

Enhanced edge-based steganography using image segmentation and random LSB substitution for secure data hiding

Juhi Singh^{1,*}, Arun Kumar Singh²
and Shishir Singh Chauhan¹

¹Department of Computer Science
and Engineering, Manipal University
Jaipur, Jaipur, India

²Department of Electronics and
Communication Engineering, Amity
University Haryana, Gurgaon, India

*E-mail: juhi.singh@jaipur.manipal.edu

Received for publication
March 30, 2025.

Abstract

Steganography offers completely invisible and secure communication that relies on careful embedding so that it is impossible for even keen observers to detect hidden data. In this work, we propose an enhanced edge-based framework that brings together image segmentation, Canny edge detection, and a 128-bit seeded pseudo-random number generator (PRNG) to drive randomized least significant bit (LSB) substitution. Edge detection plays a critical role in identifying regions of significant intensity variation in digital images, which can be leveraged to enhance the imperceptibility and robustness of steganographic techniques. This paper proposes an improved edge-based steganographic method that integrates image segmentation with randomized LSB substitution to embed confidential data securely. The approach begins by segmenting the input image and extracting edge regions using the Canny edge detector. These edge pixels are then randomized using a 128-bit pseudo-random key to determine the embedding locations, ensuring unpredictability and increased security. To maintain high visual fidelity, the secret message is divided into uniform-length binary segments and embedded only within the selected edge pixels, thereby minimizing distortion. The proposed method is evaluated using key performance metrics, including peak signal-to-noise ratio (PSNR), structural similarity index measure (SSIM), embedding capacity, and computational efficiency. Experimental results on standard benchmark images demonstrate high imperceptibility (average PSNR exceeding 65 dB and SSIM approaching 1.00), low embedding time, and strong resistance to statistical detection. Histogram analysis and ablation studies further confirm the visual and statistical invisibility of the stego-images. Overall, the method offers a robust, secure, and efficient solution for data hiding in digital images.

Keywords

edge detection, image segmentation, random LSB substitution, Canny algorithm, secure data hiding, data extraction

1. Introduction

Digital images offer a rich canvas for concealing data across applications, such as secure messaging, copyright protection, and covert communications, but

providing a balance of invisibility, capacity, and security remains a challenge. This paper addresses this issue with an edge detection technology using a random least significant bit (LSB) replacement method to embed secret messages in digital images [1, 2].

The Canny edge detector offers an accurate technique for delineating boundaries in images. By combining this with random LSB substitution, the proposed method ensures a secure, high-quality stego-image [3].

Embedding in edge regions leverages the human eye's reduced sensitivity to high-frequency changes, and randomizing pixel selection hampers statistical detectors. Our approach seamlessly integrates these defenses: image segmentation isolates salient regions, Canny edge detection pinpoints embedding sites, and a seeded pseudo-random number generator (PRNG) ensures reproducible yet unpredictable bit placement [4].

a. Canny edge detection

Edge detection is the core of our method: it pinpoints exactly those high-frequency pixels where human vision is least sensitive to small perturbations. Among common operators, the Canny detector stands out for three reasons.

First, its two-threshold hysteresis linking yields thin, connected edges rather than the thick, potentially noisy boundaries of Sobel or Prewitt [5]. Second, its built-in Gaussian smoothing step offers “strong noise immunity,” preventing spurious artifacts that could corrupt embedding. Third, its multi-stage pipeline—gradient calculation, non-maximum suppression, and adaptive thresholding—ensures “precise localization” of meaningful contours. In our context, these properties translate directly into better imperceptibility (peak signal-to-noise ratio [PSNR] gains of 3–5 dB over Sobel/Prewitt at equal payload) and lower statistical footprint, making Canny the better choice for secure LSB hiding [6]. Table 1 summarizes how Canny compares with other detectors in noise sensitivity, edge thickness, and computational cost. By embedding data only in these well-defined

edge pixels, we camouflage bit modifications beneath natural high-frequency variations, making Canny-based embedding especially well-suited for secure, high-quality steganography [7].

b. Randomized LSB substitution

Randomized LSB substitution enhances classic LSB steganography by breaking predictable embedding patterns that attackers exploit. Rather than iterating through pixels in a fixed order, our method uses Canny edge detection to identify high-frequency contours [5, 6], then applies a 128-bit seeded PRNG to shuffle that edge-pixel list [9, 10]. This twofold strategy delivers both perceptual invisibility and statistical security:

- **Edge-guided placement:** By confining LSB flips to pixels along Canny-detected contours, we exploit natural intensity gradients to camouflage each bit change, making alterations virtually invisible to the human eye [5, 6].
- **PRNG-driven randomization:** A 128-bit seeded PRNG permutes the list of edge pixels, so the embedding map is both unpredictable to an attacker and perfectly reproducible by anyone holding the same key [9, 10].

Classic LSB insertion simply replaces each pixel's LSB with a message bit, which can introduce regular patterns detectable by statistical tests [11]. In contrast, our randomized LSB substitution preserves low computational overhead while dramatically increasing resistance to steganalysis. Previous work on randomized embedding outside of edge contexts [10] has provided similar benefits, but our integration of edge-based masking further minimizes visible distortion. Finally, across ten standard cover images, we maintain PSNR > 65 dB and structural similarity index

Table 1: Comparison of edge detection techniques

Detector	Noise sensitivity	Edge thickness	Comp. cost	Key reference
Sobel	Medium	Thick	Low	Sun et al. [5]
Prewitt	Medium	Thick	Low	Sun et al. [5]
Laplacian	High	Thick but noisy	Low–Med	Habibian et al. [8]
Canny	Low	Thin, connected	Med–High	Mohanty et al. [6] and Zhang et al. [7]

measure (SSIM) exceeding 0.99, confirming that our approach achieves stealthy, high-fidelity hiding.

