ZANCO Journal of Pure and Applied Sciences

TYPE Original article
DOI http://dx.doi.org/10.21271/ZJPAS.38.3.10

OPEN ACCESS

*Corresponding author
Shang Masood Abdullah
shangg.masood09@gmail.com

RECEIVED :12 /09/2025
ACCEPTED :22/11/ 2025
PUBLISHED :30/06/2026

KEYWORDS:
Image steganography, Adaptive embedding, Region of Interest (ROI) selection, imperceptibility.

A Hybrid Region-Based Approach for Image Steganography

Shang Masood Abdullah* & Rasber Dhahir Rashid

Department of Computer Science and IT, College of Science, Salahaddin University-Erbil, Erbil-Kurdistan Region, Iraq

ABSTRACT

Steganography is the process of embedding a hidden message in a cover that is undetectable to unknown receivers. Since digital images have a high degree of redundancy that can be utilized for concealing a message, image steganography has been one of the most popular types of steganography. However, Steganalysis is focused on detecting such secret messages. Steganalysis procedures represent a major challenge to the security and accuracy of steganographic methods by analyzing statistical irregularities or structural distortions introduced during the embedding process. One of the most common questions that could be raised in this area is where the secret message should be placed so that it could be both robust and not noticeable for the attackers. This question will be addressed in the given paper by proposing a hybrid region selection method of embedding. We use a hybrid technique to detect edge areas using Canny and Sobel operators, also the texture-rich areas detected by using the concept of entropy and standard deviation filters. The hybrid method increases the payload capacity, decreases detectability, and ensures that embedding takes place in visually complex areas. Experiments show that our method is both secure and undetectable, delivering the state-of-the-art benchmark methods with PSNR above 63 dB and SSIM near to 1.

1.Introduction

Users in the modern internet use century, need fast, cheap, and safely communication routes. Therefore network security has become an important topic in the field and has been a much-discussed topic nowadays (Abdlrazaq et al., 2023). Steganography, watermarking, and cryptography are approaches used to preserve information security (Kadhim et al., 2019).

Steganography is one of the important methods in the modern world that conceals secret information inside a cover medium, such as audio, image, video, Graphics, and Text files. A stego refers to a cover that contains concealed information. Steganographic algorithms allow both the sender and the receiver to remain anonymous since they cannot be detected by attackers. One of the most popular media for hiding information is image. The effectiveness of image steganography relies on three core characteristics: capacity, robustness, and imperceptibility (Khalind, 2019).Capacity determines how much hidden data an image can store, robustness reflects the embedded information's ability to survive modifications, and imperceptibility ensures the alterations remain undetectable to human observers. These elements are fundamentally interconnected, improving one typically comes at the expense of another. (Martín et al., 2023).

One of the most popular method of image steganography is Least Significant Bit (LSB) embedding, which aims to embed the information in least significant bit (LSB) of each pixel in a way that is not visibly distorted. Although it has a high payload capacity, it can be easily detected by steganalysis tools to reveal hidden messages(Westfeld and Pfitzmann, 1999). One of the effective methods to handle the challenges in image steganography is by using adaptive approaches(Rashid and Majeed, 2019). These methods improve how data is embedded based on the characteristics of the cover image. Adaptivity can come in different approaches, such as choosing which pixels inside the image to modify, deciding how to modify them, or determining how many bits to embed in each pixel. The human eye is more sensitive to changes in smooth areas of an image and less likely to notice alterations in textured regions (Kadhim et al., 2019). Therefore, many adaptive methods focus on embedding data in the more textured regions of the image to enhance both the visual quality of the stego-image and the robustness of the embedding technique. One way to identify such complex regions is by measuring entropy, which quantifies the amount of information or randomness in an image area. High-entropy regions tend to be more textured and detailed (Yang et al., 2009). High-frequency regions such as edges or regions with rapid changes in intensity, which the human eye is insensitive to, are detected by edge-detection algorithms like Sobel or Canny filters (Yang et al., 2008). While there have been a lot of improvements, most modern spatial and adaptive steganography methods still only use one feature domain, such as entropy, edge, or texture. This makes it more difficult for them to find regions that are visually complex and can handle embedding without changing how they look. In this paper, we propose a hybrid image steganographic method that combines texture-based technique and edge detection methods to identify the most suitable regions for data embedding. The approach begins by analyzing the image using both entropy and standard deviation (std) filters, which are effective in highlighting areas rich in texture and detail. we incorporate edge detection techniques, specifically the Canny and Sobel filters. These methods help identify sharp transitions and edges within the image. By combining texture and edge information, we create a more accurate Region of Interest (ROI) map for embedding. Finally, we analyze the standard deviation of the entropy map from the original image to select the most optimal regions for data hiding The main contributions of this paper is that proposed a hybrid region-based image steganographic approach that combines both texture and edge information to define optimal embedding regions by utilizing entropy and standard deviation filtering to highlight texture-rich regions, which are less perceptible to the human visual system, regarding the edge detection we integrate Canny and Sobel edge detection to ensure data is embedded in visually insensitive, also we used statistical analysis of entropy distribution to further refine the Region of Interest (ROI) selection. As a result, the experimental results show improvements in embedding imperceptibility and resistance to steganalysis compared to some benchmark LSB-based algorithms and single-feature adaptive method

2. Related works

Adaptive embedding methods aim to improve the robustness, imperceptibility, and capacity of steganography by adapting data-hiding approaches to the image content. A well-known area of research is the use of regions of high variation in intensity, often known as image edges, where the visual variation is less noticeable. Since these regions are normally used to display high-frequency content, they can hide more information without significantly affecting the visual quality of the cover image. These techniques do not only maintain the appearance but also show a higher resistance to steganalysis compared to the other traditional techniques (Setiadi, 2022) .To increase the embedding capacity while maintaining imperceptibility, (Setiadi and Jumanto, 2018) one can use more than one edge detection methods such as Canny and Sobel edge detectors. This combination allows finding a wider range of edge pixels, thus expanding the embedding space without losing imperceptibility. According to this idea, authors in (Hardan et al., 2025)suggests a hybrid scheme combining Canny and Prewitt detectors by logical OR operation, and then dilating the edge areas. The resulting structure provides a greater payload with maintenance of visual integrity (Mohsin and Alameen, 2021). However, edge-based methods often ignore non-edge areas, which affects the embedding's capacity. To address this challenge, authors of (Al-Dmour and Al-Ani, 2016, Sultana and Kamal, 2021, Sultana et al., 2024) provides techniques to partition the pixels into edge and non-edge areas, use adaptive techniques in each subset and store more bits in the edge areas. This technique offers a high degree of visual quality and increases the level of data security because it reduces the human visual system's sensitivity to changes in the complex area.

