A Payload Enhancement using Hybrid Canny-Sobel Edge Area Detection

V. Dharanya[1],Dr.S.Jhansi Rani[2],S.S Nandini[3]
[1]M.Tech Student,Department of Computer Science & Systems Engineering
[2]Associate Professor, Department of Computer Science & Systems Engineering
[3]Research Scholar, Department of Computer Science & Systems Engineering

Abstract: *In this research a new method for increasing the embedding capacity in images based on the edge area is proposed. The new approach combines Canny and Sobel edge detection techniques to get wider edge area than existing approach combines Canny and Prewitt. Our new approach gives more embedding capacity therefore payload capacity of messages that can be inserted in the edge area increases. The secret message is concealed using the Least Significant Bit (LSB) method. Embedding capacity, PSNR for Peak Signal to Noise Ratio, SSIM for Structural Similarity Index Measurement, and MSE for Mean Square Error values are used as evaluation metrics. Based on the resulted values, the proposed method showed higher embedding capacity while keeping the PSNR, SSIM, MSE values without major changes of other methods which means keeping the imperceptibility quality of the stego image.*

Keywords: Image steganography, LSB, Hybrid edge detection, Canny, Sobel, PSNR (Peak Signal to Noise Ratio), SSIM (Structural Similarity Index Measurement), MSE (Mean Square Error).

1. Introduction

Information security and privacy have become a high priority due to urgent demand for data transmission over public channels, the use of cloud services, and multimedia transmission over social networks. Two main techniques to protect the confidentiality of the transmitted information, cryptography and steganography. Cryptography, on one hand, is the process of converting confidential information into a non-readable form however, the encrypted information raises the doubts of the intruders and reveals the importance of the data [1]. On the other hand, steganography is a technique for concealing secret information inside different types of media such as image, audio, video, etc., which is called the cover [2].

Images are considered as one of the most popular file formats in steganography, which is known as Image Steganography.[3]. Three main factors to be considered in image steganography are imperceptibility, robustness, and capacity. Imperceptibility is used for image quality measurement by applying the Peak Signal-To-Noise (PSNR). The second factor Robustness refers to protecting the secret data against any manipulation or attacks by the eavesdropper. Capacity, also known as payload, refers to the secret information amount to be hidden in the cover image [2, 4].

LSB is one of the techniques that is used in image steganography in a spatial domain. It is a very popular method that does not require high computational complexity and provides high embedding capacity [4]. The lower-order bits of the image pixels are substituted with the secret information bits [5]. Using classical LSB by itself in image steganography can be considered as a predictable and not a very strong method. Some researchers work on combining LSB with other methods to ensure data secrecy, such as using encryption techniques to encrypt the secret information before embedding it in the cover image [6, 7]. Others work on hiding the information in specific areas of the cover image such as the image edges area [8]. Edge areas are extracted by applying one of the edge detection methods such as Canny, Sobel, Roberts, Prewitt, etc.

This paper introduces a data hiding method based on embedding the secret information in a binary form within the edge area of a cover image. The main goal is to hide confidential information in a way that any unauthorized receivers will not suspect the secret text's existence. The edges of the image are extracted using a technique that combines Canny and Sobel methods together. LSB is used to embed the secret message.

2. Literature Survey

Naida A.Mohsin,Huda A. Alameen [24], propose a method aimed to increase the payload of the secrete message inside the image pixels. The reason behind using the edge area is to conceal extra secret bits without affecting the image quality because the image edge area can better tolerate the changes in the image pixels. A combination between Canny and Prewitt edge detector is used to get a thicker edge area. These two edge detection techniques methods provide a bigger edge area for more payload of message while maintaining the stego-images imperceptibility.

S. K u m a r, A. S i n g h and M. K u m a r [4], also work on hiding the secret data in the edge area. In this article, an adaptive method based on a novel fuzzy edge identification is presented. The method works on inserting secret information in gray images. The insertion does not have a perceptible change in the cover images. The method locates the sharper edges of the cover images effectively and then hides the secret information. The image edges are kept after hiding the secret message to retrieve the data at the receiver side accurately. The experimental results have shown that the proposed method achieves a better quality of stego images than other methods if the same embedding capacity is used.