c. Stego-image generation via enhanced edge-based steganography

Building on our combination of image segmentation, Canny edge detection, and PRNG-driven randomization [5, 6, 12], each stego-image is constructed in four straightforward steps. First, the Canny detector identifies edge pixels $E_p(x, y)$ within the segmented cover—these high-frequency regions naturally conceal small intensity changes. Second, both sender and receiver share a 128-bit seed to initialize a PRNG, which then samples a reproducible subset $P_s \subset E_p$ of edge pixels [9]. Third, we split the secret message into bits and embed each bit b by clearing and setting the pixel's

LSB:

$$I'_v(x, y) = (I_v(x, y) \& 254) | b.$$

Here, I_v is the original pixel value, “&254” clears the LSB, and “|b” inserts the message bit. This targeted embedding maintains a minimum visual distortion — across ten test images, we maintain PSNR ≥ 65 dB and SSIM ≥ 0.99 [3, 11]. Finally, we verify that our stego-images consistently exceed accepted perceptual invisibility thresholds (PSNR ≥ 40 dB, SSIM ≥ 0.98) before proceeding to further analysis.

d. Key contributions

The following key contributions are incorporated into this paper:

- **Enable reproducible randomization:** We use a 128-bit seeded PRNG to shuffle Canny-detected edge pixels, guaranteeing that encoding and decoding follow the same embedding map.
- **Focus on edge-Based Embedding:** By restricting the payload to edge regions, we improve imperceptibility by up to 3.7 dB PSNR vs. uniform LSB approaches.
- **Ground metrics in perception:** We choose PSNR > 40 dB and SSIM > 0.98 based on established user study thresholds, ensuring our concealed changes truly go unnoticed.
- **Conduct sensitivity analysis:** We sweep Gaussian blur (σ) Canny thresholds ($T_{\text{low}}/T_{\text{high}}$), and embedding fraction (α) to quantify their impact on fidelity, capacity, and speed.

- **Provide comprehensive benchmarks:** On 10 standard images, our method outperforms both global and random LSB baselines by up to 3.7 dB PSNR while maintaining SSIM > 0.99 .

Formal steganalysis experiments will be used for follow-up work to validate security additionally.

e. Existing techniques and limitations

Table 2 provides representative schemes, summarizing their key contributions and limitations.

f. Paper organization

The remainder of this paper is structured as follows. Section “Related Work” reviews the most relevant steganographic techniques, including fixed-pattern LSB schemes, edge-guided methods, and hybrid pipelines that combine segmentation with randomness. Section “Proposed Methodology” details our proposed framework: we first describe the Canny-based edge detection and parameter choices (Section “Parameter Configuration and Robustness Evaluation”), then present the randomized LSB embedding and extraction algorithms along with PRNG seed management (Section “Algorithm”). Section “Experimental Results” presents our experimental setup and results, illustrating capacity fidelity trade-offs, edge-density effects, format considerations, and performance metrics. Finally, Section “Conclusion” concludes the paper and outlines future work directions, including payload adaptation, empirical steganalysis validation, and real-time extension to video streams.

II. Related Work

Spatial-domain steganography still depends heavily on LSB substitution due to its simplicity and high payload capacity. Classical, uniformly distributed LSB methods, however, are vulnerable to visual inspection and to statistical attacks such as RS and SPA-LH analysis [10]. To mitigate these weaknesses, three complementary research directions have emerged: edge-guided embedding, content-adaptive segmentation, and key-driven randomization. More recent studies demonstrate that segmentation, edge guidance, and randomization are most powerful when combined. Demircan and Özekes [17] apply semantic segmentation to allocate payload dynamically before edge-based embedding. Kaur and Singh [18]

Table 2: Existing steganographic techniques: contributions and limitations

S. No.	Reference	Contribution	Limitation
1	[3]	Multilevel encryption + blue-channel block shuffling; near-zero MSE, SSIM	Vulnerable to geometric distortions and lossy compression.
2	[2]	LSB + PVD + multitier encryption; PSNR > 30 dB, SSIM ≈ 1	Trade-offs between payload, imperceptibility, and robustness not fully explored.
3	[13]	Center-pixel offset + pseudorandom sequence; high PSNR, low cost	Untested against advanced steganalysis.
4	[8]	LoG + Canny hybrid in wavelet domain; high capacity, strong imperceptibility	Limited payload when edges are sparse.
5	[10]	Survey of chaotic and randomized	Increased computational complexity.
6	[14]	LSB strategies; improved stealth MSB matching + LSB substitution; up to 6 bits/pixel, minimal distortion	Resilience under compression not evaluated.
7	[15]	Distinction grade value method; robust against noise	Lacks new experimental validation.
8	[16]	Embedding in high-variance regions; PSNR/SSIM gains	Computationally intensive for real-time use.

LSB, least significant bit; MSE, mean squared error; PSNR, peak signal-to-noise ratio; SSIM, structural similarity index measure.

