

# Payload and quality augmentation using steganographic optimization technique based on edge detection

Mafaz Alanezi, Iman Subhi Mohammed Altaay, Saja Younis Hamid Malla'alo

Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, Iraq

## Article Info

### Article history:

Received Oct 18, 2020

Revised Jun 7, 2021

Accepted Jun 14, 2021

### Keywords:

Cover image  
Edge detection  
Payload  
Steganographic  
Stego image  
Quality

## ABSTRACT

Information security is one of the most significant processes that must be taken into account when confidentially transferring information. This paper introduces a steganography technique using the edge detection method. It focused on three basic and important aspects' payload, quality, and security. Well-known edge detectors were used to generate as many edge pixels as possible to hide data and achieve the highest payload. The least significant bit (LSB) algorithm has been improved by extending the bits used to embed between 2-4 bits in smooth and sharp areas. To increase security, the transaction between the two parties is based on dividing the key and the cover image into several parts and agreeing on the type of edge detection. The experiments achieved the maximum load, for instance with a fuzzy edge detector, at first, embedding in 4 bitplanes if edge pixel, and in 2 bitplanes if non-edge pixel, the peak signal-to-noise ratio (PSNR) increased from 43.580 to 45.790. At second, embedding in 2 bitplanes if edge pixel, and in 4 bitplanes if non-edge pixel, the PSNR decreased between 38.433-41.593. The suggested scheme achieved a high payload to embed in the cover image and according to human perception, it preserved the nature of the original image.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Mafaz Alanezi  
Department of Computer Science  
College of Computer Science and Mathematics  
University of Mosul, Iraq  
Email: mafazmhalanezi@uomosul.edu.iq

## 1. INTRODUCTION

In today's world and in the time of coronavirus disease 2019 (COVID-19), full electronic communication has become a lifeline to continue work, education, research activities, and other important life requirements. Therefore, data is transferred from one party to another using various applications such as email, social media, and others. It has become increasingly important to protect our private information from misuse by attackers. The process of exchanging confidential and important information over networks is a great motivation for researchers interested in finding an approach to create a secure path for this information away from spying and penetration. In this sense, various encryption algorithms have been created to convert this information into unreadable data during the transmission process over networks. With the development of encrypt reverse engineering methods and encrypt analysis, weaknesses have arisen in these encryption algorithms, and it has become possible to penetrate, return, and read encrypted data. That is why these methods have lost their privacy and security to some extent. This prompted the researchers to search for other methods to obtain more confidentiality. Therefore, methods have been used to hide information in digital media that can be an image, video, or text without affecting the quality of these media and in a way that does not cause network hackers to suspect the existence of this information within them, thus ensuring that the network does not intercept and penetrate this data. This is called Steganography technology [1], [2].

There are many algorithms used in steganography. One of the simplest and most common of these methods is the LSB method, which depends on the inclusion of every bit of the message in the least significant bit of each plain pixel in the image [3]. The least significant bit method hides information by embedding it in the cover image bits sequentially, making it easier for an attacker to get a secret message when it intercepts. To increase the complexity and safety of this method, it can be combined with the edge detection algorithm to place the message in the image depending on the edge, so the message is randomly distributed. This gives additional security for the hide operation as well as increased storage capacity [4], [5]. In addition to confidentiality, there is another important condition that, if fulfilled, makes the concealment scheme successful. This condition is an increased capacity without side effects. This condition has become a research challenge that has taken multiple forms to show many proven and quality algorithms. One way to increase your load is to use edge detection on the cover photo [6], [7]. This is because the edge region tolerates changes in pixel values and messages can be combined with a greater capacity than smooth space. Edge detection with various edge detectors like canny, sobel, and prewitt. Also, hybrid detectors can be used to increase the area of the edge region, thereby increasing the message load that will be included in it [8], [9].

In this work, we depend on image steganography, which uses images as the cover file to hide the secret message because they contain a lot of redundancy, and redundancy information is the bits of an object that provide accuracy far greater than necessary for the object's use and display, the benefit of these bits is that they can be altered without the alteration being detected easily [7]. The portable network graphics (PNG) format was used for grayscale and coloured images, as this format was specially designed for transferring images over the internet, PNG also supports indexed color, grayscale and red, green, and blue (RGB), in addition to it supports color palette-based images from RGB images of 24-bit or red, green, blue, and alpha (RGBA) 32-bit. Non-color plate-based, grayscale, and full-color RGB images [10]. We have also worked on a combination of LSB substitution and edge detection mechanisms, some of which are based on a single derivative such as robert, sobel, prewitt, and canny, or a second derivative such as laplacian of gaussian (LOG). In addition to the fuzzy logic that increases edge expansion, a hybrid detector has also been used. The diversity of the reagents used aims to create a larger incorporation area. A comparison has been made to choose the best approach for achieving high quality based on PSNR, mean square error (MSE), and bits per pixel (BPP) quality metrics. Color images in the work were chosen to increase capacity and embedding in 24-bit rather than 8-bit as in grayscale images. The strength in the proposed system comes from achieving high secrecy using a key split into several parts. In a gray image, the cover image is split into blocks and the arrangement of these blocks is the first part of the key. Also, the text is divided into blocks and the arrangement of these blocks is the other part of the key. As for the colored images, the key has been divided into three parts, meaning there is the third part in addition to the two parts of the key used in gray images, which is dividing the text into three parts, and each section is the size of the cover image. The key is used for text retrieval when the decoding is blind. The remainder of the paper has been organized as the following: Section 2 contains a brief description of the previous studies and highlights the strengths and weaknesses of each. Section 3 presents the proposed work in all its details, and Section 4 discusses the results. In Section 5 the conclusions are included.