In addition to their advantages, edge embedding techniques have a related limit that is determined by the total amount of edges in an image. The overall embedding capacity may be significantly reduced in limited edge regions. To reduce this problem, the study described in (Hardan et al., 2025) chooses a slightly more particular classification system, this time using the Canny edge detector to partition the pixels in an image into three distinct sets: edge pixels, the neighboring pixels that lie near the edges, and non-edge pixels. The method combines least significant bit (LSB) embedding and Huffman coding to increase capacity. Prewitt Edge Detector and the Canny Edge Detector are combined in (Parah et al., 2018). Canny gives good localization and Prewitt, which claims to be fast, is based on convolution to detect edges. The hybrid framework has better quality measures as shown by the values of PSNR and histogram analysis parameters as it generates high-quality stego-images and enhances resistance to statistical attacks. The challenge with the edge-based methods in general is that an edge pixel that was initially discovered by embedding may no longer be an edge pixel after embedding. This might render the embedding strategy inconsistent and unreliable (Setiadi and Jumanto, 2018) .

The new area of study in adaptive image steganography has been on entropy-based and texture-based approaches as potential alternatives or improvements to the traditional edge-detecting techniques. The identification and utilization of areas that include significant levels of regional intensity, textured or noise areas where changes to the embedding are less noticeable and more resistant. The process described in (Roy and Changder, 2014)consists in choosing complex areas of texture by calculating entropy at the time when the process of embedding the message is embedded. Embedding of regions with the higher entropy is emphasized and the images are separated into blocks that four pixel by four pixel and blocks that do not overlap. Data hiding is made simple and reliable by the block structure that results from this, which makes it easier to locate complex areas. This guarantees that distortion is reduced to a minimum and embedding efficiency remains at its lowest level. various methods of the block-based model are developed for use in embedding decisions using statistical filters, such as entropy or standard deviation (Kaur and Juneja, 2017, Halder et al., 2019). Instead of smoothing objects, these filters detect areas with texture that could be used for steganographic manipulation. The entropy-thresholding algorithm removes blocks with an information complexity which is less than the threshold, and the standard deviation of intensities is employed to identify areas containing a large quantity of texture. These methods are often compared to more established pixel-wise embedding algorithms in order to measure their effectiveness. Among such algorithms, those are WOW (Wavelet Obtained Weights) (Holub and Fridrich, 2012) and S-UNIWARD (Spatial Universal Wavelet Relative Distortion (Holub et al., 2014). These benchmark models apply advanced methods of minimization of distortion and an advantage of the content and they are recent state-of-the-art in secure steganography. They are severe parameters of the review of the

$$H(x) = -\sum_{i\in 0}^{255} p_i \log_2 p_i \qquad (1)$$

security and effectiveness of more adaptive or region-based approaches.

HiGAN (Zhu et al., 2024), SteganoGAN (Zhang et al., 2019), and U-Net-based embedding (Zeng et al., 2023) are some of the newest deep learning methods that enable images to achieve high quality. However, they often need a lot of training data, time to fine-tune the parameters, and computing power. Handcrafted spatial methods are usually easier to understand, but they rely on limited statistical features. Our work fills this gap by making a hybrid, handcrafted ROI-based method that uses complementary descriptors to make an embedding that is easy to understand and works well without needing to train a neural network.

Unlike previous edge-only or single-feature adaptive methods, the proposed approach combines entropy, texture, and edge detection to identify robust ROIs for standard LSB embedding. This hybrid selection avoids the capacity loss seen in images with few edges, maintains imperceptibility by targeting complex regions, and enhances resistance to steganalysis, addressing the limitation of low embedding capacity in earlier edge-based techniques.

3. proposed method

In this paper, we proposed a new content-based adaptive steganographic embedding method, by finding Regions of Interest (ROIs) using a hybrid entropy, texture, and edge detection algorithms. While avoiding distortions in smoother regions, the embedding process selectively modifies least significant bits (LSBs) in high-complexity regions. the outline of the proposed method showed in Figure 1.

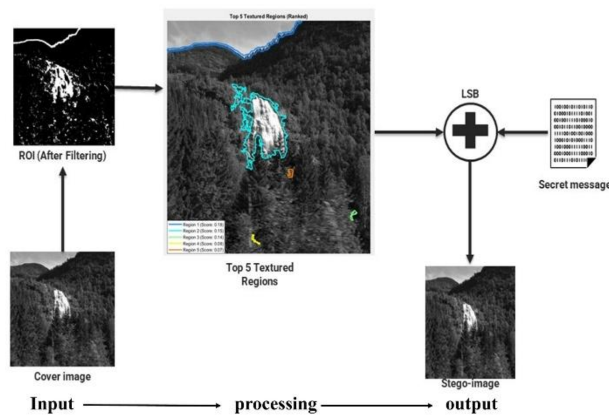


Figure 1 Proposed method

3.1 ROI Selection

A hybrid approach that combines edge detection, texture analysis, and entropy filtering is used to determine the optimal regions for data embedding. Because this method employs a range of features, embedding locations occur in regions with higher complexity and lower visual sensitivity.

3.1.1 Entropy

In image analysis and image processing, entropy is a measure of the randomness of pixel intensities that determines the complexity or unreliability of an image's texture. Entropy can be used as a measure of image quality in grayscale images due to determines the level of uncertainty in the intensity of pixels (Johnson et al., 2001). The equation of finding the entropy is as follows:

H(x) represents the image entropy, and the variable i corresponds to a possible gray-level intensity in an 8-bit image, ranging from 0 to 255. p_i denotes the probability of occurrence of each intensity value. In this work, we use entropy filtering on grayscale images to calculate a local entropy map. For this, a sliding window in the image is used, and the entropy is calculated within every neighborhood. The entropy value, representing the statistical entropy of local intensities, is consequently calculated for each pixel. A region with high entropy relates to an area in the image that is more textural or complex. These regions are particularly useful for embedding secret data, as any data change in such regions is less likely to be noticed by the human visual system. According to the implementation settings as shown in Table 1, we found that 9×9 blocking entropy filter have higher capacity than the other blocking sizes.