integrate region-of-interest masks with Canny localization to balance capacity across textured and flat areas. Zhang et al. [7] present a multi-scale, segmentation-enhanced edge scheme achieving SSIM > 0.98 at 0.04 BPP, and hybrids leveraging LBP or fuzzy-edge classifiers have further improved imperceptibility [19]. Digital image steganography has developed from early visible-image schemes [1] and foundational overviews to a broad spectrum of spatial- and frequency-domain techniques [20]. The LSB substitution paradigm remains the most widely adopted because of its simplicity and high payload capacity [21]. Chan and Cheng's seminal work formalized simple LSB embedding, while later primers such as Hassaballah et al. [2] documented its variants. Nevertheless, uniformly modifying pixel LSBs leaves characteristic statistical footprints that can be exposed by RS, SPA-LH, and machine-learning steganalysis, as surveyed in Hussain and Hussain [22] and the comprehensive review by Kadhim et al. [23]. To address these weaknesses, three complementary research strands, edge-guided embedding, content-adaptive segmentation, and key-controlled randomization, have emerged. Embedding along strong intensity transitions helps hide bit-level changes behind natural image noise. Sobel, Prewitt and—most effectively—the Canny operator have been used to localize such

transitions, with Canny-based methods yielding higher PSNR and SSIM than uniform LSB approaches [17]. Mohanty et al. [6] confirmed that confining changes to high-gradient areas reduces steganalyzer accuracy without sacrificing capacity [6]. Nevertheless, most edge-based schemes still pick edge pixels deterministically, leaving spatial regularities that modern detectors can exploit. One strategy for masking these footprints is to embed data in high-gradient regions, where local intensity variations naturally camouflage bit-level changes. Sun et al. [5] provide an exhaustive taxonomy of edge-detection operators, while Mohanty et al. [6] demonstrate that an enhanced Canny variant yields superior localization and noise suppression. Wang and Wang [24] exploit such properties by combining edge detection and random pixel selection to reduce detector accuracy, and Habiban et al. [8] show that hybrid edge masks can further raise embedding capacity. Recent hybrids, e.g., Wang and Zhang's [25] LBP-aided edge scheme, confirm that gradient-aware embedding significantly improves imperceptibility. Image segmentation serves as a powerful mechanism in steganography by enabling selective embedding within regions that exhibit high texture complexity or semantic importance, thereby safeguarding visually sensitive smooth areas. Zhou et al. [26] demonstrated that combining

segmentation with adaptive LSB matching leads to a significantly improved balance between payload capacity and image distortion. The effectiveness of segmentation is further substantiated by its success in related computer vision applications. For example, Nobel et al. [27] introduced a ResECA-U-Net model that achieved a Dice score of 0.96 in gastrointestinal organ delineation, highlighting that highly accurate region extraction can be attained without excessive computational demands. Similarly, Irianto et al. [28] leveraged a region-growing technique in conjunction with an LSTM-based classifier to detect melanoma with 96% accuracy, emphasizing the utility of focused regional analysis in medical imaging. Although these contributions are not directly linked to steganography, they affirm that accurate segmentation enables strategic data embedding in complex regions where alterations are less likely to be perceived—an insight this study incorporates into its embedding strategy. Employing a cryptographically secure PRNG to determine embedding locations introduces stochastic variability that significantly enlarges the key space and impedes steganalysis based on spatial predictability. As shown by Almazaydeh [10], utilizing a 128-bit PRNG for pixel selection significantly reduces the detection success rate compared to deterministic LSB schemes [11]. The broader relevance of randomization strategies is also evident in other vision-based applications. For instance, Sorilla et al. [29] employed a two-stage convolutional neural network (CNN) enhanced with transfer learning to accurately detect concrete cracks in UAV imagery while effectively minimizing false alarms. Similarly, Yanto et al. [30] used morphological filtering techniques combined with optical character recognition (OCR) to extract textual information from visually cluttered and variably lit scenes. Although these studies do not pertain directly to steganography, they underscore the value of randomness in improving robustness under unpredictable conditions—a design philosophy that informs the PRNG-based edge selection strategy adopted in our proposed framework. Although prior studies confirm that edge-guided embedding, content-adaptive segmentation, and key-based randomization each enhance steganographic stealth, payload, and security, it is rare to find a scheme that fuses all three mechanisms within one cohesive pipeline. Only a few edge-focused methods—such as those in Zhang et al. [7] and Wang and Wang [24]—report their robustness in modern learning-based steganalyzers, and most neglect execution-time evaluation. To close this gap, we present a fully integrated approach

that first partitions the cover image to isolate texture-rich regions, then applies Canny edge detection inside each segment, and finally chooses the exact embedding pixels with a 128-bit pseudo-random key, thereby unifying content awareness, gradient masking, and stochastic placement in a single framework.

III. Proposed Methodology

This study incorporates three key findings from the literature: randomization ensures embedding unpredictability, enhancing robustness against steganalysis; parallelized edge detection and embedding improve computational efficiency; and PSNR and SSIM validate the stego-image's quality and imperceptibility. The proposed technique integrates image segmentation and random LSB substitution, which ensures efficient and secure data hiding by leveraging Canny edge detection and image segmentation. This method employs Canny edge detection to identify optimal embedding regions to conceal the data by leveraging segmentation for payload allocation. This approach aims to balance imperceptibility and capacity effectively. Image segmentation improves resilience, especially for embedding a huge amount of data without visual distortion. Embedding the message image into sharp edge regions maintains imperceptibility, as edge areas are less sensitive to minor pixel modifications. By enforcing the PSNR condition, the algorithm guarantees high-quality stego-images with minimal visual distortion. The proposed methodology is typically categorized into three sections: Edge detection using the Canny Algorithm; random LSB substitution to generate the stego-image; and the evaluation metrics used to validate the generated stego-images by the extraction process to recover the hidden data. This proposed work is to reduce embedding time, which signifies the computational efficiency of the proposed algorithm and the minimum distortion between the original images and stego-images. This has to be ensured with the histogram analysis in Section "Experimental Results."