## 2. RELATED WORKS

Jain *et al.* [11] introduced a new method for hiding data in an image, based on the dark areas detected by the edge detector in the image, and including encoded text in the least significant bit. The strength of this approach comes from using grayscale with edge detection and embedding using the LSB method combined with random embedded leads to high confidentiality and creates an embedding image just like the original image. Arora and Anand [12] used a spatial domain technique for image steganography system to conceal the text into the color images using the edge detection way, edges of an image are detected by scanning using a 3×3 window, after that the edge pixels was randomizing by using sorting method, finally, the blue component of sorted edge pixels encoded the text. A novel channel-dependent payload partition strategy based on amplifying channel modification probabilities by Liao *et al.* [13] is proposed, to adaptive assign the embedding capacity among RGB channels. A compression-based steganography idea was proposed by Carpentieri *et al.* [14] that depended on algorithms and parameters used to create and maintain the compressed archive exploited, in addition to the hierarchical compressed archive structure itself, so that secret information is not semantically related to the contents of that compressed archive. Alam *et al.* [15] proposed a new scheme relies on using a secret key that generates random numbers using the chaotic logistic map for random compensation LSB depending on the edge pixels in the cover image, the edge detector canny was applied to get the edge image from the gray image, after that the image was divided into a set of blocks each one of size n pixels and the first bit holds the status of other pixels 1 or 2 bits are included when the pixel is non-edge if the pixels is the edge pixel, the 1-4 pixels will place and the number of built-in bits is

taken randomly by chaotic map. Banik and Bandyopadhyay [16] suggested an innovative steganography way which is a preprocessed cover image by edge detection algorithm that used sobel operator as an edge detection mask, then a secret message is embedded with a technique of multiple bits' modification which is based on classic LSB modification where the least 1<sup>st</sup> bit 2<sup>nd</sup> bit, 3<sup>rd</sup> bit 4<sup>th</sup> bit and 5<sup>th</sup> bit of edge have been changed. Parah *et al.* [17] adopted a new method to hide the data in the color images by dividing the image into three red, green, and blue plants, and using a composite edge detector represented by a prewitt, and canny detector to categorize the image pixels into edge pixels and non-edge pixels, and the method used green and blue plants to include secret data while leaving the red plane to use as an indication of the state of pixels whether it is an edge or not, the text has been divided into four blocks and encoding data with the rivest cipher 4 (RC4) algorithm to increase confidentiality and multiple bits are included in edge pixels while within one bit in a pixel that does not belong to the edge, the method has proven its efficiency by comparing its experimental results with other studies. Kaur *et al.* [6] proposed a hybrid approach which is a combination of different techniques such as RSA for secret message encryption, canny for edge detection, matching, and 4 LSB replacement for the embedded process, in which a text message was hidden inside in all layers of RGB color frames of video, to accomplish high-capacity data and high-quality of stego video based on the quality metrics PSNR, MSE and bit error rate (BER). Vanmathi and Prabu [18] introduced a technology that hides information that uses fuzzy edge detection, chaotic encryption, and a less important bit-over method. This method allows the inclusion of more confidential data that provides more security, giving the system a clear increase in the proportion of PSNR from 5% to 9% max. Gaurav and Ghanekar [19] introduced an algorithm to hide information using the canny method for defining the edges and morphological processes to optimize images based on MSB and using the XOR exclusive separation technique and accomplished that the average PSNR is close to 44 and that SSIM is 0.998 at an established space of 1.25 BPP. Setiadi [8] suggested a method that focuses on increasing the payload by including the text in the areas of the extended edge, and by encoding the data by XOR operations on the text with MSB and using the LSB method in embedding, the beginning is to include the text in the edge pixels as a higher priority and if the text has a rest it is included in the smooth areas The strength of this paper comes from the edge scaling process, which increased the payload by 18.65% while maintaining the stego image quality.

**3. THE SUGGESTED WORK**

In this paper, edge detection processes were applied to hide a large amount of text in the image by the embedding process, and we suggested using “Lena”, “Fruits”, “Cat” and “Sails” images as the cover image in the embedding process, as they are standard test images it is widely used in the field of image processing. Various edge detectors have been used such as sobel, prewitt, roberts, log, fuzzy logic, canny, hybrid, dilate hybrid (5×5) and dilate hybrid edge detector (10×10). Steganography is applied in both gray and color images, to compare results and demonstrate the maximum quality and payload obtained. The flowchart in Figure 1 represents a general outline of how the steganography works.

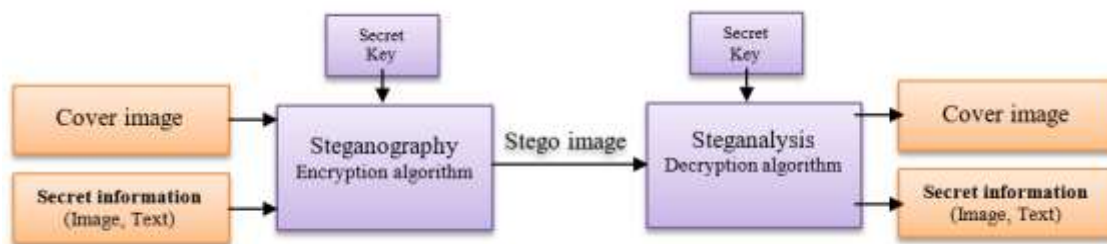






















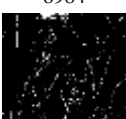

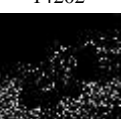
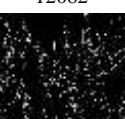
















