A Review on Edge Based Image Steganography

Deepika Dongre
Assistant Professor
Department of Computer Science & Engineering
Acropolis Technical Campus
Indore, India
deepikacs1912@gmail.com

Rina Mishra
Research Scholar
Department of Computer Science & Engineering
Patel College of Science & Technology
Indore, India
rinamishra.cse13@gmail.com

Abstract-Security of the information has always been the interesting area for researchers. Integrity, Confidentiality, and Authentication are main security principles. There are so many techniques developed to achieve these security principles using cryptography. But all these techniques are unable to keep the communication secret. Although the attacker is unable to access the secret message but he knows about the existence of the message. To overcome this limitation of cryptography a new idea is proposed by researchers that is Steganography. Steganography is the art of concealing secret message in a carrier such as text, image, audio, video and protocol messages. Different Steganography techniques are used based on these carrier messages and way of hiding. The choice of these method is depends on the requirements of application. Some application requires huge data embedding and some require high secrecy.

This paper gives a review on image Steganography based on edge detection and their comparative study. It also gives an overview of basic edge detection techniques.

Keywords- *PVD; LSB; Steganography; Integrity; Confidentiality; Authentication and Cryptography.*

*****

I. INTRODUCTION

The rapid development of technology enables high-speed and economic communication worldwide. With innovation of technology security threats are also growing rapidly. Security is the vital requirement of a communication from international communication to personal communication. A technique which only secures the content of messages like cryptography increases the chances of compromising the security. But Steganography is the technique to hide the fact that communication is taking place. It is the best way to secure the communicating messages because if attacker is unaware about the communication the chances of attack are reduced automatically.

A. Overview of Steganography:

Steganography is the Greek word which is made up of two words “stegos” means covered and “grafia” means writing, so Steganography means covered writing [1]. Steganography enables secret communication between source and destination. The main aim of Steganography is to hide secret information in carrier medium in such a way that it looks like an original medium.

Previously, various methods based on Steganography were used like wax tablet, invisible ink and shave heads and many similar techniques. In wax tablet, the secret message was written on wood and further covered with wax. In another technique, invisible ink was used to write the secret message which becomes visible only when paper got heated. Many times master used to shave his slave’s head wrote his secret message on his scalp. When slave’s hair grew up then he sent him to intended receiver. The receiver again shaved slave’s head and got the secret message.

One more technique called Microdot was developed in Germany at the time of Second World War. The photographic information was reduced in size of typed period and it was embedded into cover image.

The concept of Steganography can be understood with the help of Prisoner’s problem [3]. Two inmates hatch a plan to escape from prison. A warden is observing the secret communication. If the warden will come to know about the secret communication, he will throw in solitary confinement. That’s why they starts communicating in such a way that warden don’t know about their secret communication. They used to hide their messages into another carrier object to be unperceived.

The terms used in Steganography are: stego image, cover image, secure message and stegonalysis. Secure message is the message which we want to keep secure. Cover image is the carrier image which contains hidden message. So the stego image is that cover image which is going to be transferred with a secret message.

B. Types of Steganography:

Steganography are of different types which depend on the type of carrier medium. The carrier medium of high redundancy is most preferable choice. The commonly used mediums are [1]:

- Text Steganography: The secret message is hided in a text file which is transfer through open channel. The characters of secure message are embedded at specific character of each word or selected word. The Message hiding depends upon stego key.
- Image Steganography: Image is the most popular cover object for Steganography due to its privileged redundancy. The minor changes in image pixel are unnoticeable to human visual system and this property is utilized in image Steganography.
- Audio Steganography: It is similar to image Steganography with minor changes in audio carrier that is unnoticeable to human ear. It is not widely used due to large size of audio cover file as compare to text and image cover.

- Video Steganography: Video is the combination of audio and image. The large amount of secret messages can be embedded in the video cover.
- Protocol Steganography: The protocol messages are also used to hide secure messages. All those messages which are going to be transfer during communication according to TCP/IP protocol suit can be utilized for this purpose.