Table 1 compares different window sizes for entropy and standard deviation (std) filters. Based on maximum capacity, the optimal selections are a 9×9 window for entropy and a 5×5 window for std.

Table 1.a

Entropy 5x5				
		Std 5x5	Std 7x7	Std 9x9
Capacity	Min	7780	75708	7811
	Max	75074	7728	76380
	Mean	41426	41509	41511

Table 1.b

Entropy 7x7				
		Std 5x5	Std 7x7	Std 9x9
Capacity	Min	7824	7715	7800
	Max	77631	77834	78164
	mean	41515	41723	41760

Table 1.c

Entropy 9x9				
		Std 5x5	Std 7x7	Std 9x9
Capacity	Min	7961	7903	7415
	Max	78792	78309	77672
	Mean	41470	41647	41909

3.1.2 Texture Analysis

Standard deviation (std) is also recognized as a strong measure in the evaluation of texture in image processing. The std filter calculates local complexity defined by the pattern of pixel intensities within a specified window. In contrast, regions with more noticeable texture have higher standard deviation values and, as a result, show a high degree of pixel contrast (Miles et al., 2013). The standard deviation providing feature makes it easy to distinguish between textured and smooth areas. When used in combination with gradient-based edge detectors, the standard filter can greatly increase edge response (Miles et al., 2013). which is as follows:

σ is the standard deviation, where x_i represents

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x_i - x)^2}{n}} \qquad (2)$$

each pixel value, x is the mean pixel value, and n is the total number of pixels. High standard deviation regions are good for embedding, as they are less sensitive to minor pixel modifications. These visually complex regions naturally hide embedded data, improving imperceptibility and reducing the risk of visual or statistical detection (Lou et al., 2010). Based on experimental evaluation Table 1, we found that a 5×5 blocking std filter has a higher capacity than the other blocking sizes.

3.1.3 Edge Detection

edge detection methods detect rapid changes in intensity, which are frequently signs of object boundaries (Xie, 2008). Image steganography utilizes such types of detection since it can identify regions with strong local contrasts, or edges, that can be used to hide data without causing noticeable visual distortions. The ability of the Canny edge detector (Canny, 1986) is to identify real edges with a minimal amount of error. The Canny algorithm is still an essential component in areas where edge localization accuracy is crucial. It is made possible to localize the edge features with high accuracy with removing noise (Kaur and Kaur, 2016). One of the efficient methods of identifying the edges is the Sobel edge detector. Its greatest strength is that it can minimize the random noise besides enhancing edge contrast (Jin-Yu et al., 2009). Even though it is not that detailed as Canny in edge localization, it is very effective in determining edge direction and this is why it is a valuable tool in determining sharp edges. A hybrid that is a combination of Canny and Sobel edge detectors has been suggested. This combination could make the region choice more resilient and create more edges that can be found. Canny gives accurate and finer edge localization whereas Sobel gives larger gradient-based edge detection map. This makes it possible to conceal more data without losing invisibility and gives the edge map as an entire and safer embedding region (Setiadi and Jumanto, 2018)

3.2. Embedding Steps

The first step in embedding is converting the cover image into grayscale, which is then followed by the edge detection of the image by using two edge detectors, Canny and Sobel. The resulting binary edge maps are then combined with the logical OR operator to ensure maximum edge pixel extraction. To further analysis the complexity of the texture, the cover image is filtered with an entropy filter, that separates the areas that are noisy or unpredictable, and a standard deviation filter, that highlights areas that have a high local intensity variation. To identify the final region of interest (ROI), a logical OR operation on the edge and texture maps and then use adaptive thresholding on that map. This hybrid ROI is then a second 15x15 entropy filter applied, and standard deviation analysis follows to select only the regions with the highest standard deviation and entropy. The algorithm then selects a maximum of n high-scoring regions that connected pixel capacity is enough to carry the entire message of length. The secret message is lastly converted into a binary stream and embedded in the least significant bits (LSB) of the chosen pixels.

3.3. Extraction process

Instead of regenerating the region-of-interest (ROI) by edge detection, the receiver needs to know the region indices to which the secret data has been embedded in order to successfully extract the secret data. The pixel modification that occurred during the embedding process is the reason whether the stego image's edge structure differs from that of the original cover image. As a result, applying edge and texture detection directly to the stego image would produce different results and incomplete or incorrect data extraction. Using one of the methods mentioned in (Rashid and Majeed, 2019) to ensure accurate embedded bit recovery. The Bit Error Rate (BER) is reduced to zero, and the hidden message can be recovered with 100% accuracy if the correct embedding indices are used during extraction.

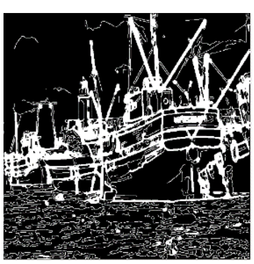
4. Experimental setup and Results

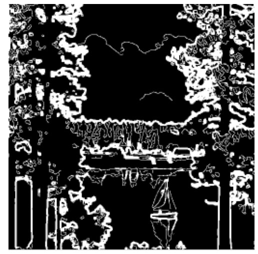
To evaluate the performance of the proposed method in comparison to the studies by Bai et al (Bai et al., 2017), Setiadi(Setiadi, 2022), Sultana et al.(Sultana and Kamal, 2021), and Setiadi et al. (Setiadi and Jumanto, 2018) we subdivided the experimental setup as follows:

4.1 Dataset

A dataset of images and 12 commonly used images were chosen as illustrated in Fig. 3. We used the standard image dataset for all of our primary experiments. The dataset named as BOSS dataset and include 10,000 images. We convert them into a grayscale image and resize them to 512x512. Once the ROI has been determined, we used regionprops() function in MATLAB to analyze and extract properties of labeled image regions, in order to separate each region from the others. We also used a set of twelve grayscale images to test the hybrid Canny-Sobel detector on cover images. Table 2 provides a summary of the binary edge maps that were produced. The combined advantages of each part allow the hybrid edge detector and fusion map to maintain dependable edge detection. We found that proposed method gets higher capacity than hybridized edge detectors such as canny and Sobel. We used a combined region-of-interest (ROI) map. Figure 3.b explains the process of choosing the most textured area to embed secret data into 12 different image covers. As an example, after determining the ROI of the baboon image, we have504 distinct regions. These regions are then sorted according to the std of their entropy of cover image regions, and in order to embed 50,000 bits, we require 91 different regions.