Figure 1. The flowchart of a general outline of how the steganography works

**3.1. Edge detectors**

Edges are commonly termed as local features since they carried a lot of information about different parts in the image and detected from the sudden change in the gray level, more ever it regarded the border between the different parts in the image, because it separates between two distinctly different parts, whereas edge detectors compute the gradient magnitude following to a formula that differs from the detector to other, some of them based on a single derivative like robert, sobel, prewitt, and canny, while other was used the second derivative as laplacian of gaussian (LOG), if the magnitude of the gradient is higher than a threshold then the edge is existence [20]. Fuzzy logic depends on the subjugation of an image window of pixels to set

fuzzy terms that highlighting all edges related to an image, as instrumental fuzzy terms to detect the relative pixels' values which can point to edge presence [21]. Another type of edge detector was a hybrid detector which is a combination of mixed detectors using OR operators between them, in Table 1 the edge detectors used in the suggested scheme are listed with the number of edge pixels detected.

Table 1. The number of edge pixels detected by Sobel, Roberts, Prewitt, LOG, Canny, Fuzzy Logic, Hybrid and Dilate Hybrid for gray images: 'Lena', 'Fruits', 'Cat' and 'Sails'

	Cover Images			
Edge Detection				
Sobel Edge Detector				
	8055	6126	10882	11658
Roberts Edge Detector				
	7785	6000	7915	8940
Prewitt Edge Detector				
	7995	6034	10907	11586
LOG Edge Detector				
	8984	8210	14202	12082
Fuzzy Logic Edge Detector				
	11378	2541	21925	16846
Canny Edge Detector				
	22438	24319	35000	41817
Hybrid Edge Detector				
	39281	32611	61499	61011
Dilate Hybrid Edge Detector (5×5)				
	98973	85438	119408	145152
Dilate Hybrid Edge Detector (10×10)				
	127381	117976	149445	180213

**3.2. The Stegaraphic method in gray**

First, the original cover image is divided into 64×64 blocks, these blocks are sorted based on the edges' information extracted from applying edge detection on the original cover image, the image's blocks order is the first part of the key. Second, we divided the text into blocks suitable to the image block's size, and then these blocks are sorted according to their data, here the text blocks order considers the second part of the key. In addition to the key, the selected edge detection type is in the deal between the two parties. The text was embedded in 4 bitplanes if edge pixel, and in 2 bitplanes if non-edge pixel, see the flowchart in Figure 2.

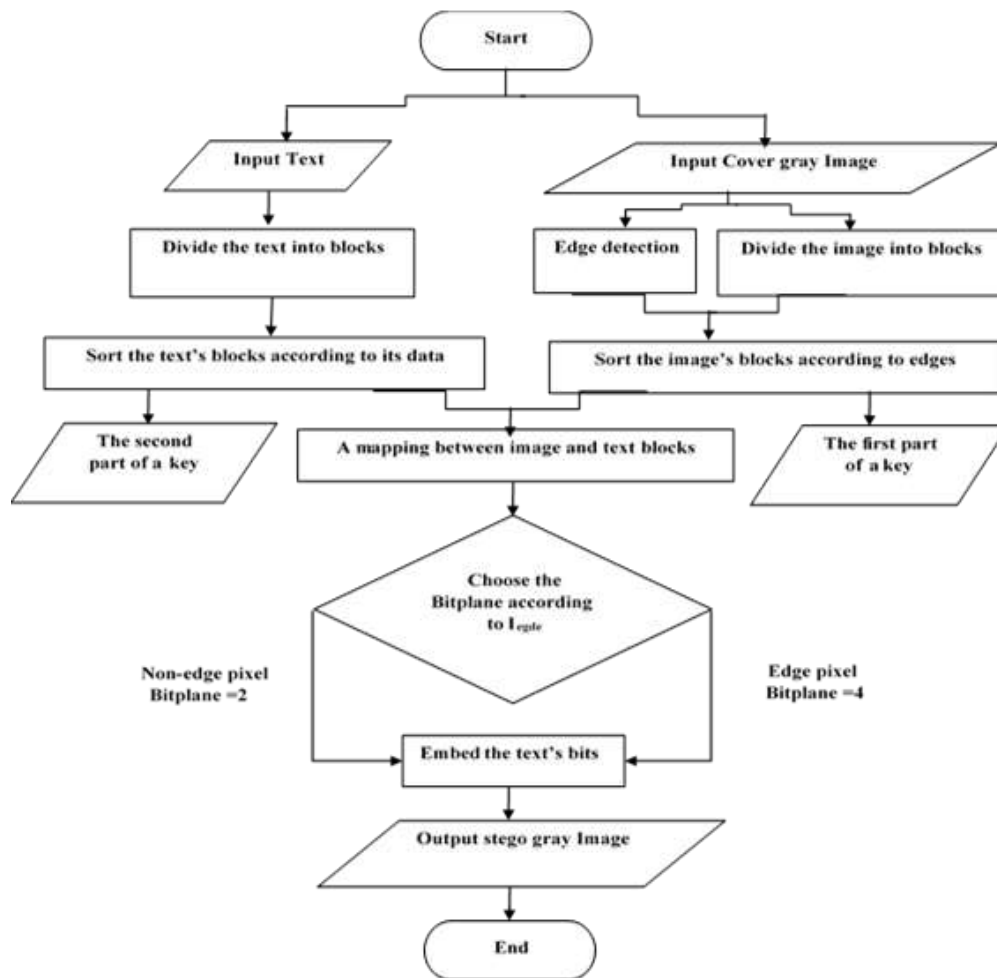


Figure 2. The flowchart of the suggested embedding phase in the gray image

**3.3. The steganographic method in color images**

To hide text in a colored image, first divide the text into three parts, each part of them is treated as a gray image and each part's size as the cover image's size, which is the first part of the key, also separate the cover image into three images Y, Cb, and Cr, so that each part of the text will be embedded in one of these three images. The process of embedding is as follows for the image and text part:

- Determine the edge detection type between the two parties.
- Divide the original cover image into 64×64 blocks, sort these blocks based on the edges' information extracted from applying edge detection on the original cover image, the image blocks order is the second part of the key.
- Divide the text into blocks suitable to the image block's size, sort these blocks according to their data, the text blocks' order considers the third part of the key.

