A Comparative Study of Image Steganography Based on Edge Detection

A Comparative Study of Image Steganography Based on Edge Detection

Huda Abdul Wahid Jasim Albayati[1]*, Suhad A. Ali2[2]

[1] Computer Science, College Science for Women, University of Babylon, Iraq.
[2] Computer Science, College Science for Women, University of Babylon, Iraq.

Email: huda.bayati@student.uobabylon.edu.iq

Abstract. Information security has become the main concern of the most famous researchers and the focus of their attention, as they are constantly trying to find the best and safest ways to transfer information through a secure tunnel to protect it from hacking attempts and common attacks on the Internet and in this research, we tried to embody one of the methods of security in protecting data. In this study, a new approach to masking information based on the incorporation of LSB replacement mechanism and edge detection is proposed. To avoid HVS mining when more covert bits are included in pixels, we classify cover pixels into edge regions and non-edge regions. Then, the pixels belonging to the edge region are used to transmit more secret bits. In addition, to increase the load as well as maintain good image quality, we adopt a clever method in which the edge information is identified by the most important bits (MSBs) of the cover image so that it does not need to be stored. At the extraction stage, the same edge information is obtained. Therefore, confidential data can be extracted correctly without confusion. Experimental results prove that our scheme achieves a much higher payload and better optical quality than that of the latest technology.

1. Introduction

Recently, due to advancements in technologies, most people choose to use the internet as the primary means of transferring data from one end to the other all over the world. Transferring data is easy, fast, and accurate using the net.

The "security threat" is one of the foremost problems related to the transmission of information over the net. counseling must be secured so on transfer it, So information security has become an awfully important and really important factor to finish the transfer successfully without compromising it. Information security refers to protecting data from hackers or unauthorized users, and it provides high security to forestall data modification. There are various techniques used for this purpose like encryption and steganography (steganography and digital watermark) to spice up security measures in transmitting information over the net [1].

Information hiding techniques are classified into two sections: steganography and watermarking. Characteristics of the techniques comprise (a) imperceptibility, (b) survivability, (c) capacity, and (d) security. This paper focuses on Steganography, which could be a field

within the domain of knowledge hiding that hides secret information in an undetectable way excepted the sender and intended recipients who have known it, making it the most candidate for hidden communication [2]. In this way used, image hiding information is a technique by which information can be secretly included by hiding through the image. The edges of the images were used to include the secret message so that the effect on the image is less than the embodiment in the direct least important bit The edges represent the most powerful areas in the image; the inclusion in them is not noticeable due to the intensity of the coloration in those areas [3]. In this method used, the last 5 least significant bits (LSB) are scanned and then 3 most significant bits (MSB) are detected, and seven types of edge detection filters are used (Sobel, Prewitt, Kirch, Robert, Laplacian, Fuzzy Logic and Canny). Information is embedding if it is an edge, 4 bits are hidden, and if it is not an edge, 2 bits are embedded [4, 5]. The experimental results were analyzed to clarify the results by some performance metrics; these metrics are Quality metrics (PSNR). The results of the secret message also measured before and after embedding by a metric Normalized Cross-Correlation [6]. The proposed system techniques and existing techniques have been simulated using MATLAB programs. The proposed system and existing techniques applied to hide a secret message (text) inside grayscale.

2. Related Works

This section displays the works that have already been done on steganography utilizing distinctive systems. There are different techniques, which are connected for secret communication of information: In 2019, Dhargupta and et.al. Presented a fuzzy edge detection based steganography approach to effectively hide data within images. The method used a fuzzy edge detection approach in order to estimate more number of pixels where the data can be hidden. At the outset, the cover image is masked and the fuzzy edge detection is performed on the masked image thus retaining edge information. The number of bits to be embedded in a particular pixel is dependent on whether the pixel is an edge pixel, where more bits are embedded. In case the pixel is not an edge pixel and also not a background pixel then the amount of data that is to be embedded depends on the Euclidean distance of the respective pixel from the nearest edge pixel and is determined by the Gaussian function [7].

In 2019, Banik and et.al. Presented data hiding technique in the image using Kirsch operator, which has unique features to find maximum edge strength in different orientations. Depending on a threshold value for the Kirsch operator and the intensity value of each pixel of the cover image, a scale with 3 ranges would be created. This scale is the basis for choosing flexible, i.e., 2, 3, or 4 LSB replacements for stenographic encoding. The threshold value is sharable to the intended receiver as a key [8].

In 2019, Bhardwaj and et.al. The presented stenographic approach that combines edge detection based stenographic techniques with Optimal Pixel Adjustment Process (OPAP). LSB substitution can be further optimized by combining it with edge detection techniques. This is because different regions in the cover image can store different numbers of bits. Complex regions or regions having an edge are less sensitive to change and can hide more data than smooth regions [9].

