BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **24**, No 1
Sofia • 2024 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2024-0009

Hybrid Edge Detection Methods in Image Steganography for High Embedding Capacity

Marwah Habiban[1], *Fatima R. Hamade*[1], *Nadia A. Mohsin*[1,2]

[1]*Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq*
[2]*Scientific Affairs Department, University of Kufa, Najaf, Iraq*
E-mails: marwa.habiban@uokufa.edu.iq nadia.mohsin@uokufa.edu.iq
fatimar.hamade@uokufa.edu.iq

***Abstract*:** *In this research, we propose two new image steganography techniques focusing on increasing image-embedding capacity. The methods will encrypt and hide secret information in the edge area. We utilized two hybrid methods for the edge detection of the images. The first method combines the Laplacian of Gaussian* (*LoG*) *with the wavelet transform algorithm and the second method mixes the LOG and Canny. The Combining was performed using addWeighted. The text message will be encrypted using the GIFT cipher method for further security and low computation. For the effectiveness evaluation of the proposed method, various evaluation metrics were used such as embedding capacity, PSNR, MSE, and SSIM. The obtained results indicate that the proposed method has a greater embedding capacity in comparison with other methods, while still maintaining high levels of imperceptibility in the cover image.*

***Keywords*:** *Image steganography, Edge detection, Wavelet transform, GIFT cipher, Embedding capacity.*

1. Introduction

Due to the increasing need for the transmission of sensitive data across public and non-secure channels and the need for cloud services, information security, and privacy have emerged as a top priority. The two main techniques used to ensure the confidentiality of transmitted information are cryptography and steganography. Cryptography involves converting confidential information into an unreadable format. However, this can trigger doubt among attackers and reveal the data. Steganography involves hiding confidential information inside various media types known as the cover media. For example, of the cover media are audio, videos, and images [1, 2]. In the field of information security, the integration of cryptographic techniques with steganography is currently an area of intense research.

Images are widely used in steganography, which involves embedding information within an image file, known as image steganography, without affecting its visual quality or size. Image steganography is popular because images are shared and distributed, making it an ideal medium for covert communication or data transfer. The spatial domain of the image is the focus of this research, which involves embedding the data directly into the pixel intensity using many techniques, such as Least Significant Bit (LSB) [2, 4, 5].

LSB is a popular, low-complexity technique used in image steganography. It may substitute more than one lower-order bits of the pixels to provide high embedding capacity [6]. However, using classical LSB alone can be considered a weak method. Some researchers are exploring ways to enhance data confidentiality by combining LSB with other techniques such as applying different encryption methods to the data before the hiding process inside the cover image [6]. Meanwhile, others are concealing the data in predetermined areas of the image, such as its edges [8].

In image processing, edges refer to abrupt changes in intensity or color between neighboring pixels, which makes it a good choice to hide the information since it is less susceptible to visual inspection. Many techniques and methods have appeared in the edge detection field. Detecting edges helps highlight boundaries and shapes within an image, often done using techniques like the Sobel, Canny, Prewitt, Laplacian, and other edge detectors [3, 4].

The GIFT cipher, inspired by Feistel Networks, represents a significant advancement in lightweight cryptography. Designed with a focus on minimizing computational demands, memory usage, and energy consumption. Its unique blend of Feistel network architecture and the Grøstl hash function not only ensures efficiency but also contributes to robust security. As the digital landscape evolves towards interconnected and energy-efficient systems, GIFT's role in providing a secure cryptographic foundation for lightweight applications becomes increasingly vital, warranting a comprehensive exploration in cryptographic research.

In this paper, we present two hybrid methods for hiding confidential data within the edge area of an image after encrypting the text using Gift cipher. The purpose is to conceal the existence of secret information from unauthorized receivers. The first method combines LoG and Wavelet, and the second combines LoG and Canny. For both methods, the LSB technique is used for confidential data concealment in the cover image.

2. Related works

In order to increase the embedding capacity to store the secret data in image pixels while maintaining the image quality, S e t i a d i and M o s e s [14] propose a method that uses the edge area to hide additional secret bits. The edge area of an image can tolerate changes to the pixels better than other areas, making it an ideal location for hiding additional data. To increase the capacity of the edge area, the researchers have used a combination of Sobel and Canny edge detectors. These two methods provide a thicker edge area to hold more data while keeping the stego images imperceptible.