A r o r a and A n a n d [18], also propose a new technique for concealing the secret text data in the edges of a coloured images edges. First, the edges are detected 100 by scanning the image using a 3×3 window. The text message is embedded in the edge area using the first component alteration technique. The results have shown a high quality of the encoded image and higher embedding capacity.

Y a n g e ta l. [25] proposed a steganographic LSB method using PVD and edge detection to obtain a large embedding capacity while maintaining the stego-image quality. In this study, the image is divided by segmentation using edge detection, so the image is divided into two areas, i.e., the edge area and smooth area. The edge area embeds more messages than the smooth area. This is because the edge image area can provide more tolerance to changes in the value of the pixel. This study has obtained the value of Peak Signal-to-Noise Ratio (PSNR) more than 33 dB with a message capacity of more than 80,000 bits. The cover image employed is a grayscale image with size of 512×512

3. Theory of Image Edge Detector and LSB Steganography

Edge detection techniques are used to identify and locate the sharp discontinuities in an image that occur due to changes in pixel intensity [9]. Edge detection process outlines and detects the image background, objects and object's boundaries. There are many methods for edge detection, but most of them can be grouped into two categories, search-based and zero-crossing-based algorithms [10]. In zero crossing the derivatives of second order is computed for detecting the edges. In search-based, the first-order derivatives are computed. The most popular methods are Sobel, Canny, Prewitt, Roberts, and Laplacian which belong to one of the above categories [11].

Many studies have proven that image edge areas are a better option to embed secret information than any other part of the cover image as any small distortion can be noticeable [12]. One concern in using the edge area is the limited embedding capacity as not all the image pixels can be used for data hiding. The edge area size depends on the method used for detecting it, the larger the edge area size is the better.

Canny edge detector can be considered as the optimal edge detection method and it is better than many other edge detection methods [9]. Applying a canny edge detector works on enhancing the signal to noise ratio. Canny is known for detecting thick edges which means that the larger edge area size is better. This detector has been widely used in various image processing algorithms that require edge detection. Performance of edge detection is highly dependent on the threshold value used [19]. This makes it very popular and widely used because it successfully provides standardized localization solutions and 77 complex mathematical calculations to collect smoothing filters [20].

Sobel detector has the smallest payload. On the other hand, the Sobel detector has obtained the highest PSNR value among other detectors. The two advantages of this algorithm are that it obtains an effect to reduce random noise in the image and that it gives off lighter and brighter-looking edge elements [26]. The Sobel operator is a partial derivative of $f(x, y)$ where x = 3 and y = 3, which technically can compute the gradient of the image intensity. If there is an image (I), then we use the horizontal Gx and vertical Gy templates to convolve the image to get the edge area, with Gx and Gy:

-1	0	+1
-2	0	+2
-1	0	+1

Gx

+1	+2	+1
0	0	0
-1	-2	-1

Gy

LSB is a method in the highly popular spatial domain used in steganography. LSB is traditionally done by changing the smallest bit values in a sequential order. When there is an image pixel value {250, 120, 80, 175} and there is a message with a value of 10, then the steps taken to insert the message are as follows:

1. First, convert the pixel values of images and messages into bit numbers Cover {250: 11111010 | 120: 0111100 | 80: 01010000 | 175: 1010111}, Message {10: 1010}.
2. Next, change the smallest bit of image pixel value with each bit value of the message. Thus, the Stego's bits becomes {11111011 | 0111100 | 01010001 | 010110}.
3. Finally re-convert pixel image bit value into decimal number. The decimal value of Stego-pixels becomes {251 | 120 | 81 | 174}

4. The Proposed Approach

In this paper, A hybrid edge detection method is proposed for detecting the image edges. The hybrid method is performed by combining Canny and Sobel methods. The secret message is concealed in the least significant bits of the cover image pixels. It is embedded only in the pixels that are part of the edge area. The reason behind using this hybrid technique is to increase the number of pixels that can be used to hide the secret message.