Table 2 presents edge detection results for twelve cover images, comparing: (1) our proposed method, which additionally generates regions of interest (ROI), and (2) a hybrid Sobel-Canny edge detector. The table demonstrates the visual output of both approaches.

image	ROI(proposed)	Edge detectors	image	ROI(proposed)	Edge detectors
Baboon	 79238	 53698	MilkDrop	 45915	 19916
Barbara	 66770	 35255	Car	 59132	 32590
Boat	 62009	 34954	Peppers	 52281	 20606

F16			Lake		
	56070	24379		57889	28041
Goldhill			bridge		
	58389	36761		68638	44823
Living room			Lenna		
	60505	30839		55524	25173

4.2 Measurements

The proposed method is analyzed based on three fundamental measurements capacity, imperceptibility, and robustness against steganalysis. Table 3 summarizes the number of edge and textured pixels that were found in twelve chosen sample images by different methods. The other method uses n-bits cleared LSBs, which embeds a secret message in edge and non-edge such as smooth areas, but our method only embeds in regions with textured and edge regions. The performance of four current methods and the suggested method as a matter of embedding capacity on twelve standard 512 x 512 test images was evaluated, as a result, the outcome completely demonstrates that our method achieves roughly 2 to 2.5 times more numbers of pixels in ROI than (Bai et al., 2017), (Setiadi, 2022). We tested the proposed method with four different payload capacities, 2048, 4096, 8192, and 16384 bits.

Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index Measure (SSIM) were used to evaluate the imperceptibility of the stego images. The results of calculating the PSNR and MSE values are presented in Tables 4 and 5. The results of the SSIM calculation are 1.00 for all different payloads. Additionally, we apply proposed method to 10,000 images in BossBase 1.01, the results are displayed in Table 6.

The robustness of the proposed method was evaluated against both visual and statistical attacks using several analytical metrics. First, the difference between standard deviations was calculated based on the cover image, sigma c and the stego image, sigma s, and the findings displayed in Figure 4 revealed that there is no significant distortion in visual representation.

$$\sigma_d = \sigma_c - \sigma_s \qquad (3)$$

where σ_c and σ_s are the standard deviations of the cover and stego images. The correlation coefficient (ρ_{SC}) between the two images, as shown in Figure 5, indicated a strong positive relation, which indicated a high identity of structure. In Figures 6 and 7 a pixel-difference histogram (PDH) analysis was recorded to determine restricted pixel-level perturbations as a mark of the invisibility of the embedding operation. Finally, the measure of statistical detectability, which is defined as a Chi-Square test, was used. The calculation of the Chi-Square value χ_{DF}^2 is done as:

$$\mathrm{X}_{DF}^2 = \frac{\sum(S_i - C_i)^2}{C_i} \qquad (4)$$

C_i and S_i are the frequency counts of pixel intensities in the cover and stego images, respectively is the degrees of freedom, calculated as:

$$DF=(h-1)\times(w-1) \qquad (5)$$

With h and w being the height and width of the images respectively.

The statistical results shown in Figure 8 indicate that the difference between the cover and stego images are not statistically significant. Together, these quantitative findings bring the effectiveness and robustness of the suggested method both visually and statistically.

The suggested content-adaptive steganographic technique shows better results in comparison to the known techniques by Bai et al. (2019) and Setiadi(Setiadi, 2022), and Setiadi et al. (Setiadi and Jumanto, 2018), particularly in the aspects of imperceptibility, the low distortion, and the possibility to scale. Unlike old methods, it inserts data only in areas of high complexity which are determined through entropy, texture and edge characteristics and thus reduces visual impairment.

The proposed content-adaptive steganographic method shows better results in comparison to the known techniques by Bai et al. Setiadi(Setiadi, 2022), and Setiadi et al. (Setiadi and Jumanto, 2018), mostly in the characteristics of imperceptibility and low distortion. Different from other methods, it embeds a secret message only in areas of high complexity which are determined through entropy, texture and edge characteristics. This superiority is realized in the advantage of the proposed method over all other payloads in the peak signal-to-noise ratio (PSNR) with the best being 75.23 dB and still high 63.18 dB with 16,384 bits payload as shown in Table7. HiGAN (Zhu et al., 2024)and HiGAN (Zhu et al., 2024)are two recent neural network-based models that achieve high robustness. However, they need a lot of computing resources and training data. The proposed hybrid method, on the other hand, provides PSNR and SSIM scores that are competitive with less complexity and better visibility. Otherwise, compared to the method of Bai et al., their approach degrades under increased payloads due to overflow, the values of mean-squared-error (MSE) in Table 7 are low. The results indicate that, compared to the reference methods, the proposed method significantly increased imperceptibility, the proposed method uses the texture-rich and edge areas to ensure high embedding rates throughout, even though other techniques based on edge-only methods are unable to detect information in images with little edge content. The MSE values, which are low through all tests, support the PSNR values, which are higher than 63 dB even at the maximum payload of 16,384 bits, indicating minimal visual distortion. The strength of the stego images is indicated by SSIM scores close to 1.0, and correlation coefficients and pixel-difference histogram analysis show that there are small modifications that the human visual system can detect. Also, the Chi-square analysis results show that there is no significant difference in the distribution of pixel intensities, which is an important signal of high resistance to statistical steganalysis. These results show that the suggested ROI selection method, which combines edge detection, entropy, and standard deviation, successfully maintains a balance between robustness, capacity, and imperceptibility while avoiding the low-capacity problem that has been determined earlier in edge-based schemes.

