analysis (WSA) method [13] are

applied because they are well-known and widely used statistical analysis methods for estimation the length of hidden message in stego-image. Table 3 and Table 4 show the estimated values of Analysis methods when applied on original and stego-images of different-size hidden messages.

Table 3: Average SPA value (estimated length of hidden message) for all dataset images when using Original, Sequential, Edge and Corner-based Hiding Images.

Hidden Message Size	**SPA Analysis Value of**			
	Original Image	Stego-Image using Sequential hiding	Stego-Image using Edge-based hiding	Stego-Image using Proposed Corner-based hiding
Msg512	0.010	0.019	0.016	0.008
Msg1K		0.025	0.019	0.012
Msg2K		0.027	0.022	0.013
Msg4K		0.031	0.024	Not applied

As shown in Table 3 and Table 4, SPA and WSA analysis methods are used to estimate length of hidden message in stego-image. Logically, WSA and SPA values of original image (there is no hidden message) will have smaller value than that extracted from stego-images. This is because, stego-images have hidden message that effect on statistical distribution of pixel values.

Table 4: Average WSA value (estimated length of hidden message) for all dataset images when using Original, Sequential, Edge and Corner-based Hiding Images.

Hidden Message Size	WSA Analysis Value of			
	Original Image	Stego-Image using Sequential hiding	Stego-Image using Edge-based hiding	Stego-Image using Proposed Corner-based hiding
Msg512	0.012	0.024	0.019	0.011
Msg1K		0.030	0.025	0.013
Msg2K		0.033	0.027	0.015
Msg4K		0.035	0.029	Not applied

From Tables' values, it can be notice that stego-image with sequential hiding has larger value of WSA and SPA analysis because sequential hiding will change statistical map of image's pixels. Whereas, in edge- and corner-based hiding method, the changing of pixels map is unnoticeable because that these pixels are located within area of different colors (high-variation colors). Therefore, the value of WSA and SPA analysis of stego-images of edge- and corner-based method less than sequential hiding method. When comparing between proposed corner-based method and edge-based method, the results show that WSA and SPA values (estimated message length) of corner- is less than the value of edge-based methods due to the participated pixels of corner method has high variation of colors compared with these of edge-based methods.

4.3 Results of Machine Learning Experiments

To approve statistical results of previous section, the machine learning method (Support Vector Machine (SVM) of multi-class classifier) is used. Firstly, SVM can be trained on specific percentage of dataset (Corel dataset of 1000 images), where training will done on discrimination features (SPA and WSA values in this research) that extracted from original and stego-image with sequential, edge-based and corner-based hiding with different message lengths. Secondly, classifier will be tested on the remaining percentages of images of dataset; results are shown in Table 5.

Table 5: Accuracy of SVM multi-class classifier on Corel Dataset of different Hiding methods with different splitting of dataset with 5 and 10 k – fold cross validation.

K-Fold	Training percentage of dataset	Testing percentage of dataset	Accuracy	Hiding Methods
K=5	70%	30%	100	Sequential
			90	Edge-based
			68	Proposed Corner-based
	50%	50%	96	Sequential
			85	Edge-based
			56	Proposed Corner-based
K=10	70%	30%	100	Sequential
			92	Edge-based
			69	Proposed Corner-based
	50%	50%	96	Sequential
			85	Edge-based
			59	Proposed Corner-based

In Table 5, the results of SVM multi-class classifier with different partitioning to Corel dataset is presented. the values 5 and 10 in k-fold cross validation are used to ensure the reliability of results. Additionally, Corel-1000 images dataset are partitioned into either (70%,30%) or (50%,50%) for training and testing the classifier respectively for fair distribution of data during classification process [14, 15].

To analysis the results, the classifier detects easily the hidden sequential message where the accuracy of detection was over 95%. In edge-based hiding, the accuracy of classifier to detect hidden message was over 85%. This mean the security of hiding message using edges was higher than sequential method, thus classifier cannot be sure from detection the hidden message. Whereas in the proposed corner-based hiding, the accuracy of classifier of detecting hidden

message was very low (50%-60%). This will ensure that the security of hiding message is very high. From worth mentioning, the MATLAB 2015 is used to implement feature extraction (SPA and WSA features) and SVM classification processes.

5. CONCLUSION

In this paper, corner-based information hiding method is proposed to hide data inside image. This is to increase security of hidden message, to avoid detect it by statistical stego-analysis (SPA and WSA) methods. Proposed method outperforms the state of art methods (edge- and sequential-based hiding methods). Additionally, sender and receiver can use edge or corner filter to find hiding map without needing to send it, this increase security of proposed method. Metrics to measure Visual and Statistical distortion (PSNR, SPA and WSA) are used to show outperformance of the proposed method. Moreover, machine learning algorithm (SVM) is also applied on Corel-1000 image dataset to confirm reliability of proposed method.

References

[1] M. Pavani, S. Naganjaneyulu, and C. Nagaraju, "A survey on LSB based steganography methods," International Journal Of Engineering And Computer Science ISSN, pp. 2319-7242, 2013.

[2] K. N. BrahmaTeja, D. G. Madhumati, and K. R. K. Rao, "Data hiding using EDGE based steganography," International Journal of Emerging Technology and Advanced Engineering, vol. 2, pp. 285-290, 2012.

[3] M. R. Modi, S. Islam, and P. Gupta, "Edge based steganography on colored images," in International Conference on Intelligent Computing, 2013, pp. 593-600.

[4] K. Hempstalk, "Hiding behind corners: Using edges in images for better steganography," in Proc. Computing Women's Congress, Hamilton, New Zealand, 2006.

[5] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, pp. 1613-1626, 2003.

[6] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," IEEE Transactions on information forensics and security, vol. 5, pp. 201-214, 2010.

[7] W.-J. Chen, C.-C. Chang, and T. H. N. Le, "High payload steganography mechanism using hybrid edge detector," Expert systems with applications, vol. 37, pp. 3292-3301, 2010.

[8] P.-Y. Chen and H.-J. Lin, "A DWT based approach for image steganography," International Journal of Applied Science and Engineering, vol. 4, pp. 275-290, 2006.

[9] K. Bailey and K. Curran, "An evaluation of image based steganography methods," Multimedia Tools and Applications, vol. 30, pp. 55-88, 2006.

[10] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems breaking the steganographic utilities EzStego, Jsteg, Steganos, and S-Tools—and some lessons learned Lecture notes in computer science. vol. 1768," ed: Berlin: Springer-Verlag, 2000.

[11] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," IEEE transactions on Signal Processing, vol. 51, pp. 1995-2007, 2003.

[12] J. Fridrich, M. Goljan, D. Hogea, and D. Soukal, "Quantitative steganalysis of digital images: estimating the secret message length," Multimedia systems, vol. 9, pp. 288-302, 2003.

[13] J. Fridrich and M. Goljan, "On estimation of secret message length in LSB steganography in spatial domain," in Electronic Imaging 2004, 2004, pp. 23-34.

[14] S. Lyu and H. Farid, "Detecting hidden messages using higher-order statistics and support vector machines," in International Workshop on Information Hiding, 2002, pp. 340-354.

[15] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," IEEE Transactions on information forensics and security, vol. 7, pp. 432-444, 2012.