1. The first step is done by reading the cover image, and then conducting an edge detection. In the Canny algorithm Sobel filter is incorporated.
2. The second step is about converting the secret test into binary form then hiding it in the edge area pixel of cover image. The Least Significant Bit (LSB) method has been used to hide the text. The result of the previous phases is an image called the carrier image which holds the secret image.
3. In the final phase we extract the secret hidden text depending on the saved map.

4.1. Algorithm of Phase One Edge Detection Using a Hybrid Technique

The image edges in our method are detected by applying Canny and Sobel edge detection methods.

The following steps explain the edge detection phase:

Step 1. Reading the cover image.

Step 2. Extracting the edges using the Canny technique (Gradient is calculated using Sobel filter) and saving the result in an image we call C. Fig. 1b shows the result of this step on the pepper image.

Step 4. Read the secret message, then add one special character at the end of the message

Step 5. Change the secret message to binary form according to ASCII.

Step 6. Embed the secret message into the smallest bit of the image edge pixel cover with the LSB replacement method

Step 7. Get the stego-image.

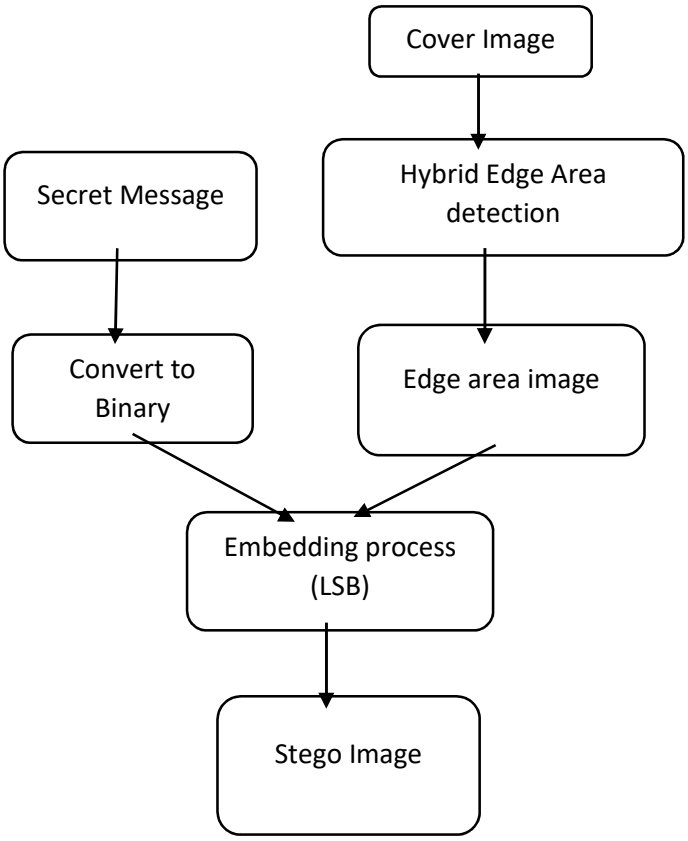


Figure 1. Process of embedding process

4.2. The Process of Extracting Secret Messages

This process is the stage for obtaining a message extraction. In order to obtain a perfect extraction, the extraction process must use the hybrid edge detectors. Fig. 3 illustrates the extraction process in the proposed method.

Here are the details of the steps of the embedding phase as shown in Figure. 3

Step 1 Read stego-image
Step 2. Read hybrid edge area as a key of extraction.
Step 3. Perform the extraction process by converting each pixel into binary form.
Step 4. Get the smallest bits sequentially from the first edge area through the last smooth area.
Step 5. Combine each of the eight smallest bits of each pixel into a character.
Step 6. Repeat the iteration to get special characters that become the final signs of the messages.
Step 7. Get secret message extraction.

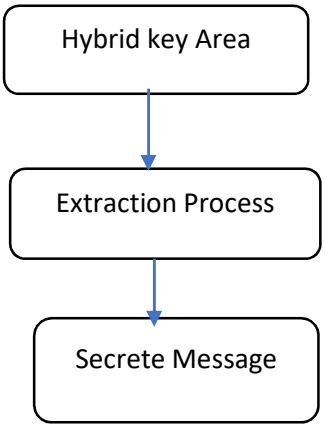


Figure 2. Phase of Extracting secret Image

5. Experimental Result and Analysis

In this section, the experimental results are presented to evaluate the performance of the proposed approach. Our method has been tested and implemented using Colab (Python). This experiment conducts a trial test, on 4 images with size different pixels as cover image and text as messages to be embedded. The sizes of the embedded text messages are 512, 1024, 2048, and 4096 bytes. Each cover image analyses and compares the payload capacity of messages that can be embedded in the image edge area. Fig. 3 shows cover images used in this test.