In 2020, Wang and et.al. Presented a hybrid steganography method based on the least significant bit (LSB) replacement and Hamming code (HLAH). Information security is also increased by using two different steganography methods. Since the sharp areas of the image can tolerate more changes than the smooth areas, more secret messages are embedded in the edge regions of the image and a small amount of information is embedded in the smooth regions [10].

In 2020, Delmi and et.al. Presented steganography, the method is used Least Significant Bit Matching Revisited (LSBMR). Embedding region was on edge digital imagery to ensure

the message was not detected in the image by visual. The method used to detect the edge region by using Canny Edge Detection [11].

In 2020, Prasad and Pal presented to improve the embedding capacity of the cover image, the hiding process of secret message bits is furnished with the help of cover image characteristic, where more number of secret message bits are embedded into the edge-region instead of the smooth region of the cover image. The secret message bits are concealed into the cover image using the modulus function-based embedding process. For improving the security of the content, where embedded the secret message bits into the cover-image with reference of keys, i.e., known as a stego-key. The scheme is implemented on some standard greyscale images [12].

In 2020, Ayub and Selwal presented an improved image steganography technique in which data is embedded in the edge pixels of the carrier image. An intruder has less suspicion about the existence of data bits in edges because edge pixels appear to be different than their neighbors and thus ensures better security. The proposed technique uses different types of edge detection filters like Prewitt, Sobel, Laplacian, and Canny in the existing image steganography using edge-based data hiding in the DCT domain algorithm. The proposed steganography technique results in a reduction of image size mainly because of image compression [13].

3. The Proposed System

The proposed method includes hiding English and Arabic texts in gray images. In this paper, the proposed system consists of two procedures:

- *Embedding procedure (sender side).*
- *Extracting procedure (receiver side).*

The embedding process is done on the sender side. It includes many steps, which depict as follow:

3.1 Embedding procedure (sender side).

3.1.1 Clear pixel

An image is a group of pixels that represent color values, or what is known as the image's density. Each pixel in the image consists of 8 bits, so at this stage clear the five least important bits of each pixel will be by substituting the value zero instead of the value of that bit.

3.1.2 Edge detection

This step is based on the previous stage, where the edge of the top four bits of importance is revealed by using a set of filters for detecting edges, including Sobel, Canny, Robert, Krich, and Prewitt. detect the pixels in the most significant bits image in the previous step as edge pixel by assign the value (1) and non- edge pixel by assigning the value (0). types of edge detection:

3.1.2.1 Sobel Edge Detection

Sobel edge detection is used in image processing techniques. The Sobel kernels are more suitable to detect edges along with the horizontal (180 degrees) and the vertical axis (90 degrees). The Sobel operator is based on convolving the image with a small separable, and integer-valued filter [4]. Sobel masks are given as in Figure1 [14]:

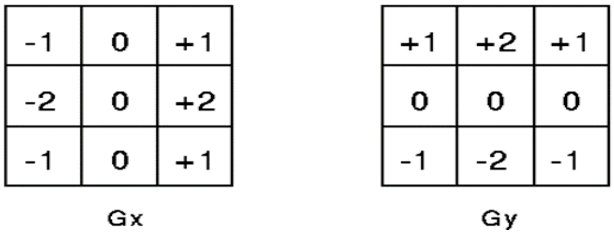


Figure1. Sobel edge detection masks.

3.1.2.2 Prewitt Edge Detection

This operator is like Sobel but with different coefficients of the mask[15]. The Prewitt edge detector is an appropriate way to estimate the magnitude and orientation of an edge. Prewitt masks are given as in Figure 2 [14]:

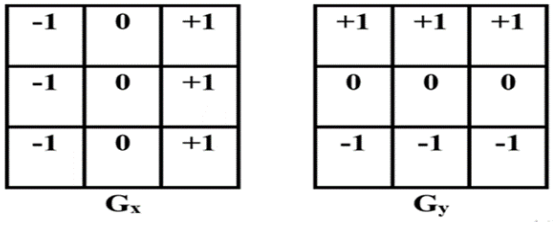


Figure 2. Prewitt edge detection masks

3.1.2.3 Robert Edge Detection

Robert Roberts locates the edges very precisely but cannot eliminate noise. Edges appear when brightness varies and have complex shapes[16]. The mask Roberts is defined as the following Figure 3.

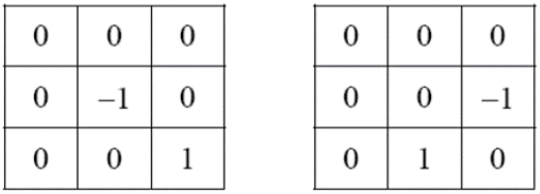


Figure 3. The Roberts operators.