Table 3 Statistics of the number of pixels in ROI

Images 512x512	methods				
	proposed	Bai et al. (Bai et al., 2017)	Setiadi etal. (Setiadi and Jumanto, 2018)	Sultana et al. (Sultana and Kamal, 2021)	Setiadi(Setiadi, 2022)
F16	**56070**	24966	69625	17640	23416
Baboon	**79238**	38383	100727	4718	34566
Boat	**62009**	26991	82727	32813	24326
Barbara	**66770**	26941	74693	6272	18521
Pepper	**52281**	25860	80497	31724	19259
Lena	**55524**	24884	75604	27664	21032
Walkbridge	**68638**	45563	123388	24133	44923
Livingroom	**60505**	35543	102571	27118	36772

Table 4 PSNR of the proposed method

Images 512x512	Payload capacity			
	1024 bits	4096 bits	8192 bits	16384 bits
F16	75.1063	69.1460	66.1117	63.2577
Baboon	75.1395	69.1817	66.1211	63.1098
Boat	75.2661	69.2929	66.2235	63.1786
Barbara	75.3178	69.2242	66.1305	63.1903
Pepper	75.1813	69.2370	66.1546	63.0703
goldhil	75.1813	69.2114	66.1472	63.2233
MilkDrop	75.3877	69.1817	66.2224	63.1648
car	75.0816	69.2370	66.1926	63.2383
lake	75.3526	69.1775	66.1441	63.1749
Lena	75.1146	69.1670	66.1284	63.1722
Walkbridge	75.3005	69.0385	66.1767	63.2631
Livingroom	75.3178	69.3408	66.1368	63.1364

Table 5 MSE of proposed Method

Images 512x512	Payload capacity			
	1024 bits	4096 bits	8192 bits	16384 bits
F16	0.0020	0.0079	0.0159	0.0307
Baboon	0.0020	0.0079	0.0159	0.0318
Boat	0.0019	0.0077	0.0155	0.0313
Barbara	0.0019	0.0078	0.0159	0.0312
Pepper	0.0020	0.0078	0.0158	0.0321
goldhil	0.0020	0.0078	0.0158	0.0314
MilkDrop	0.0019	0.0079	0.0155	0.0311
car	0.0020	0.0078	0.0156	0.0308
lake	0.0019	0.0079	0.0158	0.0313
Lena	0.0020	0.0079	0.0159	0.0313
Walkbridge	0.0019	0.0081	0.0157	0.0307
Livingroom	0.0019	0.0076	0.0158	0.0316

Table 6 PSNR, MSE, SSIM on BOSSBASE dataset

Payload capacity (bpp)	PSNR	MSE	SSIM
0.06 bpp	63.3511	0.0301	0.9999
0.12 bpp	60.3413	0.0601	0.9999
0.18 bpp	58.5805	0.0902	0.9998
0.24 bpp	57.3320	0.1202	0.9997
0.27 bpp	57.3271	0.1203	0.9997
0.30	57.3428	0.1199	0.9989

Table 7 PSNR (dB) comparison between the proposed and previous methods using the same message.

payload	Proposed	Bai et al. (Bai et al., 2017)	Setiadi etal. (Setiadi and Jumanto, 2018)	Setiadi (Setiadi, 2022)
1024 bit	75.22893	66.2163	69.2603	69.7156
4096 bit	69.20298	63.1717	66.2462	66.6396
8192 bit	66.15747	60.1287	63.2481	63.6114
16384 bit	63.18164	overflow	60.3134	60.6973

Table 8 MSE comparison between the proposed and previous methods using the same message.

payload	proposed	Bai et al. (Bai et al., 2017)	Setiadi etal. (Setiadi and Jumanto, 2018)	Setiadi (Setiadi, 2022)
1024 bit	0.00195	0.0155	0.0077	0.0070
4096 bit	0.007842	0.0313	0.0154	0.0141
8192 bit	0.015758	0.0631	0.0308	0.0283
16384 bit	0.031275	overflow	0.0605	0.0554