II. Literature Survey

Steganography is based on two important factors; first is the type of carrier and other is way of embedding. Various carriers are used as cover message for Steganography. Image Steganography is the extensively used carrier medium because images are the most frequently transferable messages over the Internet. There are lots of research have been done in the field of image Steganography. The image Steganography is basically divided into two types [4][5]:

- *Spatial domain:* This technique directly embeds the information in the intensity value of the pixels. It is specially used for images which uses lossless compression. Because embedding depends on image format. Least Significant Bit (LSB) replacement technique widely used in spatial domain.
- *Transform domain:* This technique embeds the information in frequency domain of previously transformed image. Discrete Cosine Transform and many more transformation techniques are used for hiding the data in image. JPEG images which uses lossy compression can be utilize in this technique.

There are so many techniques are proposed for image Steganography based on concept of hashing, message scrambling, edge detection and many more. This paper is mainly focused on edge based image Steganography.

Edge based Steganography:

Edge based Steganography is used to take the advantage of being undetected, because editing in edge areas cannot be easily detected by human visual system. Edge area may contain large number of secret bits as compared to smooth areas.

Edge: Edge is an important feature of an image used to fully interpret an image. An edge differentiates an image from background and differentiate adjacent component of an image. Edge of an image gives fundamental information about the image such as area, perimeter and shape.

Edge Detection: Edge detection is the process of identifying the sharp changes in intensity of adjacent pixels. The point where discontinuity occurs in image is identified as edge. Edge detection is the fundamental tool for image processing.

The basic techniques used in edge detection are classified as follows [6]:

A. Gradient Based Edge Detection
B. Gaussian Based Edge Detection

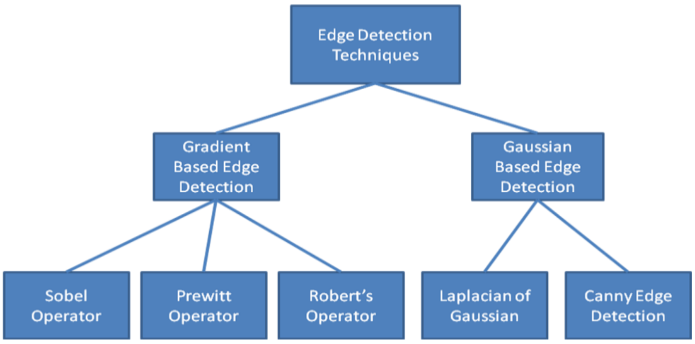

Figure 1 Classification of Edge Detection Techniques

A. Gradient Based Edge Detection:-

The edge detection in gradient method is based on maxima and minima of the first derivative of the image. Gradient is a vector, whose magnitude represents the strength of edge pixel and direction represents the direction of edge. Gradient is based on changes in pixel intensities. The pixel with high gradient is detected as edges. The natural images don't have sharp edges so that a threshold value is set to detect the edge pixels. If the magnitude of gradient of a pixel is greater than threshold that pixel comes in category of edge pixel.

Gradient magnitude $G(x,y)= (\Delta x^2 + \Delta y^2)$ ½

Gradient direction $\theta(x,y) = \tan(\Delta y/ \Delta x)$

where $\Delta x= f(x+n,y)-f(x-n,y)$, $\Delta y=f(x,y+n)–f(x,y-n)$ and n is a small integer, usually unity.

The gradient for the natural images can be estimate using operators such as Sobel, Prewitt and Robert's operator.

1) *Sobel Operator:* Sobel operator is discrete differentiation operator used to calculate 2-D spatial gradient of image intensity function [7]. The Sobel method convolves an image with a small, separable and integer valued filter in horizontal and vertical direction. Sobel uses 3x3 mask, which are convolved with the original image to calculate the approximate of the derivatives. The mask Sx and Sy are given as follows:

$$Sx= \begin{pmatrix} 1 & 0 & 1 \\ -2 & 0 & 2 \\ 1 & 0 & 1 \end{pmatrix}$$

$$Sy= \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{pmatrix}$$

2) *Prewitt Operator:* Prewitt Operator calculates magnitude and orientation of edges with the help of kernel. It is limited to 8 orientations. Eight convolution masks are calculated and the convolution with largest value is selected. The mask are

$$Sx= \begin{pmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{pmatrix}$$

$$Sy= \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ -1 & -1 & -1 \end{pmatrix}$$