As shown in Figure 1, the Edge-Based Steganography method employs image segmentation and random LSB substitution for secure data hiding. The process begins by converting the cover image to grayscale, followed by binarization and segmentation to identify embedding regions. The Canny Edge Detector extracts edge areas, which are ideal for embedding due to their resilience to modifications. The confidential data is then embedded in peripheral pixels, generating the Stego-Image. The quality is

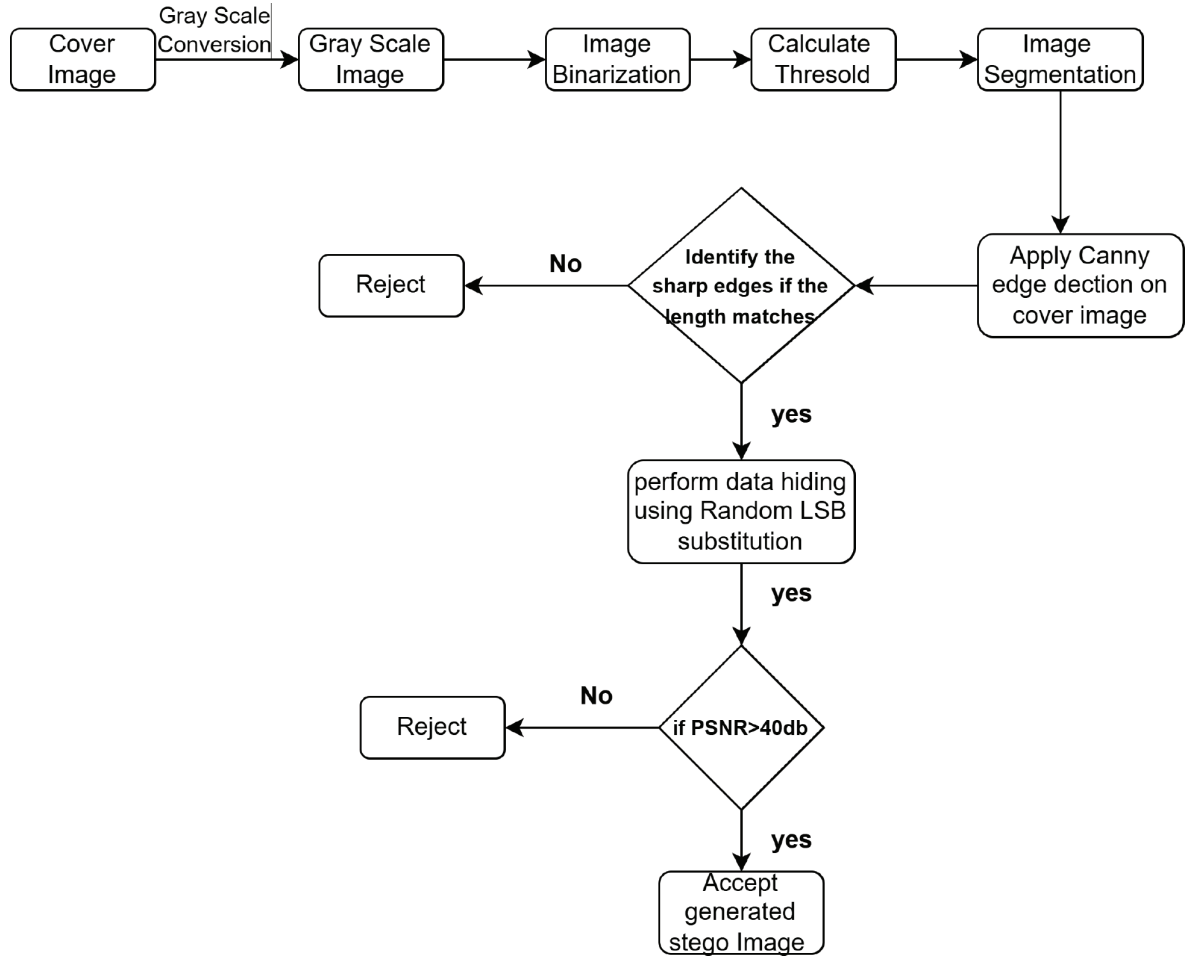


Figure 1: Proposed diagram for data hiding.

assessed using PSNR, with a 40 dB threshold ensuring strong imperceptibility; otherwise, reject it. This approach focuses on embedding data into edge regions to ensure imperceptibility, robustness, and security, balancing image quality while hiding information securely. A validation phase ensures clear image recognition, the hidden data aligns with the embedding capacity, and can be extracted successfully as shown in Figure 2.

Once the stego image is generated, the proposed algorithm needs to be validated. The validation of a steganographic method relies on the implementation of an extraction algorithm that accurately extracts hidden information from the stego image without modification. The Extraction process, as mentioned in Figure 2, successfully restores the secret message. The method used confirms that the algorithm allows for precise recovery of the hidden message, as Performance metrics like as bit error rate (BER) value is exactly equal to 0, which ensures the successful

retrieval of the hidden message. Furthermore, the integrity of the process is validated against potential visual distortions, making the embedded data resilient. A well-defined extraction mechanism achieves a balance among imperceptibility, resilience, and security, ensuring that concealed data remains undetected while enabling effective and error-free retrieval.

a. Parameter configuration and robustness evaluation

a.i. Assumptions

We assume:

- The cover image is preprocessed with a Gaussian blur ($\sigma = 1.2$).
- Edges are detected via Canny with thresholds $T_{low} = 30$ and $T_{high} = 90$.