3.1.2.4 Kirch Edge Detection

Kirsch proposed an edge-detection method which finds all eight edge responses in the pre-determined directions such as East (E), South East (SE), South (S), South West (SW), West (W), North West (NW), North (N) and North East (NE). This algorithm takes each kernel mask and rotates in 45 degrees and increments through all 8 compass directions.

The edge response is calculated as the maximum magnitude across all directions for each pixel of an image to make convolution. The following eight masks are used to calculate kirsch edge responses in Figure 4[17].

$$\underset{k_0}{E=\begin{bmatrix}-3&-3&5\\-3&0&5\\-3&-3&5\end{bmatrix}}\quad \underset{k_1}{NE=\begin{bmatrix}-3&5&5\\-3&0&5\\-3&-3&-3\end{bmatrix}}\quad \underset{k_2}{N=\begin{bmatrix}5&5&5\\-3&0&-3\\-3&-3&-3\end{bmatrix}}\quad \underset{k_3}{NW=\begin{bmatrix}5&5&-3\\5&0&-3\\-3&-3&-3\end{bmatrix}}$$

$$\underset{k_4}{W=\begin{bmatrix}5&-3&-3\\5&0&-3\\5&-3&-3\end{bmatrix}}\quad \underset{k_5}{SW=\begin{bmatrix}-3&-3&-3\\5&0&-3\\5&5&-3\end{bmatrix}}\quad \underset{k_6}{S=\begin{bmatrix}-3&-3&-3\\-3&0&-3\\5&5&5\end{bmatrix}}\quad \underset{k_7}{SE=\begin{bmatrix}-3&-3&5\\-3&0&5\\-3&5&5\end{bmatrix}}$$

Figure 4. Kirsch masks.

3.1.2.5 Laplacian Edge Detection

The Log of an image f(x,y) is a second-order derivative, the Laplacian edge detector measures the derivative of a 2D function [16]. It has two effects, it smoothes the image and it computes the Laplacian, which yields a double-edge image. Locating edges then consists of finding the zero crossings between the double edges. The digital implementation of the Laplacian function is usually made through the mask below in 'Figure 5 [18]**:**

0	-1	0
-1	4	-1
0	-1	0

G_x

-1	-1	-1
-1	8	-1
-1	-1	-1

G_y

Figure 5. Mask Laplacian.

3.1.2.6 Canny Edge Detection

In image processing since its development, Canny Edge Detection is one of the standard edge detection technologies. and it still outperforms many modern algorithms that have been developed[3]. To find edges by separating noise from the image before finding the edges of the image, Canny is a very important way. The Canny method is a better method without disturbing the edge features in the image then the direction is applied to find the edges and the dangerous value of the threshold [18].

3.1.2.7 Fuzzy logic Edge Detection

In order to accomplish the method of image processing by fuzzy logic. It can define fuzzy image processing as the whole assemblage of all methods that apprehend, represent, and process the images, their segments, and features as fuzzy sets. The most important steps on the fuzzy image processing; represent and processing depends on the selected fuzzy technique and on the problem to be solved [5].

4. Methodology

4.1. Mean Square Error (MSE)

The average of the squares of the "errors" is measured by the mean squared error of an estimator i.e. the difference between the estimator and what is estimated. The contrast happen due to randomness or as a result of the estimator doesn't calculate information that could result in a better accurate estimate. The PSNR differ inversely with the MSE. The M.S.E can be found from the following Equation (1) [14]:

$$\mathrm{MSE} = \frac{1}{\mathrm{mn}} \Sigma_{1=0}^{\mathrm{m}-1} \Sigma_{\mathrm{j}=0}^{\mathrm{n}-1} \left(\mathrm{p}_1(\mathrm{i},\mathrm{j}) - \mathrm{p}_2(\mathrm{i},\mathrm{j})\right)^2 \qquad (1)$$

4.2 Peak signal to noise ratio

The ratio between the power of corrupting noise and the most possible power of a signal that influences the sincerity of its representation is PSNR. Here, PSNR cites the ratio between the edge detected images i.e. the estimator output and the ground truth image which is also said to be the estimated image. PSNR can be rated by the following Equation (2) [14]:

$$\mathrm{PSNR} = 20 \cdot \log_{10}\left(\frac{\max i}{\sqrt{\mathrm{MSE}}}\right) \qquad (2)$$