Edge detection using wavelet transform is weak because wavelet transforms lead to losing some high-frequency sub-image details due to noise influence. P a n [15] have proposed a new method for edge detection using wavelet transform combined with a canny detector. The edges are divided into low and high frequencies and detected using the Canny and wavelet respectively. The maximum points of the local wavelet coefficient model are used for reducing the noise influence. The two sub-image edges obtained using the canny edge detector and the wavelet transform are combined according to merger rules.

A technique for increasing the embedding capacity in images has been introduced by M o h s i n and A l a m e e n [12]. The technique is based on the edge area and is a hybrid technique. The method combines two of the most popular edge detection methods, Canny, and Prewitt, using OR operation. The text is then hidden using the method of LSB. The comparison results of this study showed that the proposed method has a high embedding capacity while preserving the imperceptibility quality of the cover image.

To address some of the problems facing image steganography such as the low hiding capacity, cover image imperceptibility, and low robustness, the authors in [16] introduce a method based on the Distinction Grade Value (DGV), which involves three phases. Firstly, a novel encryption technique called Shuffle the Segments of Secret Message (SSSM) in combination with an enhanced Huffman compression algorithm for improved embedding ability. Secondly, a Fibonacci-based method extends pixel bits from 8 to 12, enhancing scheme robustness. Thirdly, an improved embedding method combines the DGV with the random block/pixel and implicitly generates the secret key.

A hybrid edge-detection approach for hiding images into another image is used in [17]. A mix of Canny and Kirsch edge detections combined using OR operation. A 5-bit LSB is utilized for image hiding, followed by morphological dilation for noise reduction and edge enhancement. The secret image is read and converted to ASCII and then to binary. The resulting stego image is a result of concealing all the bits into the cover image. This comprehensive approach combines edge detection, pixel classification, and LSB steganography to achieve adequate data hiding while addressing the limitations of pixel value reduction and ensuring optimal tolerance in the edge region.

In [18], researchers present a steganography approach for images based on edges, classifying pixels into two groups: edges and non-edges. The strategy exploits the observation that edge pixels, characterized as having a high tolerance for noise, can conceal a greater number of secret bits compared to non-edge pixels. The method introduced employs the Difference of Gaussians (DoG) edge detection and involves three stages: edge detection, embedding, and extraction. Secret bits are embedded in both edge and non-edge pixels, maintaining a specified X: Y ratio. Experimental outcomes showcase the technique's adaptable payload and satisfactory visual clarity. Through comparative analysis, the proposed method demonstrates its superiority over traditional steganography based on edge detection in terms of payload capacity.

3. The proposed methods

Two proposed techniques will be introduced based on several methods to tackle the issues confronting image steganography, such as low embedding capacity, imperceptibility, and poor robustness. The methods used will be explained briefly below.

3.1. Wavelet transform

The wavelet transforms, represented by small waves in mathematics is a mathematical function that dissects a signal into various frequencies at distinct resolutions, a process known as multi-resolution analysis. This enables the simultaneous revelation of both the spatial and frequency characteristics of an image. At higher frequencies, it offers excellent time resolution but poor frequency resolution, whereas at lower frequencies, it provides good frequency resolution but poor time resolution [7, 8]. The primary aim of the wavelet transform is to shift data from the time domain to the frequency domain, facilitating a more straightforward analysis. The wavelet transform [9] is defines in next equation:

$$Wf(u,s)=\int_{-\infty}^{+\infty} f(t)\frac{1}{\sqrt{s}}\Psi^{*}\left(\frac{t-u}{s}\right)dt. \tag{1}$$

Wavelet filters are designed to be used in a wide range of different applications and fields. Wavelet filters depend on sub-sampling high and low pass filters; these filters correspond so that the information is decomposed into high and low pass bands. The original data of the image is split into more than one level of Low (L) frequency and High (H) frequency, where the Low (L) frequency can be split into Low frequency (LL) and High frequency (LH). Also, the same decomposition in high frequency H becomes two parts HL and HH of frequency; the separation operation continues as needed [10]. The process is explained in Fig. 1.