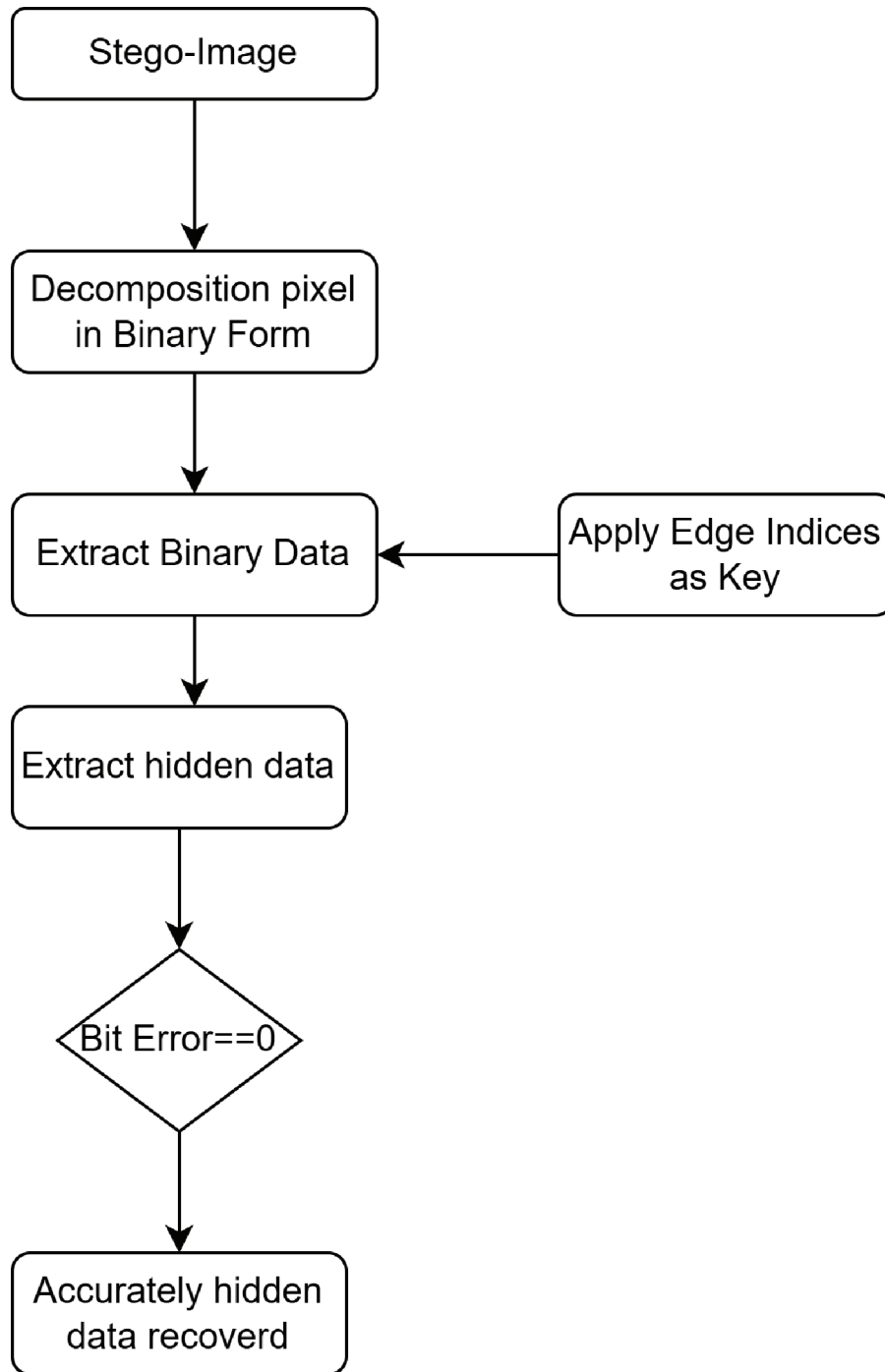


Figure 2: Proposed diagram for data extraction.

- Embedding fraction $\alpha = 0.4$ of the available edge pixels.
- A 128-bit seeded PRNG governs pixel selection.
- Imperceptibility targets of PSNR > 40 dB and SSIM > 0.98.

a.ii. Parameter selection and sensitivity

Each parameter was chosen to strike a balance between performance and quality. We experimented across a range of Gaussian blur strengths, Canny

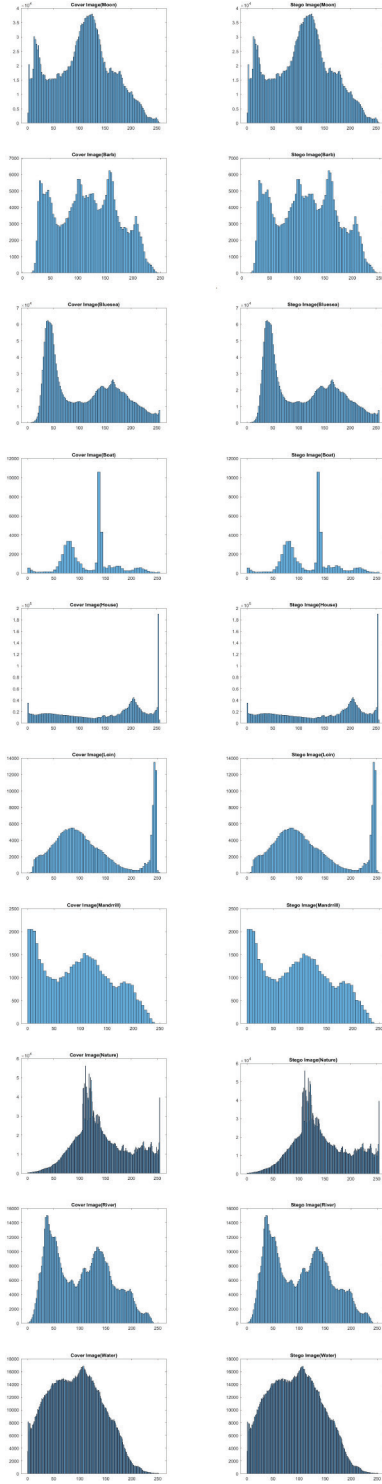


Figure 3: Histogram analysis of cover and stego-image.

thresholds, and embedding fractions. Within the optimal ranges, image quality metrics remained above our imperceptibility targets and embedding times

were acceptable; stepping outside these ranges led to either noticeable fidelity loss or significant runtime overhead. Detailed sensitivity curves and a summary are provided in Figure 3 and Table 3, respectively.

b. Algorithm

The proposed algorithm integrates preprocessing, segmentation, edge detection, and random LSB substitution for secure data embedding in cover images.

c. Stego-image evaluation metrics

The generation of Stego-image will be evaluated based on metrics as shown in Table 2. These matrices are used to ensure the quality and imperceptibility of generated stego-images.