After completing the embedding process for the three images, merge them into one image to get back the colored image, which represents the stego image, see the flowchart in Figure 3.

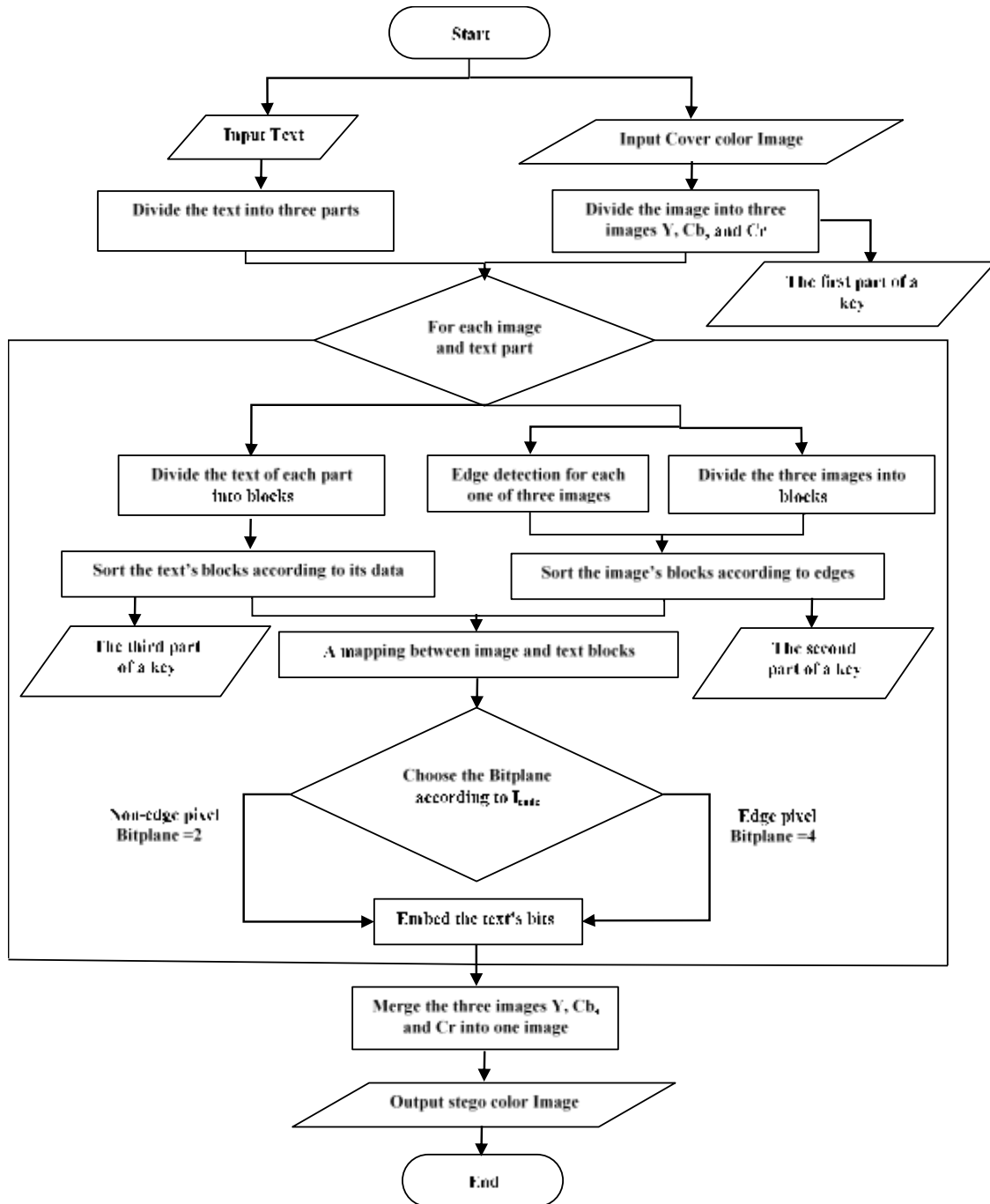


Figure 3. The flowchart of the suggested embedding phase in the color image

#### 4. EXPERIMENTATION RESULTS AND DISCUSSION

The experimentation results are executed to assess the approach performance by using some standard tests: The embedding capacity (payload) is measured by the maximum number of embedding bits per pixel (BPP) defined as in (1) [22]:

$$bpp = \frac{\text{Maximal Embedding bits}}{H*W} \quad (1)$$

Where H and W are the original cover image height and width respectively.

Peak signal-to-noise ratio (PSNR) measurement to calculate the quality difference between the original images and the stego images, higher PSNR value means less distortion. If PSNR is more than 40 dB

(decibels), then it is very good, if PSNR between 30 dB to 40 dB, then it is acceptable, and if it less than 30 dB then it is not acceptable because the distortion would be high [23], [24]. PSNR defined as in (2) [25]:

$$PSNR = 10 \times \log_{10} \frac{255 \times 255}{MSE} \tag{2}$$

Where the MSE is the mean square error between the pixels in the original image and stego image, defined as in (3) [26]:

$$MSE = \sum_{i=1}^H \sum_{j=1}^W \frac{(p_{ij} - p'_{ij})^2}{(H \times W)} \tag{3}$$

Where H and W are the original cover image or stego image height and width respectively,  $p_{ij}$  and  $p'_{ij}$  refer to pixel values of the original and the stego images, respectively. Obviously, a higher PSNR means a better quality that the stego image is very close to the original image [26]. If the stego image becomes nearer to the cover image, the value of MSE minimizes and PSNR maximizes [27], [28].