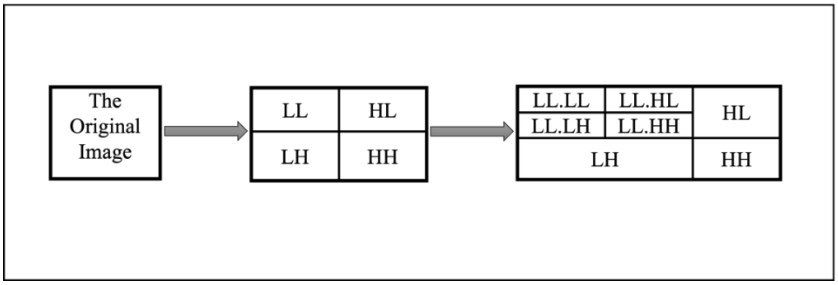


Fig. 1. Level frequency of wavelet transforms

3.2. Canny edge detection algorithm

Edge detection methods are widely used in image processing. Among various edge detection methods, the Canny edge detector is considered the most effective. Compared to other methods, it performs better [11]. Canny edge detection method has many strength points, which we can illustrate some such as: Accurate thin Edges**,** Low False Positive Rate, and it is User-friendly. A User-friendly Canny requires the selection of only two threshold values, making it more user-friendly compared to

methods that require tuning multiple parameters. A key point in the canny edge detector that it enhances the signal-to-noise ratio. At the same time Canny suffers from weakness such.

We can list the steps of applying the Canny Algorithm as follows:

1. Convert the input image into a grayscale image using the equation

(2) $$y = 0.299R + 0.587G + 0.114B.$$

2. Reduce the noise using a Gaussian filter.

3. Finding the intensity gradient of the image in the vertical and horizontal directions by using the Sobel filter, where we can find the gradient magnitude and gradient direction of each pixel as in formula:

(3) $$\text{edge}_{\text{Gradient}} = \sqrt{Gx^2 + Gy^2}.$$

4. Apply Non-maximum suppression; the resulting image will be a binary image.

5. Apply Hysteresis thresholding. In this step, specify the actual edges where there are two values, a maximum and a minimum value of thresholding as follows:

i. The edges with gradient intensity greater than the maximum value will be considered real edges.

ii. The edges with a gradient intensity less than the minimum value are not considered real edges and are ignored. Only the confirmed edges are considered.

iii. The pixels that fall between the two thresholding values can create new edges or not, depending on how they connect with existing edges. If they are connected to confirmed edges, they will be considered as part of the edges. However, if they are not, then they will be discarded.

(a) (b)

Fig. 2. Cover image (a), and Canny edge detection (b)

3.3. The Laplacian of Gaussian

The Laplacian method is widely used in image processing for detecting edges in an image. It works by searching for zero crossings in the second derivative of the image. An edge typically has the shape of a ramp in one dimension, and the Laplacian method calculates the derivative of the image to highlight the location of this ramp. In simpler terms, the Laplacian measures the second-order spatial derivative of an image, which helps detect areas of abrupt change or edges in an image. However, the Laplacian filter is susceptible to noise. Therefore, before applying the Laplacian filter, the image is usually smoothed using a Gaussian filter to remove the effect of

noise. This two-step process is called the LoG operation[2]. The steps of Laplacian of Gaussian (LoG)can be described as follows:

1. After reading an image, the Laplacian filter is applied to the input image (I) using the Laplacian function of an image pixel $L(x, y)$, which is based on the second derivative (∇^2 f) as in (4).

$$L(x,y) = \frac{\partial^2 I}{\partial x^2} + \frac{\partial^2 I}{\partial y^2}, \tag{4}$$

We can also calculate the second derivative by using the kernel mask directly:

–1	–1	–1
–1	8	–1
–1	–1	–1

or

0	–1	0
–1	4	–1
0	–1	0

2. Apply the Gaussian blur smoothing filter on the Laplacian result image to reduce the noise and details in the image. the result of combining the Laplacian and the Gaussian filter is called the Laplacian of Gaussian (LoG) and the equation of LoG in Equation (5):

$$\mathrm{LoG} = -\frac{1}{\pi\sigma^4}\left[1 - \frac{x^2+y^2}{2\sigma^2}\right] e^{-\frac{x^2+y^2}{2\sigma^2}}. \tag{5}$$

(a) (b)

Fig. 3. Cover image (a), and Laplacian of Gaussian (b)

3.4. A comparison of used edge detection methods

In our hybrid methods, we have utilized various edge detection techniques. In this section, we will provide a brief comparison of these techniques. This comparison will help in identifying the strengths and limitations of each technique to provide an insight into their suitability for different applications. We will be looking at their sensitivity to noise, edge thickness, edge localization, and computational complexity. It is important to note that, unlike the other methods, Wavelet transform is not exclusively designed for edge detection. It is a versatile mathematical tool that can be used for various signal and image processing applications, including edge detection [3, 7, 11].