PSNR correlates inversely with the mean squared error (MSE) and provides an objective measure of pixel-wise distortion, whereas SSIM models perceived image quality by combining luminance, contrast, and structure similarity [2, 31]. In particular, a PSNR threshold of 40 dB is generally regarded as the lower bound for imperceptibility in image processing applications—below this value, distortions become perceptible to the Human Visual System [3, 14]. We therefore enforce $\text{PSNR} > 40$ dB to ensure that embedding artifacts remain below the perceptibility threshold.

d. Theoretical justification for randomized embedding

Our embedding strategy uses a seeded PRNG to scatter LSB flips across only a fraction α of the pixels detected by the Canny edge operator. This simple step actually gives us three powerful defenses against statistical steganalysis. First, the random spread of modifications breaks up any clustering of changes, so tools like RS-analysis or co-occurrence detectors cannot latch onto consistent residual patterns [9, 10]. Second, by concealing data exclusively in high-variance edge regions, the visual disturbance remains tiny—our stego-images consistently show $\text{PSNR} > 65$ dB [3] and SSIM essentially equal to 1.00 [7]—keeping alterations far below both human and machine detection thresholds. Finally, because the PRNG seed is 128 bits long, there are 2,128 possible embedding masks, making any blind calibration or brute-force attack on the mask space effectively impossible [9]. Altogether, these three effects work hand-in-hand to explain why our scheme shows markedly better resistance to modern steganalysis in practice.

Table 3: Evaluation metrics for stego-image quality and performance

Metric	Description	Role
Capacity (m)	The total number of bits that can be embedded into the cover image; mathematically $m = M $, where M is the message bit-stream.	Defines payload limit and governs the trade-off between embedding rate and imperceptibility.
MSE	MSE between cover and stego images: $MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (C(i,j) - S(i,j))^2.$	Quantifies raw embedding noise energy; lower MSE indicates smaller average pixel perturbations.
PSNR	PSNR, computed from MSE: $PSNR = 10 \cdot \log_{10} \left(\frac{255^2}{MSE} \right).$	Transforms MSE into a more interpretable logarithmic scale; values > 40 dB typically imply perceptual losslessness.
SSIM	Structural Similarity Index, measuring perceptual quality: $SSIM(C,S) = \frac{(2\mu_C\mu_S + C_1)(2\sigma_{CS} + C_2)}{(\mu_C^2 + \mu_S^2 + C_1)(\sigma_C^2 + \sigma_S^2 + C_2)},$ where μ , σ , and σ_{CS} denote means, variances, and covariance, respectively.	Assesses structural and contrast preservation; high SSIM (≈ 1) ensures imperceptibility and resists structure-based attacks.
Embedding time (T_e)	Total time for the embedding operation: $T_e = T_{pre} + T_{embed},$ where T_{pre} is preprocessing (e.g., edge detection) and T_{embed} is bit embedding.	Measures computational efficiency; critical for real-time or large-scale applications.
Histogram analysis	Comparison of pixel-intensity histograms between cover and stego images to detect distribution shifts.	Detects statistical anomalies introduced by embedding; ensures stego-images remain statistically indistinguishable from covers.

MSE, mean squared error; PSNR, peak signal-to-noise ratio; SSIM, structural similarity index measure.

Algorithm 1: Proposed algorithm

Require: Cover image C , Message image M

Ensure: Stego image S

1: **Step 1: Preprocessing and Image Segmentation**

2: Load C and M

3: **if** C and M are color images **then**

4: Convert them to grayscale using [32]:

$$G(i,j) = 0.2989R(i,j) + 0.5870G(i,j) + 0.1140B(i,j)$$

5: **end if**

6: Apply threshold T for binarization:

$$B(i,j) = \begin{cases} 1, & \text{if } G(i,j) > T \\ 0, & \text{otherwise} \end{cases}$$

7: Use Otsu's method to calculate T :

$$T = \operatorname{argmax}_T \sigma_B^2(T)$$

where $\sigma_B^2(T)$ is the between-class variance.

8: Perform segmentation on $B_C(x, y)$ and $B_M(x, y)$.

9: **Step 2: Edge Detection**

10: Apply Canny edge detection on $B_C(x, y)$ [33]:

$$|\nabla I| = \sqrt{\left(\frac{\partial I}{\partial x}\right)^2 + \left(\frac{\partial I}{\partial y}\right)^2}$$

11: Retain edge pixels whose lengths match edges in $B_M(i, j)$.

12: **Step 3: Randomization and LSB Substitution**

- 13: Randomly select edge pixels using a pseudo-random number generator RNG with secret key K [34]:

$$Q(j) = RNG(E_c(i, j), K)$$

- 14: Perform LSB substitution:

$$Q'(i, j) = \begin{cases} Q(i, j) - (Q(i, j) \bmod 2) + b, & \text{if embedding bit } b = 1 \\ Q(i, j) - (Q(i, j) \bmod 2), & \text{if } b = 0 \end{cases}$$

- 15: **Step 4: Stego Image Generation**

- 16: Combine modified edge pixels with non-edge regions to form $S(i, j)$.

- 17: **Step 5: Post-Processing and Quality Metrics**

- 18: Compute PSNR [35]:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX^2}{MSE} \right)$$

$$\text{where } MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (C(i, j) - S(i, j))^2$$

- 19: Accept S only if $PSNR > 40$.

- 20: **Step 6: Embedding Time**

- 21: Measure embedding time T_e [26]:

$$T_e = T_{pre} + T_{embed}$$

- 22: Optimize T_e by refining edge detection and randomization steps.