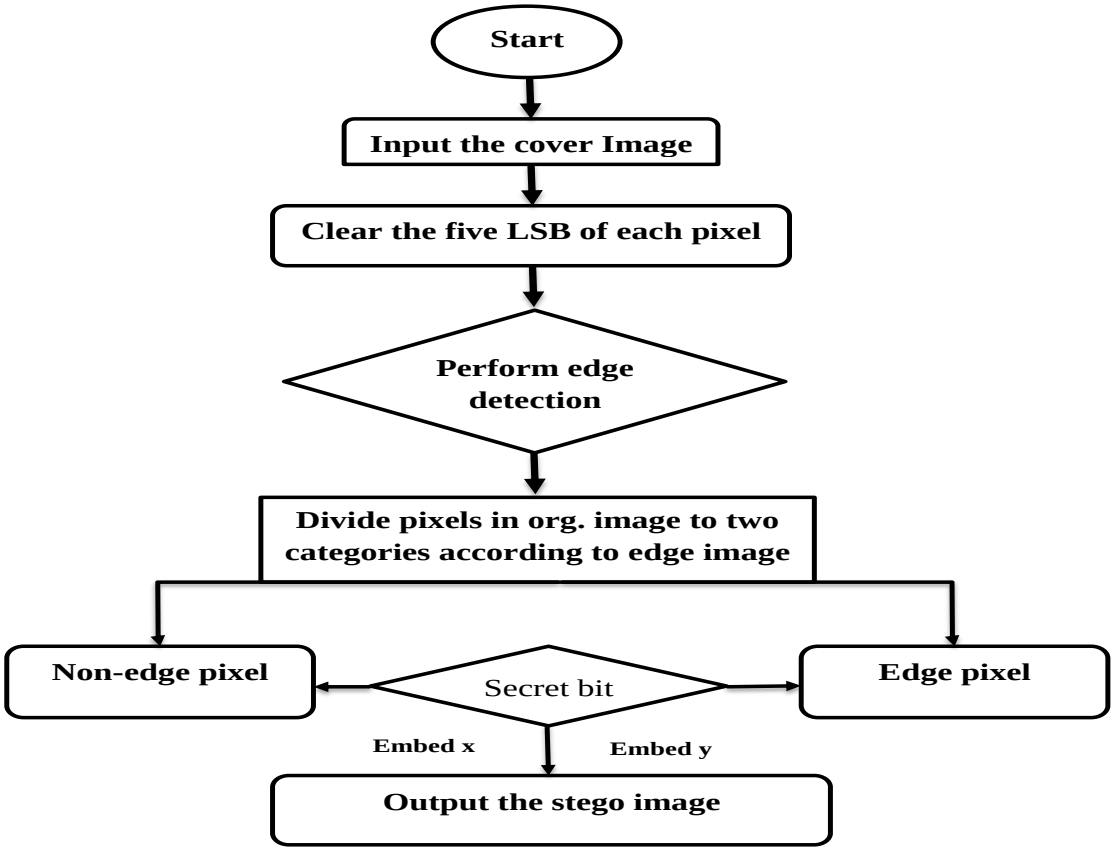


Figure 6. The flowchart of the proposed embedding phase.

4.3 Embedding process

Depending on the previous stage, the cover image original pixels are categorized into two categories, non-edge pixels, and edge pixels, respectively. Where x and y are used, where x means the number of secret bits to be included in non-edge pixels and corresponding y means the number of secret bits that will be included in edge pixels.

The embedding Procedure

input : I Cover Image

x number of bits that can be hidden in one pixel if it is not an edge.

y number of bits that can be hidden in one pixel if it is an edge.

S secret text message

output: EI Embedded Image.

Begin

Step 1. read the cover mage

Step 2. read the text to be hidden (message).

Step 3. Enter a value (process number) representing the filter selection used for edge detection. There are seven types of edge detection filters (Sobel, Prewitt, Kirch, Robert, Laplacian, fuzzy logic and Canny)

Step 4. Next, the edge reveals the five least significant bits of each pixel according to the specific filter type, i.e. if we enter zero (process number) zero, the edge is detected using the Sobel filter and if we enter 1, the edge is with the Prewitt filter and if 2 Kirch and if 3 Robert 4 If Laplacian 5 if Fuzzy Logic 6 If If Canny.

Step 5. Convert text to bits. Then we compare each pixel in the original image with a pixel that corresponds to it in the Edge Detection image. If the pixel is an edge, the bits will be hidden by the number y, and if the edge is not we hide the number x.