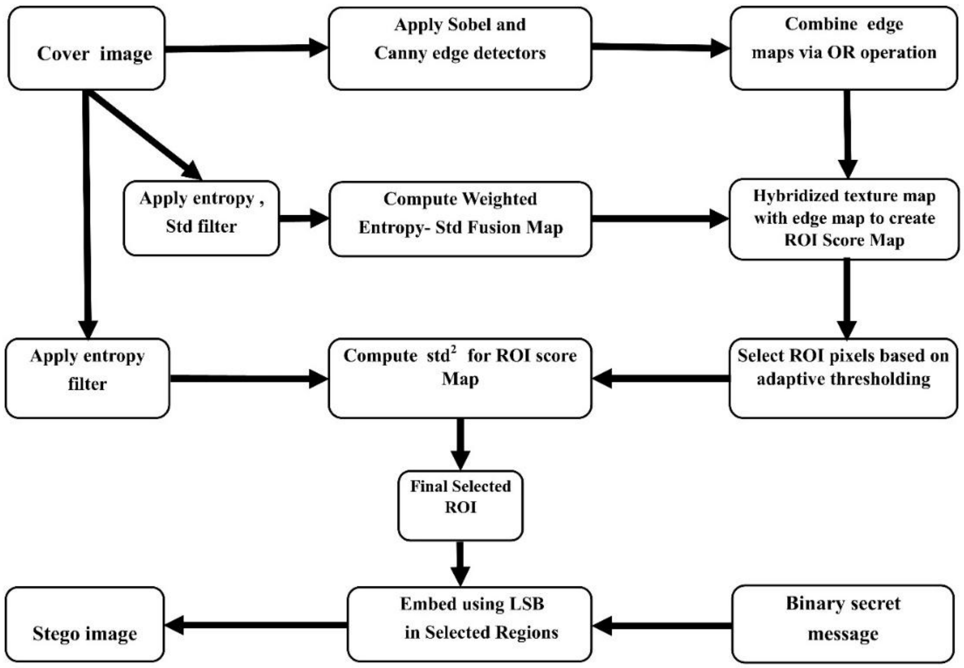


Figure 2 Proposed embedding steps

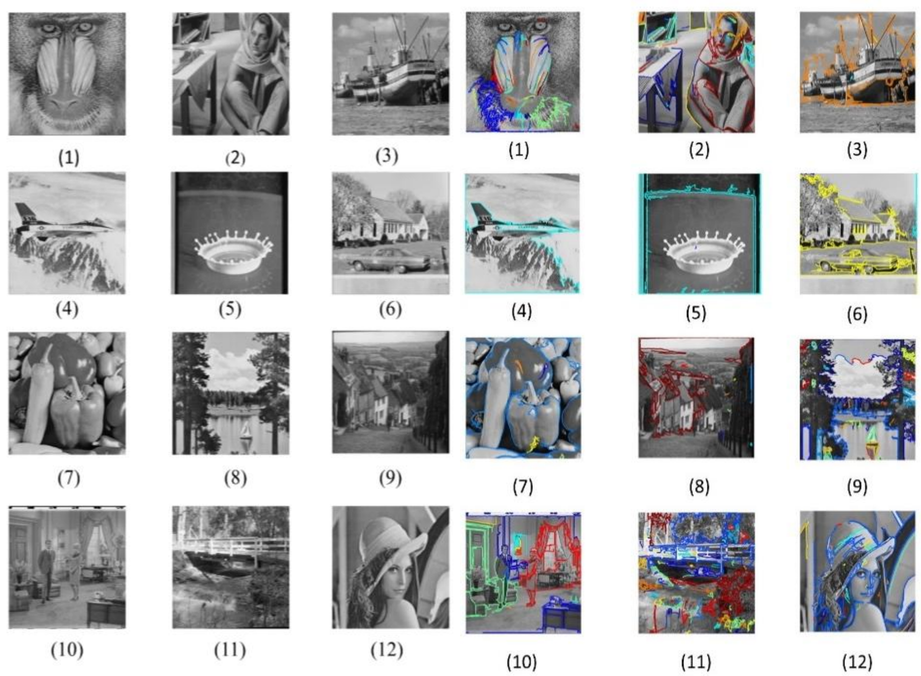


Figure3.a **Figure 3.b**

Figure 3. a The 12 benchmark images commonly used in existing studies.
Figure3.b illustrates the proposed method's adaptive region selection, highlighting its ability to prioritize areas with distinct textures and edges.