In case the suggested scheme is executed using values of non EdgeBitPlane =2 and EdgeBitPlane =4, edge detection (fuzzy logic, canny, hybrid dilate (5×5) and dilate (10×10)) on four gray images: ‘Lena’, ‘Fruits’, ‘Cat’ and ‘Sails’ of size 512×512 for conduct the experiments. The goal is to embed  $2^{12}$ B and  $2^{13}$  B, all possible cases of the suggested scheme are listed in Table 2. In the case text Size ( $2^{12} = 40064$ B), the suggested scheme achieves hiding all text data which is the maximum Payload 1.223bpp on all images with all edge detectors, in the same time it maintains the image quality, where, PSNR is high from 43.003dB to 45.790 dB by using a fuzzy logic detector. In other cases, text Size ( $2^{13} = 80128$ B) the maximum possible payload value is 2.445bpp, and the resulting payload for images range from 2.019bpp to 2.445bpp depend on the edge detector used and how many the image contain edges. The maximum payload (2.445bpp) was achieved by using dilate edge detector (5×5) and (10×10) with the ‘Sails’ image while the image quality remains acceptable with PSNR = 35.286db.

To see the difference between embedding more in the edge or non-edge better, here the suggested scheme is executed using values of non EdgeBitPlane = 4 and EdgeBitPlane = 2, edge detection (fuzzy logic, canny, hybrid dilate (5×5) and dilate (10×10)) on four gray images: ‘Lena’, ‘Fruits’, ‘Cat’ and ‘Sails’ of size 512×512 for conduct the experiments. As shown in Table 3, although the suggested scheme achieves the same maximum payload of 1.223 bpp with a text size of (40064B), in contrast, the PSNR values decrease, for example, the PSNR value decrease from 44.401 (Table 2) to 37.023db (Table 3) for the ‘Lina’ image with the fuzzy logic detector and all other images.

Finally, applying the suggested scheme on color images, where, it is executed using values of non EdgeBitPlane = 2 and EdgeBitPlane = 4, edge detection (fuzzy logic, canny, hybrid dilate (5×5)) on four-color images: ‘Lena’, ‘Fruits’, ‘Cat’ and ‘Sails’ of size 512×512 for conducting the experiments.

As shown in Table 4, in the case text size ( $2^{12} = 40064$ B), the suggested scheme achieves text hiding with maximum payload 1.223bpp on all images with all edge detectors, in the same time it maintains the image quality, where, PSNR is higher from 40.579 dB to 41.766 dB by using the canny detector. So, we increase the hidden text size until (199680B) where the maximum payload for it is 6.096 BPP, the results show that almost all images reach the maximum payload with acceptable PSNR in thirties values. Table 5 shows there is no apparent distortion in the images after hiding payload more than 6 BPP.

Table 2. The experimentation outcomes of the suggested scheme utilizing values of Non-EdgeBitPlane = 2 and EdgeBitPlane = 4 on gray images ‘Lena’, ‘Fruits’, ‘Cat’ and ‘Sails’, gray images size of 512×512

Edge Detection	Text Size (Byte)	Lena		Fruits		Cat		Sails	
		PSNR (dB)	Payload (bpp)	PSNR (dB)	Payload (bpp)	PSNR (dB)	Payload (bpp)	PSNR (dB)	Payload (bpp)
Fuzzy Logic	40064B	44.401	1.223	45.790	1.223	43.003	1.223	43.649	1.223
Canny	40064B	42.962	1.223	42.876	1.223	42.041	1.223	41.406	1.223
Hybrid	40064B	41.782	1.223	42.172	1.223	40.749	1.223	40.494	1.223
Dilate (5×5)	40064B	39.478	1.223	39.805	1.223	39.198	1.223	38.274	1.223
Dilate(10×10)	40064B	38.815	1.223	38.928	1.223	38.755	1.223	37.811	1.223
Fuzzy Logic	80128B	42.086	2.087	43.580	2.019	40.421	2.166	41.135	2.129
Canny	80128B	40.356	2.170	40.266	2.186	39.220	2.256	38.660	2.319
Hybrid	80128B	39.078	2.262	39.467	2.245	37.770	2.312	37.568	2.399
Dilate (5×5)	80128B	36.552	2.389	36.785	2.396	36.105	2.357	35.286	2.445
Dilate(10×10)	80128B	35.851	2.417	35.948	2.414	35.561	2.370	34.789	2.445

Table 3. The experimentation outcomes of the suggested scheme utilizing values of NonEdgeBitPlane=4 and EdgeBitPlane =2 on gray images 'Lena', 'Fruits', 'Cat' and 'Sails', gray images size of 512×512

Edge Detection	Text Size (Byte)	Lena		Fruits		Cat		Sails	
		PSNR (dB)	Payload (bpp)	PSNR (dB)	Payload (bpp)	PSNR (dB)	Payload (bpp)	PSNR (dB)	Payload (bpp)
Fuzzy Logic	40064B	37.023	1.223	36.991	1.223	37.219	1.223	37.115	1.223
Canny	40064B	37.174	1.223	37.196	1.223	37.400	1.223	37.329	1.223
Hybrid	40064B	37.248	1.223	37.271	1.223	37.694	1.223	37.542	1.223
Dilate (5×5)	40064B	38.059	1.223	37.857	1.223	38.660	1.223	38.835	1.223
Dilate(10×10)	40064B	38.620	1.223	38.395	1.223	39.414	1.223	39.859	1.223