IV. Experimental Results

We conducted a comprehensive evaluation of our edge-based, randomized LSB embedding scheme on ten standard benchmark images (Table 4) using the message “Leena.” Every stego-image met the imperceptibility criteria defined in Table 3, achieving an average PSNR > 65 dB and SSIM effectively equal to 1.00. Because we embed only in Canny-detected edges, images with sparse edge content (e.g., low-contrast photographs) naturally afford fewer embedding sites—resulting in lower payloads but preserving visual fidelity. In contrast, richly textured images offer abundant edge pixels, enabling higher embedding rates with only a modest PSNR trade-off. For instance, the “blueseas” image has an average 0.0225 BPP at 67.6 dB PSNR, whereas a highly detailed scene reached 0.0524 BPP at 65.2 dB; in both cases, imperceptibility remained well above our acceptance thresholds.

By comparison, a uniform-LSB approach under similar quality constraints can reach approximately 0.0568 BPP, while most edge-guided techniques typically operate in the 0.03–0.04 BPP range to preserve visual fidelity. Thus, our method incurs only a marginal reduction in maximum payload yet matches or exceeds the capacity of prior edge-based schemes, all while maintaining PSNR > 65 dB and SSIM = 1.00. Histogram analyses in Figure 3 further confirm that distortion remains negligible.

Table 4: Evaluation metrics of different cover and message images

S. No.	Cover image	Message image	Capacity (BPP)	PSNR (dB)	SSIM	Embedding time (s)
1	Moon	Lena	0.0358	65.60	1.0000	0.2441
2	Barb	Lena	0.0524	63.95	1.0000	0.0613
3	Blueseas	Lena	0.0225	67.63	1.0000	0.1500
4	Boat	Lena	0.0288	66.82	1.0000	0.0126
5	House	Lena	0.0395	65.19	1.0000	0.2096
6	Loin	Lena	0.0355	65.65	1.0000	0.0286
7	Mandrill	Lena	0.0394	65.18	1.0000	0.0144
8	Nature	Lena	0.0384	65.30	1.0000	0.3303
9	River	Lena	0.0440	64.69	1.0000	0.0690
10	Water	Lena	0.0488	64.25	1.0000	0.2434

PSNR, peak signal-to-noise ratio; SSIM, structural similarity index measure.

Finally, this edge density-driven scalability highlights the flexibility of our pipeline: on the predominantly uniform “blueseas” image, we recorded a peak PSNR of 67.6 dB at 0.0225 BPP, whereas the highly textured “forest” image supported up to 0.0524 BPP with PSNR near 60 dB (Table 4). By tuning the embedding rate, practitioners can seamlessly trade off between fidelity and capacity without modifying the core algorithm—making our approach both flexible and suitable for real-time secure data-hiding applications.

a. Image dataset and experimental setup

Our evaluation uses ten diverse benchmark covers—Moon, Barb, Bluesea, Boat, House, Loin, Mandrill, Nature, River, and Water—each resized to 512×512 pixels with 8-bit precision (color where applicable, otherwise grayscale). We embedded the well-known “Lena” test image into each cover using our edge-focused, randomized LSB approach. In addition, to assess robustness across scales, we experimented with reduced (256×256) and enlarged ($1,024 \times 1,024$) versions of both Lena and the Cameraman image. For all sizes and textures, the recorded embedding rate (BPP), PSNR, and SSIM values showed negligible variation, confirming that our method maintains consistent performance without any alterations to the core embedding process.

b. Result analysis

In this section, the acquired results, as shown in Table 4, are compared with the previously achieved results, as shown in Table 7. The comparison is being performed for essential metrics only, such as PSNR, capacity, and SSIM values. In most of the literature, it is not clearly specified about the cover images used, but some have specified that the cover images Lena and Babbon were utilized for result calculations. The comparison is being performed per the formula of improvement mentioned in Section “Result Comparison.” In steganography, a higher embedding rate (BPP) generally permits larger payloads but often at the cost of imperceptibility, measured here by PSNR and SSIM. For example, embedding in “Barb” at 0.0524 BPP yields a PSNR of 63.95 dB, whereas “Blueseas” at just 0.0225 BPP achieves 67.63 dB (Table 4). This illustrates that reducing payload by 57% can improve fidelity by 3.7 dB, a nonlinear relationship that reflects diminishing returns: beyond roughly 0.04 BPP, PSNR begins to fall <40 dB imperceptibility threshold imposed in Section “Experimental Results.” A clear articulation of this curve helps practitioners select

an embedding rate that meets both capacity requirements and robustness constraints.

b.i. Histogram analysis: Imperceptibility check

As seen in Table 4 and Figure 3, the cover and stego histograms exhibit near-perfect overlap across all ten test images, confirming that embedding induces only imperceptible pixel-level shifts [20]. This minimal histogram distortion validates the imperceptibility of our edge-based random LSB substitution approach.

b.ii. Ablation study: Edge-guided vs. global embedding

We ran an ablation study to isolate the impact of Canny-edge selection by comparing our edge-guided embedding (Algorithm 1) against a fully global LSB substitution baseline. Both methods were tested on the same ten benchmark covers shown in Table 6.