Table 1. A comparison of Edge detection methods

Method	Noise sensitivity	Edge thickness	Edge localization	Computational complexity
Canny	Sensitive to noise	Thin edges	Precise and well-defined edges	expensive due to Gaussian convolution and Laplacian operation
LoG	Effectively handles noise due to Gaussian smoothing	Thicker edges	Accurate edges due to noise suppression and emphasizing the intensity changes	Involves multiple stages but is less computationally intensive compared to LoG
Wavelet	Effectively denoises by separating details at different scales	Depending on decomposition levels	Accurate edges due to decomposing the image into different frequencies	depends on the type of wavelet and decomposition levels

3.5. GIFT

GIFT is a highly efficient algorithm that offers significant improvements in terms of speed and size. Not only that, but it also addresses the known vulnerability of PRESENT when it comes to linear hulls. GIFT is one of the substitution-permutation networks (SPN). Two versions are presented: GIFT 64-128 and GIFT 128-128. In GIFT-64-128, they used a block of size 64, a key of size 128, and 28 rounds. GIFT 128-128, 128 block size, 128 key sizes, and 40 rounds are used [12].

Three main stages are in this GIFT method that can be like wrapping a gift (and it is the reason behind the name).

First stage. Insert the content in a box or what is called the substitution layer. A 4-bit substitution box is used as the GIFT substitution box GS as shown below in Table 1 [12]**.**

Table 2. GIFT substitution box

I	0	1	2	3	4	5	6	7	8	9	*a*	*b*	*c*	*D*	*E*	*f*
GS(i)	1	*A*	4	*C*	6	*f*	3	9	2	*d*	*b*	7	5	0	8	*e*

Second stage. Wrap the box with ribbons or the permutation layer. Bits are mapped from a bit in position i into a bit in position $p(i)$. The bit permutation will always arrive at the same position as the appropriate s-box as shown in Fig. 4.

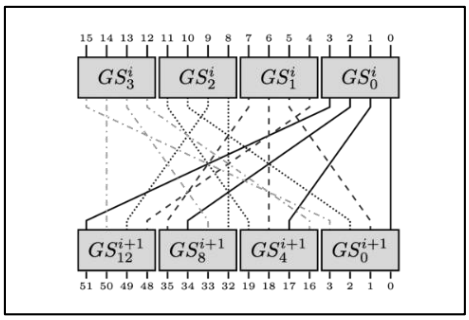


Fig. 4. Gift bit permutation

The GIFT-64 permutation can be expressed as follows:

$$P_{64}(i) = 4\left\lfloor \frac{i}{16} \right\rfloor + 16\left(\left(3\left\lfloor \frac{i \bmod 16}{4} \right\rfloor + (i \bmod 4) \right) \bmod 4 \right) + (i \bmod 4). \quad (6)$$

Third stage. Make a knot to lock the box or add-around key. This stage is divided into two steps, adding the round key, and adding the Round Constants. Adding the round key begins by extracting a 32-bit from the 128-state key. Then this 32-bit is divided into two 16-bit keys as in the next equations:

$$\text{RK} = D \| V, \quad (7)$$

$$\text{RK} = d_{15}, ..., d_0 \ \| \ v_{15}, ..., v_0. \quad (8)$$

The D and V subkeys are respectively XORed with the $b4i+1$ and $b4i$. The state key K which can be expressed as $K = K_0, K_1, \ldots, K_7$ is updated each round by rotating the K_0 12 bits and K_1 2 bits.