Table 4. The experimentation outcomes of the suggested scheme utilizing values of Non-EdgeBitPlane=4 and EdgeBitPlane =2 on color images 'Lena', 'Fruits', 'Cat' and 'Sails', color images size of 512×512

Edge Detection	Text Size (Byte)	Lena		Fruits		Cat		Sails	
		PSNR (dB)	Payload (bpp)	PSNR (dB)	Payload (bpp)	PSNR (dB)	Payload (bpp)	PSNR (dB)	Payload (bpp)
Fuzzy Logic	40064B	39.982	1.223	40.365	1.223	41.593	1.223	39.815	1.223
Canny	40064B	41.766	1.223	41.595	1.223	40.579	1.223	40.925	1.223
Hybrid	40064B	39.212	1.223	39.381	1.223	39.567	1.223	38.776	1.223
Dilate (5×5)	40064B	39.069	1.223	39.176	1.223	38.433	1.223	38.259	1.223
Fuzzy Logic	199680B	33.201	6.078	33.639	6.065	34.900	6.074	33.056	6.072
Canny	199680B	35.045	6.090	34.827	6.090	33.814	6.089	34.199	6.089
Hybrid	199680B	32.376	6.092	32.570	6.091	32.737	6.089	31.947	6.096
Dilate (5×5)	199680B	32.104	6.092	32.150	6.091	31.538	6.089	31.357	6.090

Table 5. Show the experimentation outcomes of the suggested scheme with several edge detectors











Original Image	Fuzzy	Canny	Hybrid	Dilate
				
PSNR = Payload =	32.139dB 6.088bpp	33.069dB 6.094bpp	31.057dB 6.094bpp	30.407dB 6.094bpp
				
PSNR = Payload =	33.056dB 6.072bpp	34.199dB 6.089bpp	31.947dB 6.091bpp	31.357Db 6.090bpp

Figure 4 shows a comparison of the outcomes PSNR of gray images, 'Lena', 'Fruits', 'Cat' and 'Sails', images size of 512 × 512 utilizing values of Non-EdgeBitPlane = 2 and EdgeBitPlane = 4, embedded text size = "40064B". Also a compared the PSNR results for the "40064B" or "80128B" embedded text size. In the '512 × 512' 'Lena' gray image using Non-EdgeBitPlane = 2 and EdgeBitPlane = 4, as shown in Figure 5. The comparison was made between the two methods of embedding, the first method in which text is embedded in 4 bitplanes if it is pixel edge, and in 2 bits if the pixel is non-edge, and the second method of embedding in 2 bitplanes if it is an edge pixel, and in 4 bitplanes if it is a non-edge pixel, by comparing the PSNR results against a 512 × 512 Lena gray image, embedded text size = "40064B" see the graph in Figure 6 and Figure 7 it is a comparison of the outcomes PSNR on 'Lena' gray image and 'Lena' color image, size of 512 × 512 utilizing values of Non-EdgeBitPlane = 2 and EdgeBitPlane = 4, embedded text size = "40064B".

To evaluate the performance of the proposed method, a comparative analysis was performed based on PSNR, which measure the percentage distortions in perception, to measure the performance of various methods by using uniform experimental settings, based on some same parameter like stego image, technical properties, and security aspects. For experimentations both color and greyscale Lena.png and Baboon.png were used as cover images, with dimensions of 512×512 pixels for the two images. Table 6 shows



comparisons of PSNR values for the methods rojali the scheme which used a modification VIGENERE cipher, LSB method, and dictionary-based compression method, YUNG the scheme used k-means algorithm for ‘training the palette’, EZ-stego scheme, Fridrich the scheme used palette-based steganography method [10], and proposed scheme.