3) *Robert's Operator:* The Rober's operator calculates 2-D spatial gradient of an image. The pixels which have high spatial frequency are detected as edge pixel. Mask used by Robert's operator are:

$$Sx= \begin{pmatrix} -2 & 0 \\ 1 & 0 \end{pmatrix}$$

$$Sy= \begin{pmatrix} -2 & 0 \\ 1 & 0 \end{pmatrix}$$

B. Gaussian Based Edge Detection

1) Laplacian of Gaussian: The Laplace method [8] finds the second derivative and further zero crossing of this derivative to detect edges. The second derivative is sensitive to noise. So Laplacian of Gaussian is used to overcome the noise. The image is first filtered through Gaussian filter to smooth the image then Laplace is applied to find second derivative for enhancement. And the last step is detection of edges with the help of zero crossing in the second derivative with the corresponding high peak in the first derivative.
2) Canny Edge Detection: Canny edge detection [9] is based on finite difference approximation of the partial derivative. First image smoothing is performed using Gaussian filter then gradient magnitude and orientation is computed with the help of partial derivative. Further non maxima suppression and threshold technique applied for accurate edge detection.

Edge detection based image Steganography review:

In this section, we are presenting some of the research work of the prominent authors in this field and will be giving various ways in which secure image Steganography is done using edge detection**.**

In **"Hiding behind corners using edge in image for better Steganography"** [10] author eliminates the need of sending original cover image for extract the secret message from stego image. They gave an idea of a new method Battlesteg which is combination of traditional Hideseek and Filterfirst method. Hideseek is a method in which a random seed is used to select the bit to hide secret message bit. The hideseek method is open to Steganalysis by using Laplace magnitude count. To overcome this problem Filterfirst algorithm is proposed in which Laplace filter is used to detect edge pixel and hiding is performed at highest value of Firstfilter. Battlesteg is combination of both these methods in which a random pixel position is picked and h% of the highest filter value is used for hiding the secret message. The author perform Steganalysis of four algorithms Blindhide, Hideseek Filterfirst and Battlesteg using WEKA's Support Vector Machine. The experimental results showed that Firstfilter gave the best performance over other three methods.

In **"Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems"** [11], author proposed an adaptive image Steganography technique based on LSB and pixel value difference technique. This research enhanced the concept given by" **Wu and Tsai's scheme**". First the image is divided into 2x2 blocks and pixel value difference is calculated. The three levels high level, middle level and low level are decided according to this difference. The edge area may contain large number of bits as compare to smooth area without being detected. So the number of secret message bits embedded into pixel depends on the level in which this difference exists. Same numbers of bits are embedded in both pixels of 2x2 blocks. Then modified LSB substitution is applied and readjusting is performed if embedding changes the level of pixel value difference. An experimental comparison is performed between Wu *et al.*'s, method and this proposed method. The experiment is performed for 3-4 division and 3-4-5 division. The proposed approach gave higher PSNR than Wu *et al.*'s method in both divisions. It also provides higher embedding rate.

In **"A high quality steganographic method with pixel-value differencing and modulus function"** [12], author presented improved PVD method with modulus function. Instead of modifying the pixel value the reminder of two consecutive pixels is calculated and secret data is embedded by modifying these reminder values. The experiment result shows that the proposed algorithm gave better performance than Wu and Tsai's scheme. It gives higher PSNR ratio because edge distortion is highly improved. It also provides better performance than Chang and Tseng's two-side match scheme. It is robust against the RS detection attack.

In **"High payload Steganography mechanism using hybrid edge detector"** [13], author proposed an approach that provides high embedding capacity and better quality stego image by combing LSB technique with edge detection. Two edge detection techniques fuzzy edge detection and canny edge detection are performed on image successively. The combination of both edge detectors gives large number of edge pixel with less computational overhead. After detecting the edge pixel image is divided into block of n pixel and first pixel contain status information of all pixels in that block. And finally embedding is performed based on edge pixel and smooth pixel using LSB substitution method. The proposed method has property to resist Steganography from statistical Steganalysis.