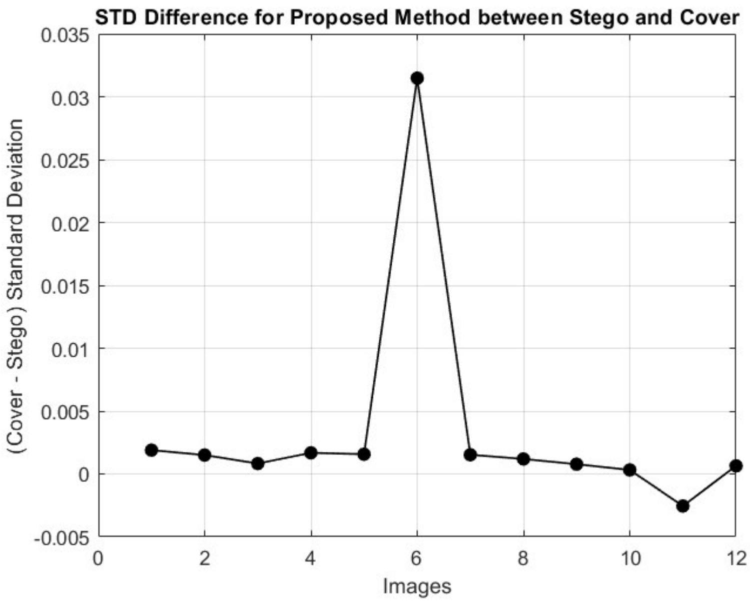


Figure 4 STD between the cover and the stego images

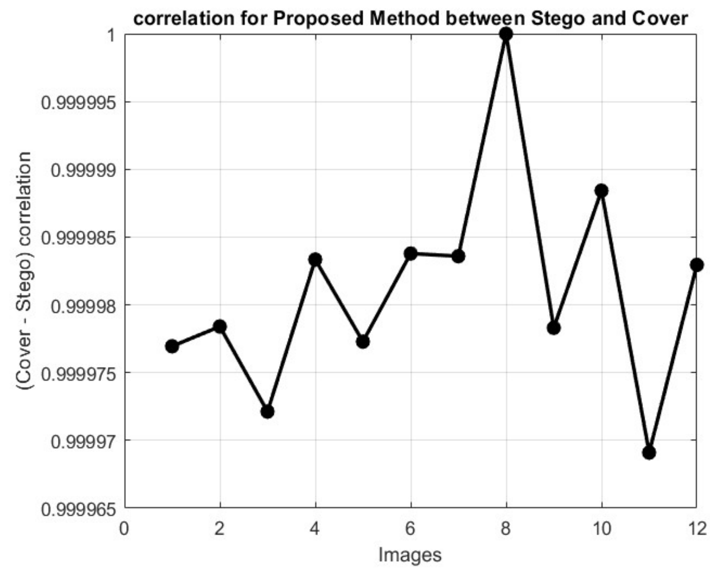


Figure 5 Correlation between the cover and the stego images

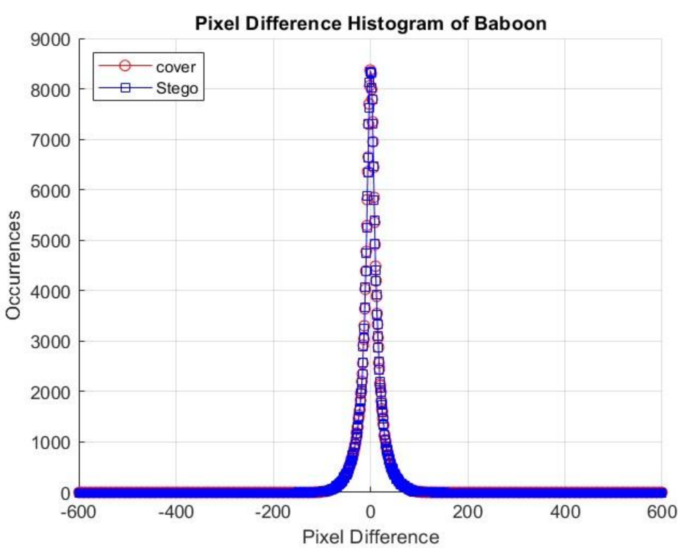


Figure 6PDH between the cover of Baboon and the stego image

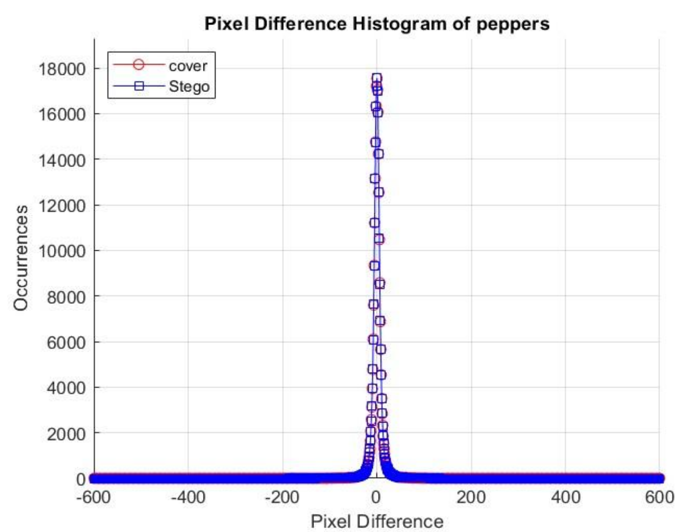


Figure 7 PDH between the cover of peppers and the stego image

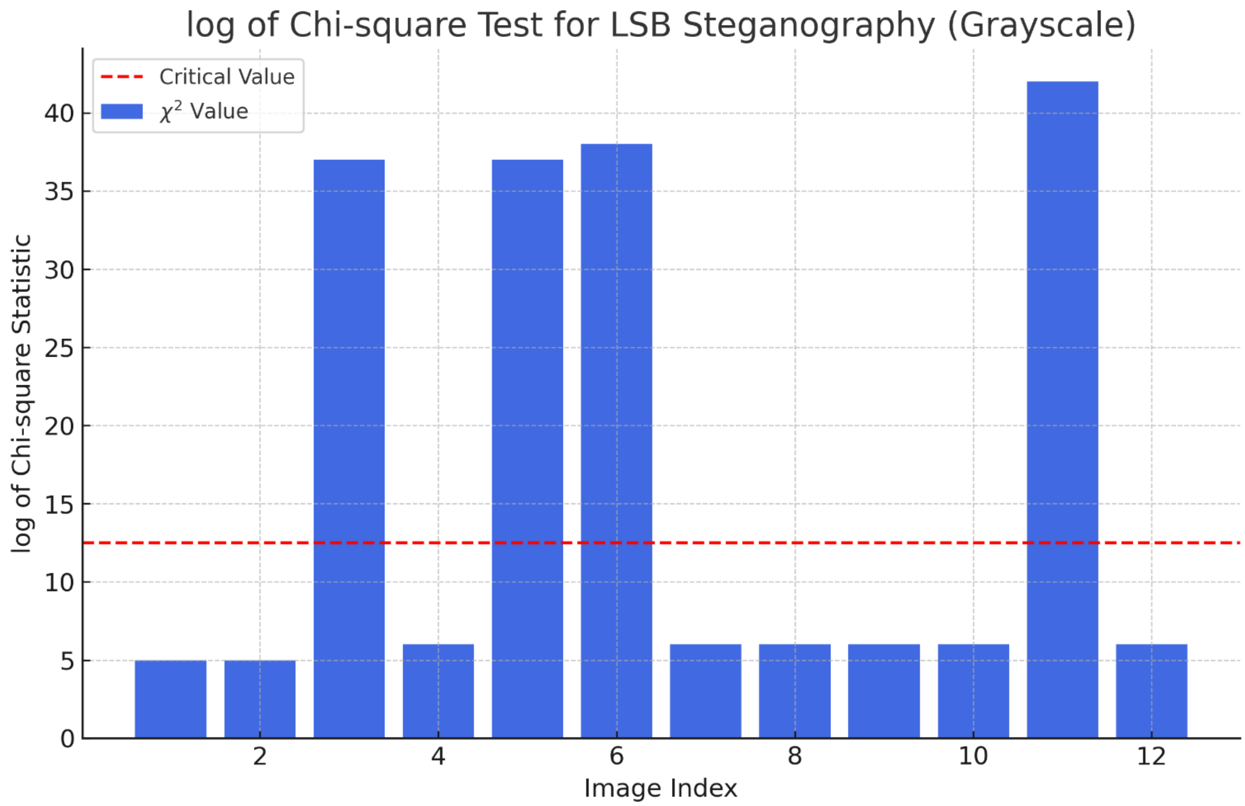


Figure 8 Chi-square for similarity between stego and cover images

5. Conclusion

This paper introduced a content adaptive approach for image steganography that combines hybrid Canny-Sobel edge detection, standard deviation analysis, and entropy filtering to determine the best regions for data embedding. By using texture-rich and edge regions and improving the selection process through statistical analysis of entropy distribution, the proposed method addresses the low-capacity problem of the other edge-based methods while maintaining imperceptibility. These results confirm the process as a scalable, secure, and invisible steganographic method that supports a range of image types and payloads. The experimental results showed that PSNR and SSIM scores were better than those of recent benchmark methods, with PSNR scores of over 63 dB even with larger payloads. This method can be useful for protecting sensitive visual data, and also to earn sending images. Future studies could apply the proposed ROI selection framework to color image steganography and apply more feature extraction methods, like deep convolutional neural networks, to more accurately identify regions and evaluate the framework's resistance to more types of active attacks, which could improve security and adaptability in real-world applications.

Acknowledgment: Authors would like to thank Salahaddin University-Erbil for their support throughout the research.

Financial support: No financial support.

Potential conflicts of interest: Authors declare no conflicts of interest relevant to this article.

Funding: This research received no external funding.

Conflict of Interest: The authors declare no conflict of interest.