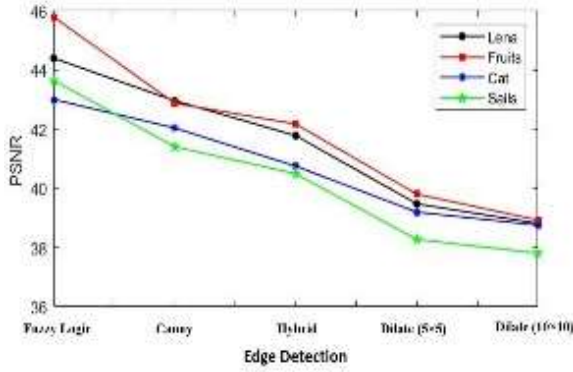


Figure 4. Comparison of the outcomes PSNR on 4 gray images

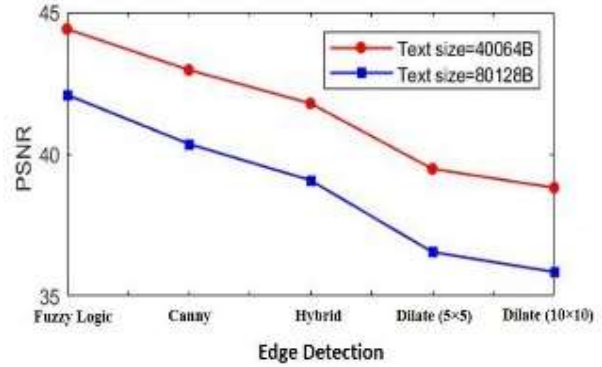


Figure 5. Comparing PSNR results based on the embedded text size

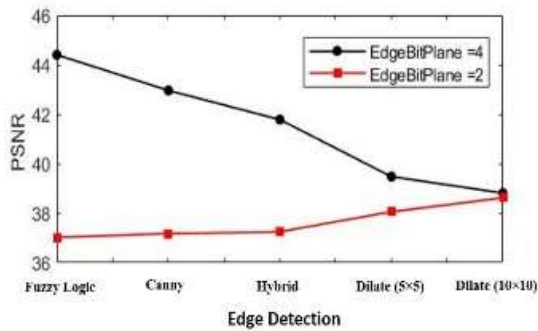


Figure 6. Comparison of PSNR results according to the embedding method

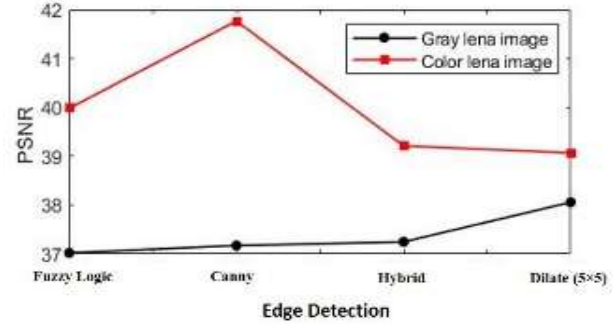


Figure 7. Compare PSNR results based on gray or color images

Table 6. The comparisons of PSNR values for several works with the proposed method

Cover Image	Rojali Scheme	YUNG Scheme	EZ-stego Scheme	Fridrich Scheme	Proposed Method
Lena	51	37	14	31	51
Baboon	51	36	15	1	51

### 5. CONCLUSIONS

In this paper, a steganography approach employing edge detection was suggested. This scheme is a good choice because it prevents the human eye from noticing any difference in the stego image. Our goal is edge detection and carries a greater number of embedding bits to achieve high payload without affecting the image clarity and quality and improving the efficiency of the system not only in terms of payload and quality but also in terms of security and confidentiality of the hidden information. Although steganography images in the spatial domain are usually easy to be attacked and penetrated, it provides more payloads. For this reason, we have focused our work on increasing confidentiality and security by preparing a secure communication technique that has been prepared that contains a key consisting of two or three parts used in the process of embedding information in images gray and colored respectively. In addition to agreeing at the beginning of the deal on the type of edge detector to be used in the embedding process. Experiments were performed using edge pixels detected by sobel, roberts, prewitt, LOG, canny, fuzzy logic, hybrid, dilate, and hybrid on both gray and colored images. The large edge pixels, resulting from the use of hybrid and fuzzy detection allow more secret data to achieve higher payloads, so it can be said that the work contributes to generating the

largest possible number of edges to hide the data. The experimental results show that the PSNR was increased from a minimum of 5% to a maximum of 8%, which means that the suggested steganography technique approach is the best in terms of payload, confidentiality as well as quality so that the stego image appears as close as possible to the original image. In the future, our approach may be applied after making enhancements to images or canceling noise from them, and steganography may be applied in the frequency domain of the image.

#### ACKNOWLEDGEMENTS

The researchers thank the Department of Computer Science, College of Computer Science and Mathematics, University of Mosul.

#### REFERENCES

- [1] Mare, S. F., Vladutiu, M., and Prodan, L., "High capacity steganographic algorithm based on payload adaptation and optimization," *7th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 2021, pp. 87–92, doi: 10.1109/saci.2012.6249981.
- [2] D. Setiadi and J. Jumanto, "An Enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel Edge Detection," *Cybernetics and Information Technologies*, vol. 18, no. 2, pp. 74–88, 2018, doi: <https://doi.org/10.2478/cait-2018-0029>.
- [3] S. Singh and A. Datar, "Improved Hash Based Approach for Secure Color Image Steganography using Canny Edge Detection Method," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 15, no. 7, pp. 92–98, 2015.
- [4] Kusuma, E. J., Indriani, O. R., Sari, C. A., and Rachmawanto, E. H., "An imperceptible LSB image hiding on edge region using des encryption," *2017 International Conference on Innovative and Creative Information Technology (ICITech)*, 2017, vol. 2018, pp. 1–6, doi: 10.1109/INNOCIT.2017.8319132.
- [5] Essa, R. J., Abdullah, N. A., and Al-Dabbagh, R. D., "Steganography Technique using Genetic Algorithm," *Iraqi J. Sci.*, vol. 59, no. 3A, 2018, doi: 10.24996/ijcs.2018.59.3a.19.
- [6] R. Kaur, Pooja, Varsha., "A hybrid approach for video steganography using edge detection and identical match techniques," *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2016, pp. 867–871, doi: 10.1109/WiSPNET.2016.7566255.
- [7] S. Arora and S. Anand, "A New Approach for Image Steganography using Edge Detection Method," *International Journal of innovative Research in computer and communication Engineering*, vol. 1, no. 3, pp. 626–629, 2013.
- [8] D. R. I. M. Setiadi, "Payload enhancement on least significant bit image steganography using edge area dilation," *Int. J. Electron. Telecommun.*, vol. 65, no. 2, pp. 287–292, 2019, doi: 10.24425/ijet.2019.126312.
- [9] Chen, W. J., Chang, C. C., and Le, T. H. N., "High payload steganography mechanism using hybrid edge detector," *Expert Systems with applications*, vol. 37, no. 4, pp. 3292–3301, 2010, doi: 10.1016/j.eswa.2009.09.050.
- [10] Ansari, A. S., Mohammadi, M. S., and Parvez, M. T., "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats," *International Journal of Computer Network and Information Security*, vol. 11, no. 1, pp. 11–25, 2019, doi: 10.5815/ijcnis.2019.01.02.
- [11] Jain, N., Meshram, S., and Dubey, S., "Image steganography using LSB and edge-detection technique," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 2, no. 3, pp. 217–222, 2012.
- [12] S. Arora and S. Anand, "A Proposed Method for Image Steganography using Edge Detection," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 2, pp. 22–25, 2013, doi: 10.31031/rmes.2018.03.000569.
- [13] Liao, X., Yu, Y., Li, B., Li, Z., and Qin, Z., "A New Payload Partition Strategy in Color Image Steganography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 3, pp. 685–696, 2020, doi: 10.1109/TCSVT.2019.2896270.
- [14] Carpentieri, B., Castiglione, A., De Santis, A., Palmieri, F., and Pizzolante, R., "Compression-based steganography," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 8, p. e5322, 2020, doi: <https://doi.org/10.1002/cpe.5322>.
- [15] Alam, S., Kumar, V., Siddiqui, W. A., and Ahmad, M., "Key dependent image steganography using edge detection," *International Conference on Advanced Computing & Communication Technologies*, 2014, pp. 85–88, doi: 10.1109/ACCT.2014.72.
- [16] B. G. Banik and S. K. Bandyopadhyay, "an Image Steganography Method on Edge Detection Using Multiple Lsb Modification Technique," *J. Basic Appl. Res. Int.*, vol. 9, no. 2, pp. 75–80, 2015.
- [17] Parah, S. A., Sheikh, J. A., Akhoun, J. A., Loan, N. A., and Bhat, G. M., "Information hiding in edges: A high capacity information hiding technique using hybrid edge detection," *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 185–207, 2018, doi: 10.1007/s11042-016-4253-x.
- [18] C. Vanmathi and S. Prabu, "Image Steganography Using Fuzzy Logic and Chaotic for Large Payload and High Imperceptibility," *International Journal of Fuzzy Systems*, vol. 20, no. 2, pp. 460–473, 2018, doi: 10.1007/s40815-017-0420-0.
- [19] K. Gaurav and U. Ghanekar, "Image steganography based on Canny edge detection, dilation operator and hybrid coding," *Journal of Information Security and Applications*, vol. 41, pp. 41–51, 2018, doi: 10.1016/j.jisa.2018.05.001.