The difference in cover image and stego image increases the chances of Steganalysis. Several techniques proposed by researchers based on pixel value differencing (PVD). But most of the PVD methods are affected by histogram based attack. It is assumed that Steganography gives the uniform distributed message histogram but it is not really possible. The PVD Steganography modify the histogram so the steganalyst can take advantage of this property to detect the existence of secret message. In **"Adaptive Steganographic method using floor function with practical message formats"** [14], author presented an adaptive and secure steganographic algorithm to preserve histogram with the help of PDHist table, Candidate table and Takefill adjusting Algorithm. PDHist table maintains the lower and upper bound of PVD histogram for each pixel difference value. The embedding is performed through new steganography algorithm which can alter the difference by one and TakeFill algorithm is used for adjusting the histogram. Candidate table is also used to deal with changes in histogram of cover and stego image. The experimental analysis done and the performance of proposed method is compared with previously PVD based methods. This method proved secure against well known Steganalysis and all histogram based attacks.

In "**Information Hiding Using Edge Boundaries of Objects**", [15] author pay more attention on difference of boundary pixel of cover image and stego image. Some methods applied on stego object to reduce this difference so that stego image can be used at the receiver side as an original image for further processing. First the edges are detected using canny edge detector. Then absolute difference of edge pixel and its upper edge pixel is calculated. If this difference is less than threshold value then LSB technique is used for embedding. Now again edge detection of stego image is performed using canny edge detector. If edges are not identical then threshold value is updated. This process is repeatedly performed until edges of cover image and stego image is not identical. This method is more secure and having low computational overhead.

In **"Chaos based Edge Adaptive Image Steganography"** [16] , author uses the fact that some region of the image like edges or any specific object are more efficient for hiding the secret information and these regions are called region of interest(ROI).This approach uses the edge as ROI to embed secret information. First the scrambling is performed using Cat mapping technique, edges are detected using canny edge detector then message is embedded into edges. Cat mapping is applied to increase the security of hidden message. The matrix encoding and LSB matching is used for embedding. The experiment performed with sample images and result shows high PSNR for all sample cover images and payload sizes. It produces high fidelity stego image with minimum visible distortion. A most important benefit of this approach is that if an adversary knows about existence of secret information, he will never be able to access that information. It is managed with the help of chaos based payload scrambling-descrambling.

In **"Steganography in images using Sobel Edge Detection with 2^k Correction Method"** [17], author proposed an edge based image Steganography that uses sobel edge detector and 2^k correction method. To provide better imperceptibility 2k method is used because cover image and stego image have differences. If the difference of actual pixel value and Stego Pixel Value (SPV) is greater than2^k-1 then stego pixel value is modified by SPV-2^k or SPV+2^k. The PSNR and Mean Square Error (MSE) are calculated in experiment. This method provides better embedding capacity and PSNR than LSB technique.

Following table shows the comparative analysis of image based image Steganography techniques.

TABLE I

COMPARATIVE ANALYSIS OF EDGE BASED IMAGE STEGANOGRAPHY TECHNIQUES

Proposed Method	**Mechanism**	**Benefit**
Hiding behind corners	Combination of Hideseek and Filterfirst method, Filterfirst method uses Laplace filter for edge detection	Eliminates the need of sending original cover image with stego image
Adaptive data hiding in edge areas of images with spatial LSB domain systems	Combination of modified LSB and PVD	Higher PSNR and embedding rate than Wu *et al.*'s method
A high quality Steganography method with pixel-value differencing and modulus function	Based on PVD, embedding is done by modifying the reminder of pixels of each block	Robust again RS detection attack
High payload Steganography mechanism using hybrid edge detector	Fuzzy and Canny edge detector is used for edge detection and LSB for embedding	Robust against statistical Steganalysis
Adaptive Steganographic method using floor function with practical message formats	PDHist table, Candidate table and Takefill adjusting Algorithm used for message histogram preservation	Secure against Steganalysis and histogram based attack
Information Hiding Using Edge Boundaries of Objects	Canny edge detection is performed before and after the message embedding for better imperceptibility	More secure and low computational overhead
Chaos based Edge Adaptive Image Steganography	Message scrambling using Cat mapping, matrix encoding and LSB used for embedding	Higher PSNR for all cover images and for any payload size
A New Image Steganography Based on 2^k Correction Method and Canny Edge Detection	Based on sobel edge detector and 2^k correction method	Better embedding capacity and PSNR than LSB technique