Each cover image does an edge detection with a Sobel, a Canny and hybrid algorithms. This edge area will be used as a container for storing messages. Fig. 3 is a sample of edge detection of the cover image used (baboon.png, happyfish.jpg, lena.png, and desert.jpg). The edge area shown in Fig. 5 has a significant difference. The edge area obtained from the Canny-Sobel hybrid method has a very clear border. Based on the results of calculations, it is also evident that the entire image of the cover has a bigger number of hybrid Canny-Sobel edge area than the edge area of the Sobel and Canny individually.

Three evaluation metrics have been used, first the embedding capacity. The other factors are standard image quality assessment factors, the Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measurement (SSIM), and MSR for Mean Square Error. The last metric is the Character Error Rate (CER) which is the ratio of wrong extracted characters to the length of the secret message [23].

$$\text{MSE} = \sum \sum \| c(m, n) - s(m. n)\ n\ n{=}0\ m\ m{=}0 \|$$

where m and n are the cover image width and height; c and s stand for the cover image and the Stego image [23].

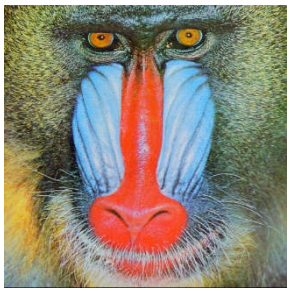
$$\text{PSNR} = 10\log10\ (\ 2552\ \sqrt{}\text{MSE}).$$

PSNR is the way for evaluating the quality of the reconstructed image. It is hard for the human visual system to see the difference between the original image and the stego image with PSNR values less than 35, which means a higher value of PSNR provides better image quality.

The SSIM calculates the similarity between the cover and the stego images. The similarity is calculated regarding contrasts, local luminance, and spatial structure.

SSIM $(C, S) = (2\mu c\mu s+y)\ (2\sigma cs+y2)\ (\mu c\ 2+\mu s\ 2+y1)\ (\sigma c\ 2+\sigma s\ 2+\ y2)$

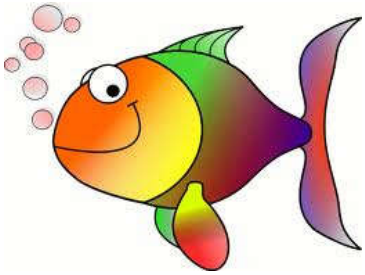
where μc and μs are the means of C and S; σcs is the covariance of the Cover and Stego images; y1 and y2 are the variables for stabilizing the division with a weak denominator; σc 2 and σs 2 are the variants of C and S.



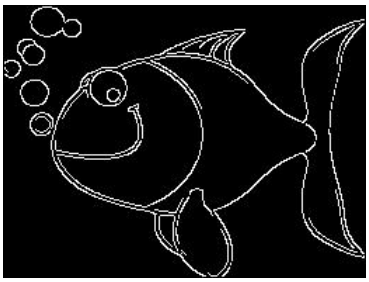
(a)

(b)

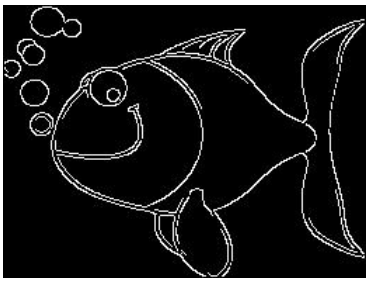
(c)



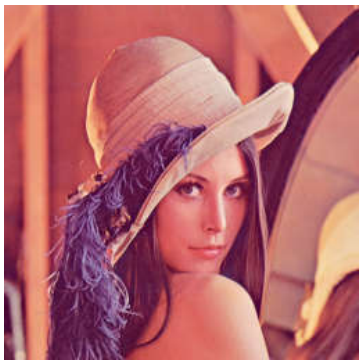
(d)