Adding the round constants is done by setting the six-bit round constants to zero first. Then the round constants are updated before being used as

$$(cn_0, cn_1, cn_2, cn_3, cn_4, cn_5) \leftarrow (cn_5, cn_0, cn_1, cn_2, cn_3, cn_4 \text{ XOR } cn_4 \text{ XOR1}). \quad (9)$$

After that, the round constant key C of 6-bits and a one-bit "1" are XORed to the cipher, $\text{bit}_{n-1} = \text{bit}_{n-1}$ XOR 1, $\text{bit}_{23} = \text{bit}_{23}$ XOR cn_5, $\text{bit}_{19} = \text{bit}_{19}$ XOR cn_4, $\text{bit}_{15} = \text{bit}_{15}$ XOR cn_3, $\text{bit}_{11} = \text{bit}_{11}$ XOR cn_2, $\text{bit}_7 = \text{bit}_7$ XOR cn_1, and $\text{bit}_3 = \text{bit}_3$ XOR cn_0 [12].

3.6. The proposed methods

In this paper, we present new hybrid methods that combines text encryption and image steganography. The encrypted text is concealed in the edges of the image, which are located using two hybrid methods for edge localization. The first approach depends on blending the Laplacian of Gaussian with canny edge detection. The second approach also depends on merging the Laplacian of Gaussian with Haar wavelet transform and finding the result. Comparing the two results and selecting the best one to use in cipher text operation, the best edge detection method depends on the one with a higher embedding capacity and keeping high image quality. The secret message is transformed into a binary form and encrypted using GIFT ciphering.

Both methods have three main steps. First, edge extracting is used to find the embedding area. The second step is to transform the string into a series of zeros and ones, applying GIFT-64 encryption on it, and saving the result. The third and final step is to use the LSB method for hiding the encrypted string. The result of these steps will be a binary image that holds the confidential text string.

The first technique will be by combining the Laplacian of Gaussian (LoG) filter with the wavelet transform. Ten steps describe the process.

Step 1. Read the text T.

Step 2. Encrypt the text using GIFT encryption.

Step 3. Read the source image I.

Step 4. Convert the source image to a grayscale image.

Step 5. Apply the wavelet transform using Haar wavelets to decompose the grayscale image into different frequency bands and spatial scales and save the edge details (which are LH, HL, and HH that contain the high-frequency information).

Step 6. Normalize and transform the edge details from the previous step into an edge image called *W*.

Step 7. Apply the Laplacian of Gaussian (LoG) filter for the same grayscale image to find the edges and the result saved in *L*.

Step 8. Combining *W* and *L* using addWeighted function

(10) $$R = W \text{ add}W\text{eighted } L.$$

Step 9. The result of Step 8 will be saved as a map to be used later in the text extraction at the receiver side.

Step 10. Conceal the encrypted text in *R* by employing the LSB method using 1 bit per edge pixel, where: *W* is the result edges using Haar wavelets; *L* is the result edges using LoG; alpha = 0.50; *R* is the result of combining the Haar wavelets and LoG.

The second method follows the same steps the only difference is the edge localization depends on mixing the LoG with the canny. Nine steps describe the blend technique.

Step 1. Read the source image I.

Step 2. Read the text T.

Step 3. Encrypt the text using GIFT encryption.

Step 4. Convert the source image to a grayscale image.

Step 5. Find the edges using LoG and save the image in *L*.

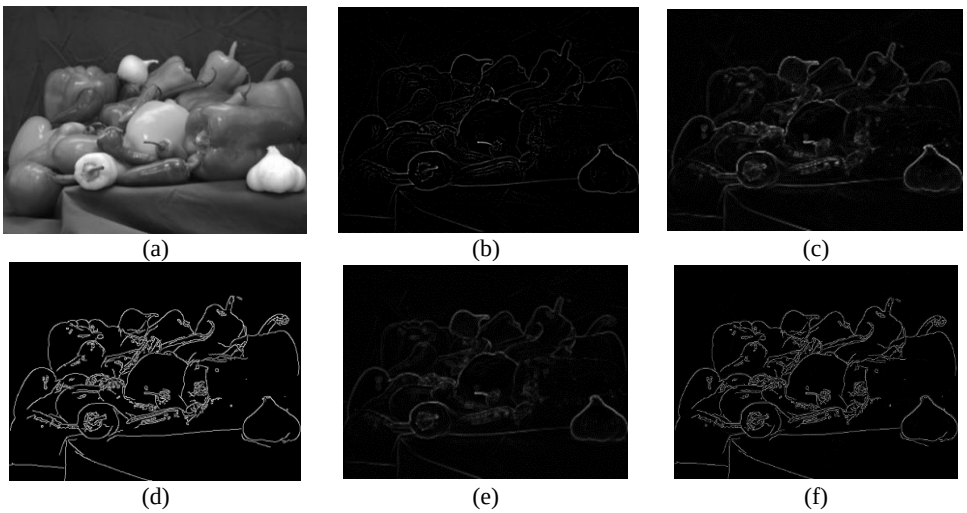
Step 6. Find the edges using the Canny operator.