III. CONCLUSION

Steganography is a prominent method for secure communication. The area where the use of cryptography is strictly prohibited, Steganography is the best solution. Sometimes both these methods are used in combination to provide more security. The purpose of this paper is to review different edge based image Steganography techniques and their comparative analysis. Different edge detectors such as canny edge detector, Sobel operator, Laplace formula and other terms when applied in combination provide best image Steganography algorithm with higher imperceptibility.

References:

[1] T.Morkel, J.H.P.Eloff, M.S. Olivier,"An Overview of image steganography"

[2] Pritam Kumari et.al,"Data Security Using Image Steganography and Weighing its techniques",International Journal Of Science & Technology Research Volume 2, Issue 11, November 2013

[3] G. Simmons, "The prisoners problem and the subliminal channel",CRYPTO, pp. 51-67, 1983.

[4] M. Goljan, J. Fridrich, and T. Holotyak, New blind steganalysis and its implications, IST/SPIE Electronic Imaging: Security, Steganography of Multimedia Contents VIII, vol. 6072, pp. 1-13, 2006.

[5] Y. Wang and P. Moulin, Optimized feature extraction for learning-based image steganalysis, IEEE Trans. Information Forensics and Security, vol. 2, no. 1, pp. 31-45, 2007.

[6] G.T. Shrivakshan, Dr.C. Chandrasekar "A Comparison of various Edge Detection Techniques used in Image Processing", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 1, September 2012

[7] Nick Kanopoulos, et.al. ; "Design of an Image Edge Detection Filter using the Sobel Operator", Journal of Solid State Circuits,IEEE, vol. 23, Issue: 2, pp. 358-367, April 1988.

[8] Huertas, A. and Medioni, G., "Detection of intensity changes with sub pixel accuracy using Laplacian-Gaussian masks," IEEE Trans. On Pattern Analysis and Machine

[9] Dr.S.Vijayarani1, Mrs.M.Vinupriya ,"Performance Analysis of Canny and Sobel Edge Detection Algorithms in Image Mining", International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 8, October 2013

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

[11] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun,"Adaptive data hiding in edge areas of images with spatial LSB domain systems," IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 488–497, Sep. 2008.

[12] C. M. Wang, N. I. Wu, C. S. Tsai, and M. S. Hwang, "A high quality steganography method with pixel-value differencing and modulus function," J. Syst. Softw., vol. 81, pp. 150–158, 2008.

[13] Wen-Jan Chen, Chin-Chen Chang, T-Hoang Ngan Le, "High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications 37 (2010) 3292–3301, ELSEVIER.

[14] J.C.Joo,T.W.Oh,H.Y.Lee and H.K.Lee,"Adaptive Steganographic method using floor function with practical message formats",International Journal of Innovative Computing,Information and Control Volume 7,Number 1,January 2011

[15] M. Hussain,"Information Hiding Using Edge Boundaries of Objects", International Journal of Security and Its Applications Vol. 5 No. 3, July, 2011

[16] R.Roy,A. Shankar,S.Changder," Chaos based Edge Adaptive Image Steganography", International Conference on Computational Intelligence: Modeling Techniques and Applications(CIMTA) 2013.

[17] Simrat Pal Kaur and Sarbjeet Singh, "A New Image Steganography Based on 2k Correction Method and Canny Edge Detection", International Journal of Computing & Business Research ISSN: 2229-6166 2014.