6. References

Abdlrazaq, A. A., Azzez, S. N., Anwer, M. A. & Hassen, S. I. 2023. Proposed Solutions for the Main Challenges and Security Issues in IoT Smart Home Technology. *Zanco Journal of Pure and Applied Sciences,* 35**,** 84-96.

Al-Dmour, H. & Al-Ani, A. 2016. A steganography embedding method based on edge identification and XOR coding. *Expert systems with Applications,* 46**,** 293-306.

Bai, J., Chang, C.-C., Nguyen, T.-S., Zhu, C. & Liu, Y. 2017. A high payload steganographic algorithm based on edge detection. *Displays,* 46**,** 42-51.

Canny, J. 1986. A computational approach to edge detection. *IEEE Transactions on pattern analysis and machine intelligence***,** 679-698.

Halder, T., Karforma, S. & Mandal, R. 2019. A block-based adaptive data hiding approach using pixel value difference and LSB substitution to secure e-governance documents. *Journal of Information Processing Systems,* 15**,** 261-270.

Hardan, H., Khashan, O. A. & Alshinwan, M. 2025. Edge-Based Data Hiding and Extraction Algorithm to Increase Payload Capacity and Data Security.

Holub, V. & Fridrich, J. Designing steganographic distortion using directional filters. 2012 IEEE International workshop on information forensics and security (WIFS), 2012. IEEE, 234-239.

Holub, V., Fridrich, J. & Denemark, T. 2014. Universal distortion function for steganography in an arbitrary domain. *EURASIP Journal on Information Security,* 2014**,** 1-13.

Jin-Yu, Z., Yan, C. & Xian-Xiang, H. Edge detection of images based on improved Sobel operator and genetic algorithms. 2009 International Conference on Image Analysis and Signal Processing, 2009. IEEE, 31-35.

Johnson, N. F., Duric, Z. & Jajodia, S. 2001. Information hiding: Steganography and Watermarking-attacks and Countermeasures. *(No Title)*.

Kadhim, I. J., Premaratne, P., Vial, P. J. & Halloran, B. 2019. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing,* 335**,** 299-326.

Kaur, M. & Juneja, M. Adaptive block based steganographic model with dynamic block estimation with fuzzy rules. Innovations in Computer Science and Engineering: Proceedings of the Fourth ICICSE 2016, 2017. Springer, 167-176.

Kaur, P. & Kaur, B. 2-D geometric shape recognition using canny edge detection technique. 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016. IEEE, 3161-3164.

Khalind, O. S. 2019. Steganography-based password management: A conceptual model. *Zanco J. Appl. Sci,* 31**,** 61-68.

Lou, D.-C., Wu, N.-I., Wang, C.-M., Lin, Z.-H. & Tsai, C.-S. 2010. A novel adaptive steganography based on local complexity and human vision sensitivity. *Journal of Systems and Software,* 83**,** 1236-1248.

Martín, A., Hernández, A., Alazab, M., Jung, J. & Camacho, D. 2023. Evolving Generative Adversarial Networks to improve image steganography. *Expert Systems with Applications,* 222**,** 119841.

Miles, K. A., Ganeshan, B. & Hayball, M. P. 2013. CT texture analysis using the filtration-histogram method: what do the measurements mean? *Cancer Imaging,* 13**,** 400.

Mohsin, N. A. & Alameen, H. A. 2021. A hybrid method for payload enhancement in image steganography based on edge area detection. *Cybernetics and Information Technologies,* 21**,** 97-107.

Parah, S. A., Sheikh, J. A., Akhoon, J. A., Loan, N. A. & Bhat, G. M. 2018. Information hiding in edges: A high capacity information hiding technique using hybrid edge detection. *Multimedia Tools and Applications,* 77**,** 185-207.

Rashid, R. D. & Majeed, T. F. Edge based image steganography: Problems and solution. 2019 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), 2019. IEEE, 1-5.

Roy, R. & Changder, S. Image steganography with block entropy based segmentation and variable rate embedding. 2014 2nd International Conference on Business and Information Management (ICBIM), 2014. IEEE, 75-80.

Setiadi, D. R. I. M. 2022. Improved payload capacity in LSB image steganography uses dilated hybrid edge detection.

Setiadi, D. R. I. M. & Jumanto, J. 2018. An enhanced LSB-image steganography using the hybrid Canny-Sobel edge detection. *Cybernetics and information technologies,* 18**,** 74-88.

Sultana, H. & Kamal, A. Image Steganography System based on Hybrid Edge Detector. 2021 24th International Conference on Computer and Information Technology (ICCIT), 2021. IEEE, 1-6.

Sultana, H., Kamal, A., Apon, T. S. & Alam, M. G. R. 2024. Increasing embedding capacity of stego images by exploiting edge pixels in prediction error space. *Cyber Security and Applications,* 2**,** 100028.

Westfeld, A. & Pfitzmann, A. Attacks on steganographic systems: Breaking the steganographic utilities EzStego, Jsteg, Steganos, and S-Tools-and some lessons learned. International workshop on information hiding, 1999. Springer, 61-76.

Xie, X. 2008. A review of recent advances in surface defect detection using texture analysis techniques. *ELCVIA: electronic letters on computer vision and image analysis***,** 1-22.

Yang, C.-H., Weng, C.-Y., Wang, S.-J. & Sun, H.-M. 2008. Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on Information Forensics and Security,* 3**,** 488-497.

Yang, H., Sun, X. & Sun, G. 2009. A high-capacity image data hiding scheme using adaptive LSB substitution. *Radioengineering,* 18**,** 509-516.

Zeng, L., Yang, N., Li, X., Chen, A., Jing, H. & Zhang, J. 2023. Advanced Image Steganography Using a U-Net-Based Architecture with Multi-Scale Fusion and Perceptual Loss. *Electronics,* 12**,** 3808.

Zhang, K. A., Cuesta-Infante, A., Xu, L. & Veeramachaneni, K. 2019. SteganoGAN: High capacity image steganography with GANs. *arXiv preprint arXiv:1901.03892*.

Zhu, Y., Dong, Y., Song, B. & Yao, S. 2024. Hiding image into image with hybrid attention mechanism based on GANs. *IET Image Processing,* 18**,** 2679-2689.