Step 6. Apply the PSNR scale between the original image and the image after hiding to find the similarity between the two images:

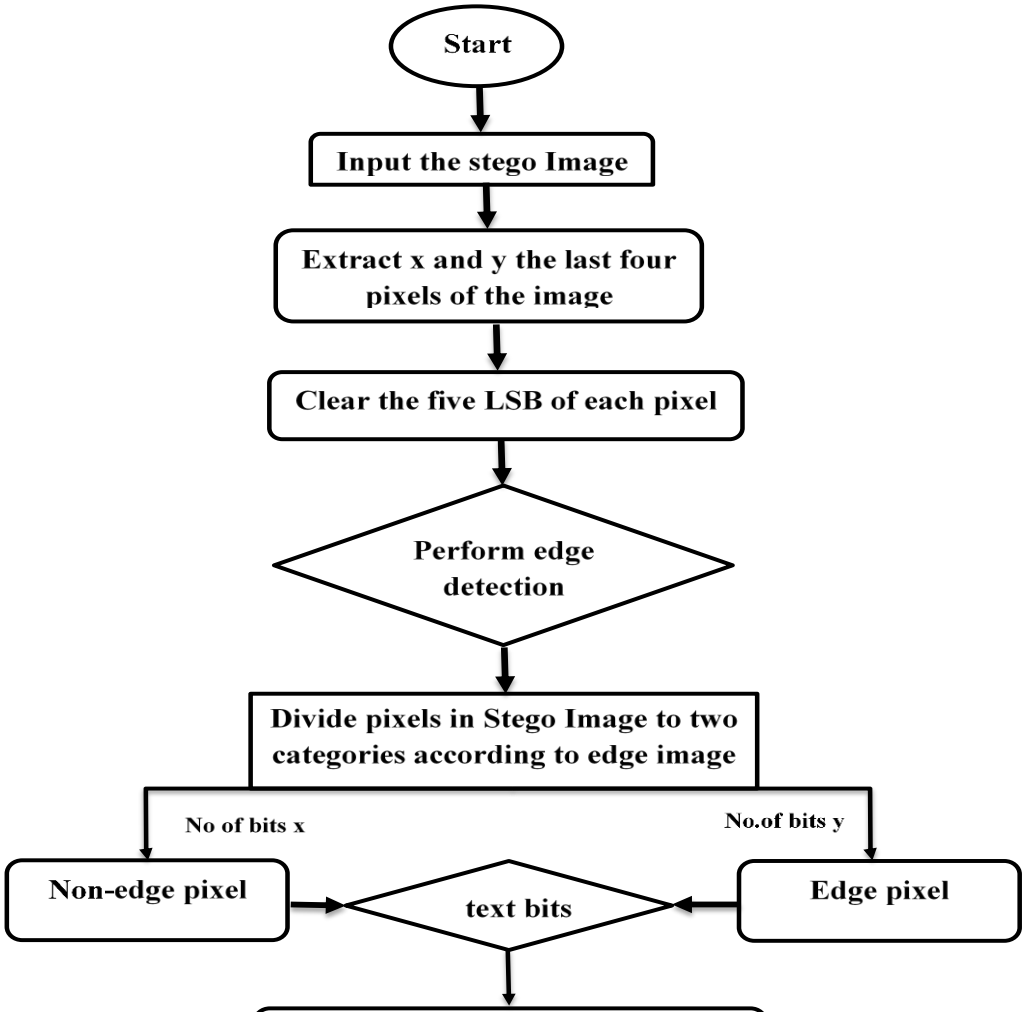
$$MSE = \sum_{i=1}^{M}\sum_{j=1}^{N}\left(I(i,j) - C(i,j)\right)^2 \Big/ M * N$$

$$PSNR = 10\, log10\, (255^{\,2} / MSE)$$

End

4.4 Extracting procedure (receiver side).

The embedded image will go through the clear pixel stage and edge detection stage. In the extraction phase, the receiver first extracts the two parameters x and y from the pixels of the image. Also, the edge information is determined the same as in the embedding phase. Therefore, the secret data will be extracted exactly. Figure7 shows the extraction process.



Figuer 7. The flowchart of the proposed extraction phase

The extracting procedure

Input: EI Embedded Image.

Output: ES Extract The Message.

Begin

Step 1. Enter a value (process number) representing the filter selection used for edge detection. There are seven types of edge detection filters (Sobel, Prewitt, Kirch, Robert, Laplacian, fuzzy logic and Canny)

Step 2. Next, the edge reveals the five least significant bits of each pixel according to the specific filter type, i.e. if we enter zero (process number) zero, the edge is detected using the Sobel filter and if we enter 1, the edge is with the Prewitt filter and if 2 Kirch and if 3 Robert 4 If Laplacian 5 if Fuzzy Logic 6 If If Canny.

Step3. Extract x secret bits from non-edge pixels and y from edge pixels.