- [20] T. Acharya and A. K. Ray, *Image processing: principles and applications*. John Wiley & Sons, 2005.
- [21] Bai, J., Chang, C. C., Nguyen, T. S., Zhu, C., and Liu, Y., "A high payload steganographic algorithm based on edge detection," *Displays*, vol. 46, pp. 42–51, 2017, doi: 10.1016/j.displa.2016.12.004.
- [22] A. Miri and K. Faez, "Adaptive image steganography based on transform domain via genetic algorithm," *Optik*, vol. 145, pp. 158–168, 2017, doi: 10.1016/j.ijleo.2017.07.043.
- [23] Pradhan, A., Sahu, A. K., Swain, G., and Sekhar, K. R., "Performance Evaluation Parameters of Image Steganography Techniques," in *2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS)*, 2016, pp. 1–6, doi: 10.1109/RAINS.2016.7764399.
- [24] Islam, M. S., Ahsan Ullah, M., and Prakash Dhar, J., "An imperceptible & robust digital image watermarking scheme based on DWT, entropy and neural network," *Karbala International Journal of Modern Science*, vol. 5, no. 1, 2019, doi: 10.33640/2405-609X.1068.
- [25] H. Al-Dmour and A. Al-Ani, "A steganography embedding method based on edge identification and XOR coding," *Expert systems with Applications*, vol. 46, pp. 293–306, 2016, doi: 10.1016/j.eswa.2015.10.024.
- [26] Z. Wang and A. C. Bovik, "Mean Squared Error: Love It or Leave It? A New Look at Signal Fidelity Measures," *IEEE signal processing magazine*, vol. 26, no. 1, pp. 98–117, 2009, doi: 10.1109/MSP.2008.930649.
- [27] Sara, U., Akter, M., and Uddin, M. S., "Image quality assessment through FSIM, SSIM, MSE and PSNR - a comparative study," *Journal of Computer and Communications*, vol. 7, no. 3, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.
- [28] Jude Hemanth, D., Anitha, J., Popescu, D. E., and Son, L. H., "A modified genetic algorithm for performance improvement of transform based image steganography systems," *Journal of Intelligent & Fuzzy Systems*, vol. 35, no. 1, pp. 197–209, 2018, doi: 10.3233/JIFS-169580.

## BIOGRAPHIES OF AUTHORS



**Mafaz Alanezi** She is a faculty member at the Department of Computer Science, University of Mosul, IRAQ. She obtained her Ph.D. degree in Computer Science in the field of Computer and Network Security from University of Mosul/Iraq in 2012. Her M.Sc. degree was also in Computer Science in the field of Image Processing from the University of Mosul/IRAQ in 2003. Her current area of research deals with Computer and Network Security, Artificial Intelligence, and cloud computing.



**Iman Subhi Mohammed Altaay** She is a faculty member at the Department of Computer Science, University of Mosul, IRAQ. She obtained her M.Sc. degree in Computer Science in the field of Image Processing from the University of Mosul/IRAQ in 2017. Her current area of research deals with Digital Image Processing, Computer Vision and Artificial Intelligence.



**Saja Younis Hamid Malla'alo** She is a faculty member at the Department of Computer Science, University of Mosul, IRAQ. Her M.Sc. degree was in Computer Science in the field of Image Processing from the University of Mosul/IRAQ. Her current area of research deals with Image Processing and Artificial Intelligence.