Step 7. Combining the two results *L* and *C* using the addWeighted function in the result saved in LC.

Step 8. The result of Step 7 will be saved as a map to be used later in the text extraction at the receiver side.

Step 9. Conceal the encrypted text in LC by employing the LSB method using 1 bit per edge pixel.

It is essential to mention that we will not discuss the map exchange technique in this research.



(a) (b) (c)

(d) (e) (f)

Fig. 5. Cover image (a), Laplacian of Gaussian (b), Wavelets (c), Canny (d), LoG-wavelets (e), LoG-Canny (f)

4. Experimental results

This section shows the experimental outcomes conducted to assess the effectiveness of the suggested methodologies. The methodologies were implemented and tested using Python and MATLAB R2023b. Standard grey images were employed for the evaluation. Both proposed techniques were compared with other methods relying on edge-based hiding techniques. The embedded messages varied in sizes of 512, 1042, 2048, and 4096 bytes.

In this scholarly work, we employed four assessment criteria, encompassing embedding capacity, Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measurement (SSIM), and Mean Square Error (MSE), Firstly, the embedding capacity denotes the quantity of edge pixels capable of concealing confidential information.

PSNR, which stands for Peak Signal-to-Noise Ratio, is widely used in the field of image processing to evaluate the quality of reconstructed images. Interestingly, the human visual system finds it very difficult to detect any differences between the stego and the original images if the PSNR value is less than 35. This that a higher PSNR value indicates better image quality. PSNR is defined by a logarithmic scale, which is commonly used as a standard tool for evaluating image quality:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{\sqrt{\mathrm{MSE}}}\right). \tag{11}$$

The MSE values are calculated using the next equation:

$$\mathrm{MSE} = \sum_{m=0}^{m}\sum_{n=0}^{n}\|c(m,n) - s(m,n)\|. \tag{12}$$

The values of m and n represent the height and the width of the cover image, while C and S denote the cover image and the Stego image, respectively. It is well known that as the stego image approaches the cover image, the MSE value decreases while the PSNR value increases. SSIM is used to measure the similarity between the cover and the stego-images, considering the differences in contrast, local luminance, and spatial structure. The below formula is for SSIM calculation:

$$\mathrm{SSIM}(C,S) = \frac{(2\mu_C\mu_S+y)(2\sigma_{CS}+y_2)}{(\mu_C^2+\mu_S^2+y_1)(\sigma_C^2+\sigma_S^2+y_2)}. \tag{13}$$

Each C and μ_C represents the cover image and its mean, respectively. S and μ_S represent the stego image and its mean value. The covariance of the cover and stego images is defined by σ_{CS}. Y_1 and Y_2 are variables that stabilize the division with a weak denominator. σ_C^2 and σ_S^2 are the cover and stego image variances, respectively.

Fig. 6 illustrates detailed information regarding the average count of edge regions in images employing different edge detection techniques, illustrating the embedding capacity across diverse methods. The assessment considers both LoG-Wavelet and LoG-Canny with and without edge dilation. The results indicate that both suggested approaches exhibit a better embedding capacity than alternative methods across all images. Comparing our methods to the one introduced in [12], which combines Canny and Prewitt and applies edge dilation, we notice that our methods achieve better results when applying edge dilation, too.