Step4. Convert the extracted bits into text and save in the (ES)

Step 5. find similarities between the original text and the extracted text by using NC according to the following equation:

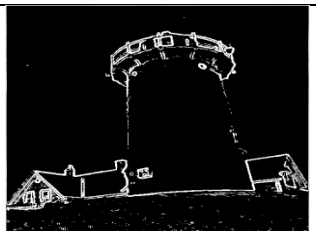
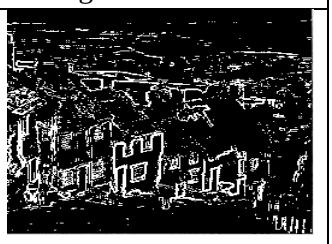
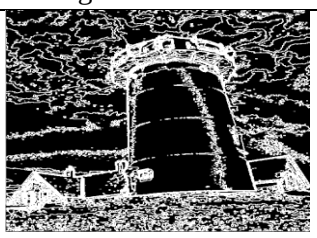
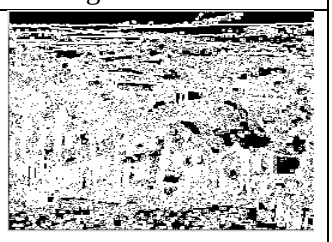
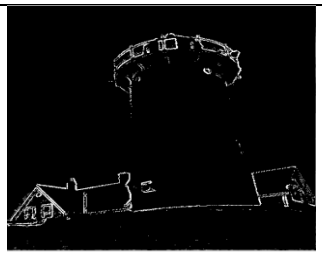
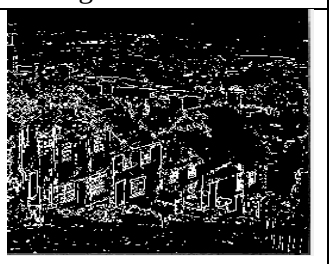
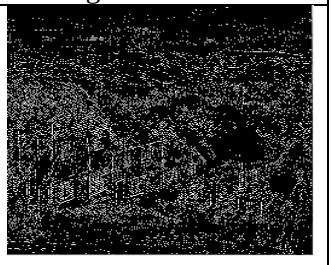
$$\text{Normalized Cross Correlation} = \frac{\sum A * B}{\sqrt{\sum A^2 * \sum B^2}}$$

End

5. The Experimental Results

The proposed algorithm implemented with many gray scale images to test the algorithm performance, the performance measured by using PSNR. In this part, we will explain the results of applying the proposed algorithm in masking English and Arabic texts.

Edge detection	I_{org}			

	I_{clear} 5bit			
Sobel	Edge image of I_{clear}	 Edge count= 67579	 Edge count= 32814	 Edge count= 15898
prwitt	Edge image of I_{clear}	 Edge count= 39421	 Edge count= 13587	 Edge count= 8812
Kirch	Edge image of I_{clear}	 Edge count= 145992	 Edge count= 86743	 Edge count= 46083
Robert	Edge image of I_{clear}	 Edge count= 3014	 Edge count= 5765	 Edge count= 8679
Laplacian	Edge image of I_{clear}	 Edge detection= 5722	 Edge count= 3397	 Edge count= 7900

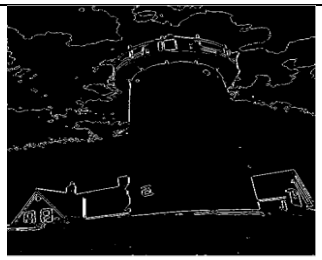
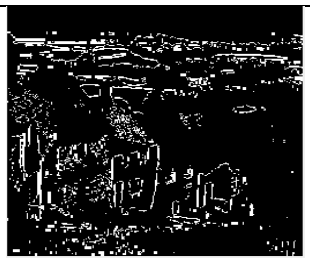
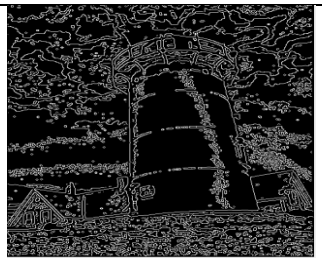
Fuzzy Logic	Edge image of I_{clear}	 Edge detection= 1011	 Edge detection= 9900	 Edge count= 5766
Canny	Edge image of I_{clear}	 Edge detection= 22259	 Edge count= 9711	 Edge count= 7727

Figure 8 . The number of edge pixels detected by Sobel, Prwitt, Krich, Robert, Laplacian and Fuzzy logic and Canny operators with set images.

Figure 8 shows the original image and the edge detection of the image after scanning the five least important bits. The filters used were applied and the number of edges was calculated for each image. There are clear differences between the edge detection filters, some of which show the smallest details in the image as an edge, and some of them are limited to the clear objects in the image. The greater the number of edges in the image, the better the more data is included in the image.