(e)



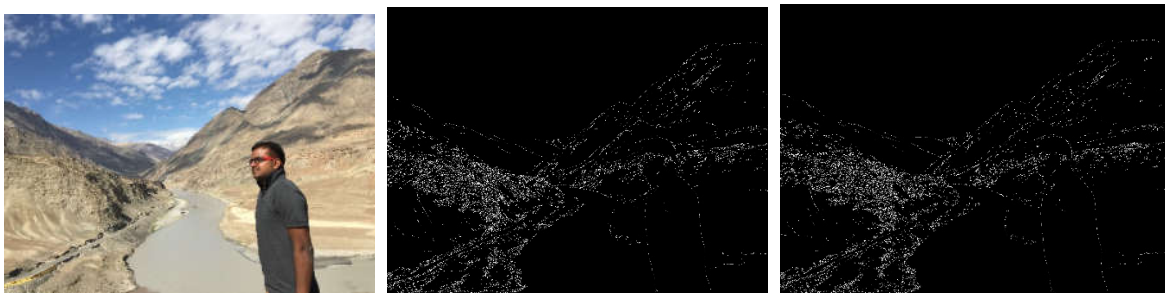
(f)



(g)

(h)

(i)



(j) (k) (l)

Figure. 3. Edge areas of cover image {Baboon (a); Baboon-Hybrid (b); Baboon-Stego (c); Happyfish (d); Happyfish-Hybrid (e); Happyfish-stego (f); Lena (g); Lena-hybrid (h); Lena-stego (i); Mountain(j); Mountain-Hybrid (k); Mountain- stego(l)}

Table 1: PSNR, SSIM, RMSE after embedding secret message

No	Image	RMSE	PSNR	SSIM
1	Happyfish	0.015	48.72	0.99
2	Baboon	0.012	45.5	0.99
3	Mountain	0.015	52.5	0.99
4	Lena	0.015	47.59	0.99

6. Conclusions

In this paper, a new approach for hiding a secret text in digital images is presented. The approach works by concealing the text in the edge area. Inserting message bits in the edge area also serves as an alternative solution to improve the security of message insertion. We have come to the conclusion that these two advantages can be obtained when we apply steganographic techniques. A hybrid edge detection method consisting of combining Canny and Sobel methods. According to the experimental results, it is proven that using the combination of the Canny-Sobel method increases the embedding capacity, more than using these methods separately. Therefore, the payload capacity of messages that can be inserted in the edge area increases. The experiment has also proven that inserting messages on the hybrid edge area with the same payload message is better than the case of the Canny edge area or the Sobel edge area.

References

(1) *Ghosal, S. K., A. Chatterjee, R. Sarkar. Image Steganography Based on Kirsch Edge Detection. – Multimedia Systems, 2020, pp. 1-15.*

(2) *Zhang, H., L. Hu. A Data Hiding Scheme Based on Multidirectional Line Encoding and Integer Wavelet Transform. – Signal Processing: Image Communication, Vol. 78, 2019, pp. 331-344.*

(3) *Hamid, N., et al. Image Steganography Techniques: An Overview. – International Journal of Computer Science and Security (IJCSS), Vol. 6, 2012, No 3, pp. 168-187.*

(4) *Kumar, S., A. Singh, M. Kumar. Information Hiding with Adaptive Steganography Based on Novel Fuzzy Edge Identification. – Defence Technology, Vol. 15, 2019, No 2, pp. 162-169.*

(5) *Alabaichi, Ashwak, M. A. Abid, A. K. Al-Dabbas, A. Salih. Image Steganography Using Least Significant Bit and Secret Map Techniques. – International Journal of Electrical & Computer Engineering, Vol. 10, 2020, No 1 pp. 2088-8708.*

(6) *Kordov, K., B. Stoyanov. Least Significant Bit Steganography Using Hitzl-Zele Chaotic Map. – International Journal of Electronics and Telecommunications, Vol. 63, 2017.*