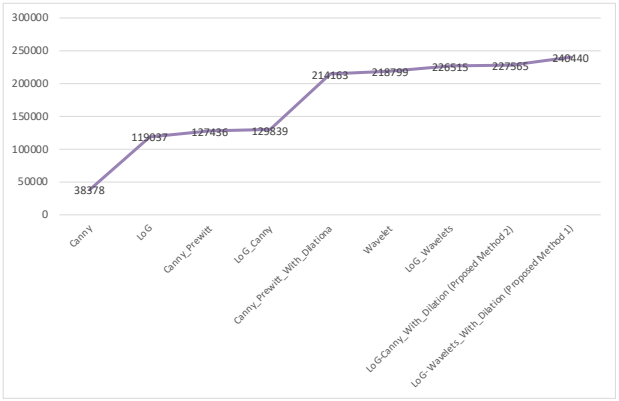


Fig. 6. The Average Number of Edge Pixels (Embedding capacity)

Table 3. Concealment of 512 byte

No	Edge detection method	PSNR	SSIM	MSE
1	Canny	69.90	0.99999951	0.0071084
2	Wavelet	69.99	0.99988879	0.0069901
3	LoG	70.11	0.99989913	0.0069901
4	Canny_Prewitt [12]	70.03	0.99994259	0.0069065
5	Proposed Approach_1(LoG_Wavelet)	70.01	0.99989368	0.0069132
6	Proposed Approach_2 (LoG_Canny)	69.90	0.9998843	0.0070899
7	Canny_Prewitt with Dilation [12]	69.96	0.99995042	0.0069688
8	Proposed Approach_1 with Dilation	70.04	0.99990496	0.0068568
9	Proposed Approach_2 with Dilation	69.80	0.99988668	0.0073729

Table 4. Concealment of 1024 byte

No	Edge detection method	PSNR	SSIM	MSE
1	Canny	66.89	0.9999991	0.0142168
2	Wavelet	67.34	0.99978433	0.0128388
3	LoG	67.45	0.99978899	0.0124939
4	Canny_Prewitt [12]	67.35	0.99990838	0.0127532
5	Proposed Approach_1(LoG_Wavelet)	67.32	0.99981022	0.012836
6	Proposed Approach_2 (LoG_Canny)	66.91	0.9997662	0.0141551
7	Canny_Prewitt withDilation [12]	66.90	0.99990127	0.0141957
8	Proposed Approach_1 with Dilation	67.00	0.99980678	0.0138245
9	Proposed Approach_2 with Dilation	66.95	0.99976766	0.0140133

Table 5. Concealment of 2048 byte

No	Edge detection method	PSNR	SSIM	MSE
1	Canny	65.04	0.99999877	0.0218043
2	Wavelet	64.03	0.99961521	0.0276021
3	LoG	63.36	0.99946259	0.0321272
4	Canny_Prewitt [12]	64.03	0.99977828	0.0279167
5	Proposed Approach_1(LoG_Wavelet)	63.65	0.99956839	0.0298561
6	Proposed Approach_2 (LoG_Canny)	63.80	0.99962958	0.0288242
7	Canny_Prewitt withDilation [12]	64.16	0.99980303	0.0271773
8	Proposed Approach_1 with Dilation	63.61	0.9996041	0.0301547
9	Proposed Approach_2 with Dilation	63.61	0.99957583	0.0299778

Table 6. Concealment of 4096 byte

No	Edge detection method	PSNR	SSIM	MSE
1	Canny	62.83	0.99999807	0.0356037
2	Wavelet	61.03	0.99929668	0.0549864
3	LoG	60.24	0.99897265	0.0658303
4	Canny_Prewitt [12]	60.39	0.99952211	0.06175
5	Proposed Approach_1(LoG_Wavelet)	60.59	0.99915841	0.060307
6	Proposed Approach_2 (LoG_Canny)	60.81	0.99938013	0.0573304
7	Canny_Prewitt withDilation [12]	61.20	0.99964568	0.054026
8	Proposed Approach_1 with Dilation	60.54	0.99950131	0.0556511
9	Proposed Approach_2 with Dilation	60.58	0.99921991	0.0603201

Fig. 7. Cover images

Tables 3-6 represent the PSNR, MSE, and SSIM values. They conclude the average values of the eight cover images illustrated in Fig. 7. The methods discussed here involve hiding a secret message in edge area pixels. Since each byte consists of 8 bits and only 1 bit is used in each pixel, a 1024-byte message would require

8192 pixels. The proposed approach offers a larger edge area of pixels that can be used for secret text hiding.

PSNR values obtained of the suggested methods in Tables 3-6 we can notice that the values are slightly changing up and down for the same message size with different methods. When examining MSE and SSIM values, they appear identical when rounded to three decimal places across all methods and various text sizes. This consistency implies that hiding with our method is superior, given the significantly greater number of edge area pixels it possesses compared to other methods. Thus, it can be concluded that the two proposed methods are better for embedding larger messages while maintaining a very close values, regarding the calculated measurement aspects of the image quality, compared to other methods.