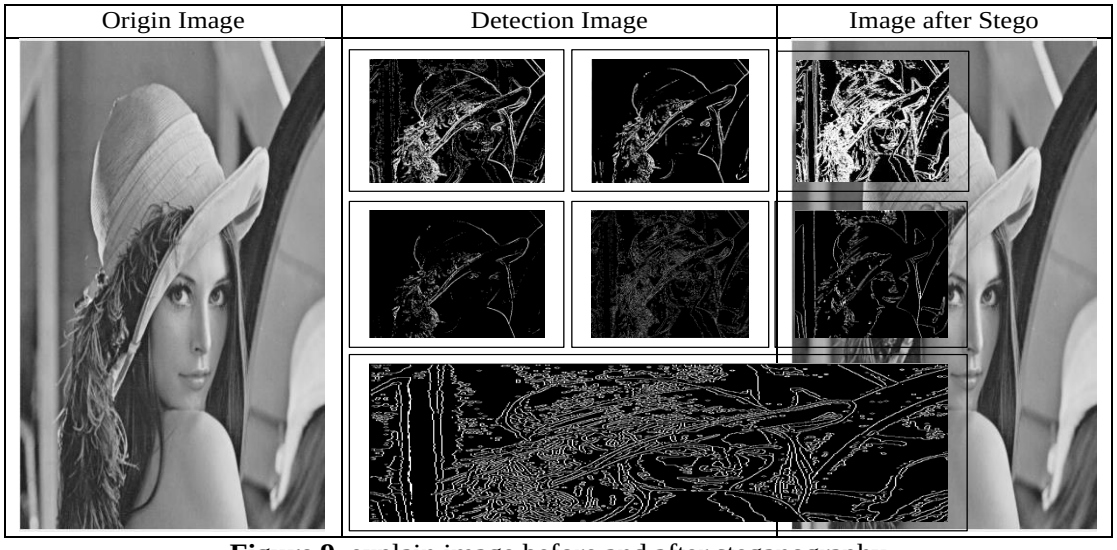


Figure 9. explain image before and after steganography

Figure 9 shows the application of the proposed method on the image of Lena, where the English text was included, "Iraq is a country of civilizations and glories". The PSNR scale found to measure the similarity between the images before and after the inclusion, as well as the NC

scale, which measures the percentage of similarity between the original and the text after extraction as shown in the table 1.

Table 1. Experimental results of the proposed scheme using various values of x and y on 'Lena' image size of 512*512

Edge detection		**Sobel**		**Prwitt**		**Krich**		**Robert**		**Laplacian**		**Fuzzy Canny**	
Schemes													
x	**y**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**
1	2	80.149	1	80.149	1	80.149	1	80.149	1	80.149	1	80.149	1
80.149	1												
1	3	80.149	1	80.149	1	80.149	1	80.149	1	80.149	1	80.149	1
80.149	1												
1	4	80.149	1	80.149	1	80.149	1	80.149	1	80.149	1	80.149	1
80.149	1												
2	3	76.835	1	76.835	1	76.835	1	76.835	1	76.835	1	76.835	1
76.835	1												
2	4	76.835	1	76.835	1	76.835	1	76.835	1	76.835	1	76.835	1
76.835	1												
3	4	71.447	1	71.447	1	71.447	1	71.447	1	71.447	1	71.447	1
71.447	1												

Table 2 shows the scales results for the Arabic text "العراق بلد الحضارات والامجاد".

Table 2. Experimental results of the proposed scheme using various values of x and y on 'Lena' image size of 512*512

Edge detection		**Sobel**		**Prwitt**		**Krich**		**Robert**		**Laplacian**		**Fuzzy Canny**	
Schemes													
x	**y**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**
1	2	83.429	1	83.429	1	83.429	1	83.429	1	83.429	1	83.429	1
83.429	1												
1	3	83.429	1	83.429	1	83.429	1	83.429	1	83.429	1	83.429	1
83.429	1												
1	4	83.429	1	83.429	1	83.429	1	83.429	1	83.429	1	83.429	1
83.429	1												
2	3	78.639	1	78.639	1	78.639	1	78.639	1	78.639	1	78.639	1
78.639	1												
2	4	78.639	1	78.639	1	78.639	1	78.639	1	78.639	1	78.639	1
78.639	1												
3	4	72.885	1	72.885	1	72.885	1	72.885	1	72.885	1	72.885	1
72.885	1												

Figure 10 the following text "A word is enough to the wise" was included, and the results were as follows:

Filters	Origin image	Stego image	PSNR
Sobel			**79.4788**
Prewitt			**79.4788**
Kirch			**79.4788**
Robert			**79.4788**
Laplacian			**79.4788**
Fuzzy Logic			**79.4788**

Canny			**79.4788**

Figure 10. explain image before and after steganography

6. Conclusion

In a suggested method for the implementation of the steganography process, we notice that the peak noise signal (PSNR) is the best estimate of the optimization efficiency, the higher the PSNR quality, the stego image is very close to the original image. One of the suggested methods for detecting edges is that the best way to detect the edge is the canny method because it applies the direction to find the edges and the dangerous value of the threshold and includes criteria. In addition, that a certain edge of the image should be distinguished only once and the noise should not produce any false edges. An image with many objects is much better than an image with few objects. Embedding capacity becomes larger because can generate more pixel edges than simple images.