(7) *I r a w a n, C., C. A. S a r i, E. H. R a c h m a w a n t o. Hiding and Securing Message on Edge Areas of Image Using LSB Steganography and OTP Encryption. – In: Proc of 1st International Conference on Informatics and Computational Sciences (ICICoS'17), IEEE, 2017.*

(8) *T r i p a t h y, S. K., R. S r i v a s t a v a. An Edge-Based Image Steganography Method Using Modulus-3 Strategy and Comparative Analysis. – In: Proc of International Conference on Computer Vision and Image Processing, Singapore, Springer, 2019.*

(9) *B h a r d w a j, S., A. M i t t a l. A Survey on Various Edge Detector Techniques. – Procedia Technology, Vol. 4, 2012, pp. 220-226.*

(10) *Z h a n g, H., L. H u. A Data Hiding Scheme Based on Multidirectional Line Encoding and Integer Wavelet Transform. – Signal Processing: Image Communication, Vol. 78, 2019, pp. 331-344.*

(11) *B a s s i l, Y. Image Steganography Based on a Parameterized Canny Edge Detection Algorithm. – arXiv preprint arXiv:1212.6259, 2012.*

(12) *I s l a m, S., M. R. M o d i, P. G u p t a. Edge-Based Image Steganography. – EURASIP Journal on Information Security, Vol. 2014, 2014, No 1, pp. 1-14.*

(13) *M a i n i, R., H. A g g a r w a l. Study and Comparison of Various Image Edge Detection Techniques. – International Journal of Image Processing (IJIP), Vol. 3, 2009, No 1, pp. 1-11.*

(14) *G a u r a v, K., U. G h a n e k a r. Image Steganography Based on Canny Edge Detection, Dilation Operator and Hybrid Coding. – Journal of Information Security and Applications, Vol. 41, 2018, pp. 41-51.*

(15) *K a d h i m, I. J., et al. Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research. – Neurocomputing, Vol. 335, 2019, pp. 299-326.*

(16) *H a m e e d, M. A., et al. An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques. – IEEE Access, Vol. 7, 2019, pp. 185189-185204.*

(17) *J u m a n t o, J. An Enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel Edge Detection. – Cybernetics and Information Technologies, Vol. 18, 2018, No 2, pp. 74-88.*

(18) *A r o r a, S., S. A n a n d . A Proposed Method for Image Steganography Using Edge Detection. – International Journal of Emerging Technology and Advanced Engineering, Vol. 3, 2013, No 2, pp. 296-297.*

(19) *B a s s i l, Y. Image Steganography Based on a Parameterized Canny Edge Detection Algorithm. – arXiv preprint arXiv:1212.6259, 2012.*

(20) *H e m p s t a l k, K. Hiding Behind Corners: Using Edges in Images for Better Steganography. – In: Proc of Computing Women's Congress, Hamilton, New Zealand. 2006.*

(21) *K a d h i m, I. J., P. P r e m a r a t n e, P. J. V i a l. High Capacity Adaptive Image Steganography with Cover Region Selection Using Dual-Tree Complex Wavelet Transform. – Cognitive Systems Research, Vol. 60, 2020, pp. 20-32.*

(22) *S e t i a d i, D e R o s a l, I. M o s e s. PSNR vs SSIM: Imperceptibility Quality Assessment for Image Steganography. – Multimedia Tools and Applications, 2020.*

(23) *S e t i a d i, D e R o s a l, I. M o s e s. Payload Enhancement on Least Significant Bit Image Steganography Using Edge Area Dilation. – International Journal of Electronics and Telecommunications, Vol. 65, 2019.*

(24) *Naida A.Mohsin.Huda A. Alameen. A Hybrid Method for payload Enhancement in Image steganography Based on Edge Area Detection. Volume 21. No 3.*

(25) *Y a n g, C.-H., C.-Y. W e n g, S.-J. W a n g, H.-M. S u n. Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems. – IEEE Transactions on Information Forensics and Security, Vol. 3, 2008, No 3, pp. 488-497.*

(26) *G a o, W., X. Z h a n g, L. Y a n g, H. L i u. An Improved Sobel Edge Detection. – In: IEEE International Conference on Computer Science and Information Technology (ICCSIT'10), Chengdu, 2010.*