5. Conclusions

This paper presents two new methods for encrypting and steganography of confidential data in images. The methods involve encrypting the text using GIFT cryptography and concealing the encrypted message in the edges of the image. For edge specification, a hybrid method is utilized, with the first approach combining LoG and Wavelet for hybrid edge detection. On the other hand, the second approach combines LoG and Canny to enlarge the size of the embedding area.

According to experimental results, the combination of LoG-Wavelets results in a higher embedding capacity compared to using these techniques separately. The Canny method has an average edge area (embedding capacity) of 38,378 pixels, while the wavelet method has an average of 218,799 pixels. In LoG-Wavelet and LoG_Canny methods, the average number of pixels is 240,440 and 227,565, respectively. More pixels introduce a higher opportunity to hide a larger amount of data without compromising the quality of the image. This is because PSNR, SSIM, and MSE values remain almost unchanged.

References

1. Ghosal, S. K., A. Chatterjee, R. Sarkar. Image Steganography Based on Kirsch Edge Detection. – Multimedia Systems, Vol. **27**, 2021, No 1, pp. 73-87.
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. Maini, R., H. Aggarwal. Study and Comparison of Various Image Edge Detection Techniques. – International Journal of Image Processing (IJIP), Vol. **3**, 2009, No 1, pp. 1-11.
4. Amer, G. M. H., A. M. Abushaala. Edge Detection Methods. – In: Proc. of 2nd World Symposium on Web Applications and Networking (WSWAN'15), IEEE, 2015.
5. 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.
6. ALabaichi, A., 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 (2088-8708), Vol. **10**, 2020, No 1.
7. Kumar, K., et al. Image Edge Detection Scheme Using Wavelet Transform. – In: Proc. of 11th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP'14), IEEE, 2014.

8. J u n g, U., J.-C. L u. A Wavelet-Based Random Effect Model for Multiple Sets of Complicated Functional Data. Technical Report, Scool of Industrial and Systems Engeneering, Georgia Institute of Technology, Atlanta, USA, 2004.
9. D. Baleanu, Ed. Advances in Wavelet Theory and Their Applications in Engineering, Physics, and Technology. BoD-Books on Demand, 2012.
10. M a l l a t, S. A Wavelet Tour of Signal Processing. Elsevier, 1999.
11. K u m a r, G., 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.
12. M o h s i n, N. A., H. A. A l a m e e n. A Hybrid Method for Payload Enhancement in Image Steganography Based on Edge Area Detection. – Cybernetics and Information Technologies, Vol. **21**, 2021, No 3, pp. 97-107.
13. B a n i k, S., et al. GIFT: A Small Present: Towards Reaching the Limit of Lightweight Encryption. – In: Proc. of 19th International Conference, Cryptographic Hardware and Embedded Systems (CHES'17), Taipei, Taiwan, 25-28 September 2017, Springer International Publishing, 2017.
14. 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.
15. P a n, J. Edge Detection Combining Wavelet Transform and Canny Operator Based on Fusion Rules/Pan Jianjia. – International Conference on Wavelet Analysis and Pattern Recognition, Baoding, Vol. **328**, 2009, p. 324.
16. T a h a, M. S., et al. High Payload Image Steganography Scheme with Minimum Distortion Based on Distinction Grade Value Method. – Multimedia Tools and Applications, Vol. **81**, 2022, No 18, pp. 25913-25946.
17. B e l a g a l i, P., V. R. U d u p i. Robust Image Steganography Based on Hybrid Edge Detection. – Tuijin Jishu/Journal of Propulsion Technology, Vol. **44**, 2023, No 3, pp. 1509-1521.
18. P a t w a r i, B., U. N a n d i, S. K. G h o s a l. Image Steganography Based on the Difference of Gaussians Edge Detection. – Multimedia Tools and Applications, 2023, pp. 1-21.
19. X u e, L.-Y., J.-J. P a n. Edge Detection Combining Wavelet Transform and Canny Operator Based on Fusion Rules. – In: Proc. of International Conference on Wavelet Analysis and Pattern Recognition, IEEE, 2009.

Received: 29.11.2023; Second Version: 22.01.2024; Accepted: 07.02.2024 (fast track)