References

[1] N. koduri, "Information security through image steganography using least significant bit algorithm," Master Thesis, Information Security and Computer Forensics University of East London, 2011.

[2] M. Bilal , S. Imtiaz , W. Abdul , S. Ghouzali , and S. Asif, "Chaos based Zero-steganography algorithm," Multimedia tools and applications, vol. 72, No. 2, pp. 1073-1092, 2014.

[3] Deepak Mathur, Dr. Prabhat Mathur "EDGE DETECTION TECHNIQUES IN IMAGE PROCESSING WITH ELABORATIVE APPROACH TOWARDS CANNY" Computer Science Department, LACHOO MEMORIAL COLLEGE OF SCIENCE & TECHNOLOGY,2016.

[4] Dr. A. K. Saxena "Edge Detection Operators on Digital Image" , SRCEM, Banmore(M.P.), India,2013.

[5] Abdulrahman Moffaq Alawad, Farah Diyana Abdul Rahman, Othman O. Khalifa,Norun Abdul Malek "Fuzzy Logic based Edge Detection Method for Image Processing", Faculity of Electrical and Computer Engineering, International Islamic University Malaysia, Malaysia, Department of Electrical and Computer Engineering, International Islamic University Malaysia, Malaysia ,2018.

[6] Naga Ranjith Kumar Kesa thesis “Steganography A Data Hiding Technique”, Master of Science in Information Assurance & St. Cloud State University 12-2018.

[7] Dhargupta, S., Chakraborty, A., Ghosal, S. K., Saha, S., & Sarkar, R. "Fuzzy edge detection based steganography using modified Gaussian distribution". Multimedia Tools and Applications, 78(13), 17589-17606, 2019.

[8] Banik, B. G., Poddar, M. K., & Bandyopadhyay, S. K. "Image Steganography Using Edge Detection by Kirsch Operator and Flexible Replacement Technique". In Emerging Technologies in Data Mining and Information Security (pp. 175-187). Springer, Singapore, 2019.

[9] Bhardwaj, M., Singh, L., & Saini, K. K. "An Efficient Approach to Information Hiding through Image Steganography using Edge Detection". In 2019 4th International Conference on Information Systems and Computer Networks (ISCON) (pp. 564-571). IEEE, November 2019.

[10] Wang, Y., Tang, M., & Wang, Z." High-capacity adaptive steganography based on LSB and Hamming code". Optik, 164685, 2020.

[11] Delmi, A., Suryadi, S., & Satria, Y. "Digital image steganography by using edge adaptive based chaos cryptography". In Journal of Physics: Conference Series (Vol. 1442, No. 1, p. 012041). IOP Publishing, January 2020.

[12] Prasad, S., & Pal, A. K."Stego-key-based image steganography scheme using edge detector and modulus function". International Journal of Computational Vision and Robotics, 10(3), 223-24, 2020.

[13] Ayub, N, & Selwal, A."An improved image steganography technique using edge-based data hiding in DCT domain". Journal of Interdisciplinary Mathematics, 23(2), 357-366, 2020.

[14] Ahmed Shihab "COMPARATIVE STUDY AMONG SOBEL, PREWITT AND CANNY EDGE DETECTION OPERATORS USED IN IMAGE PROCESSING", University of Baghdad College of Nursing, October 2018.

[15] Sujeet Das "Comparison of Various Edge Detection Technique".International Journal of Signal Processing, Image Processing, and Pattern Recognition Vol.9, No.2, 2016.

[16] Yuanxi Fu. "Automatic License Plate Recognition UsingNeural Network and Signal Processing "A Thesis submitted in partial satisfaction of the requirements for the degree of Master of Science in Electrical Engineering, UNIVERSITY OF CALIFORNIA RIVERSIDE, March 2019.

[17] Sivaiah Bellamkonda, N. P. Gopalan. "Facial Expression Recognition using Kirsch Edge Detection, LBP and Gabor Wavelets", Department of Computer Applications National Institute of Technology, Tiruchirappalli Tamil Nadu, India,2018.

[18] Muthukrishnan R. "Edge Detection Techniques For Image Segmentation", Bharathiar University,2011.