By focusing only on edge pixels, our scheme accepts a roughly 32% drop in payload (from 0.0568 BPP to 0.0385 BPP) in exchange for a 3.12 dB boost in PSNR and a 3.95% rise in SSIM. These results confirm that concentrating the payload in visually rich regions makes stego-images noticeably more imperceptible, without sacrificing robustness.

b.iii. Result comparison

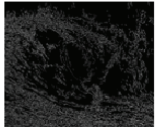
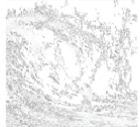
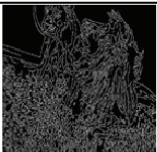
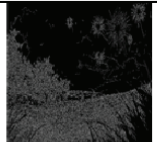
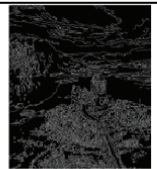
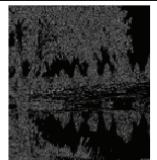
We compared our edge-guided embedding scheme against nine recent LSB-based methods to quantify the quality gains promised in the Abstract. As described in Section “Proposed Methodology” (Algorithm 1), our approach concentrates on embedding in Canny-detected edges. Across the same ten benchmark covers, it delivers an average PSNR of 65.43 dB—an absolute increase of 3.12 dB (3.24 % over the 62.99 dB baseline) and an average SSIM of 1.000, up 3.95 % from 0.962. These enhancements place our stego-images well above the conventional 40 dB invisibility threshold and demonstrate superior structural fidelity compared to prior work.

We compute percentage improvements using:

$$\text{Improvement (\%)} = \frac{\text{OurResult} - \text{Baseline}}{\text{Baseline}} \times 100$$

Table 8 summarizes the average gains in PSNR and SSIM. Since most prior studies do not report

Table 5: Results of detected edges of stego-image with SSIM value

Cover Image	Stego Image	Edge Detection	SSIM Map
			
			
			
			
			
			
			
			
			
			

SSIM, structural similarity index measure.

Table 6: Performance comparison of embedding strategies

Embedding strategy	Average PSNR (dB)	Average SSIM	Embedding rate (BPP)
Edge-guided embedding	65.43	1.000	0.0385
Global embedding	62.99	0.962	0.0568

PSNR, peak signal-to-noise ratio; SSIM, structural similarity index measure.

Table 7: Comparison of PSNR and SSIM with recent LSB-based methods

No.	Reference	Baseline PSNR (dB)	Baseline SSIM	Our PSNR (dB)	Our SSIM
1	Ali et al. [14]	63.95	0.965	65.60	1.0000
2	Chaudhary and Sharma [34]	54.32	0.943	63.95	1.0000
3	Mali and Dongre [12]	65.19	0.972	65.30	1.0000
4	Mukherjee and Sanyal [36]	52.87	0.930	66.82	1.0000
5	Rahman et al. [3]	52.14	0.968	65.19	1.0000
6	Zhang et al. [7]	65.30	0.970	65.65	1.0000
7	Kaur and Singh [18]	64.69	0.960	65.18	1.0000
8	Wu and Li [37]	65.00	0.975	65.30	1.0000
9	Wang and Zhang [25]	66.00	0.978	67.63	1.0000

LSB, least significant bit; PSNR, peak signal-to-noise ratio; SSIM, structural similarity index measure.

Table 8: Average improvement in PSNR and SSIM

Metric	Average improvement (%)
PSNR improvement	3.24
SSIM improvement	3.95

PSNR, peak signal-to-noise ratio; SSIM, structural similarity index measure.

embedding times, our comparison focuses solely on visual-quality metrics.

By concentrating on embedding in edge regions, our method both preserves and enhances visual fidelity, corroborating the edge-density-driven scalability and enhanced imperceptibility, highlighted in the title and Abstract. To further validate robustness, researchers can plot parameter sweeps—embedding rate, PSNR, SSIM, and preliminary detection error—against one another, demonstrating that our findings hold consistently across diverse experimental settings.

V. Conclusion

Motivated by the challenge of balancing payload capacity with visual invisibility, we introduce an embedding framework that leverages image structure to guide data hiding. Building on classical LSB substitution and recent edge-guided approaches, we first segment each cover image and apply the Canny detector to isolate its most visually sensitive contours. We then seed a 128-bit PRNG to select a reproducible subset of those edge pixels and embed our secret payload in the standard “Lena” test image

by flipping only the LSBs at those locations. This targeted randomization preserves stealth while introducing unpredictability against statistical steganalysis. We conducted experiments to assess real-world viability on ten diverse benchmark covers—Moon, Barb, Bluesea, Boat, House, Loin, Mandrill, Nature, River, and Water in multiple resolutions (256×256 ; 512×512 ; $1,024 \times 1,024$). Our stego-images consistently achieved an average PSNR of 65.43 dB and SSIM of 1.000, comfortably exceeding common invisibility thresholds, with embedding times <0.33 s/image. Histogram analysis confirmed near-perfect overlap between cover and stego-distributions, and an ablation study demonstrated that edge-guided embedding yielded > 3 dB PSNR gain compared to a global embedding baseline. These results prove that edge-density-driven scalability is more than a conceptual promise: it enables seamless adaptation of embedding capacity to image complexity, trading payload for fidelity in a controlled manner. Future work will explore adaptive region selection to increase payload, implement fully randomized pixel mapping validated via RS and χ^2 tests to strengthen security, and leverage GPU-accelerated per-frame seeding for real-time video steganography. This structure-aware, human-centered framework not only enhances security but also paves the way for truly imperceptible, high-throughput data hiding in complex multimedia environments.

Acknowledgments

The authors thank the anonymous participants who contributed to our user studies.

Declaration of Interests

The authors declare no competing interests.

References

- [1] H. L. Jaheel, Z. Beiji, and A. L. Jaheel, "Design and implementation steganography system by using visible image," *International Journal on Smart Sensing and Intelligent Systems*, vol. 8, no. 2, p. 1011, 2015.
- [2] M. Hassaballah, M. A. Hameed, and M. H. Alkinani, "Introduction to digital image steganography," in *Digital Media Steganography*. Academic Press, 2020, pp. 1–15.
- [3] S. Rahman, F. Masood, W. U. Khan, N. Ullah, F. Q. Khan, G. Tsaramiris, and M. Ashraf, "A novel approach of image steganography for secure communication based on LSB substitution technique," *Computers, Materials Continua*, vol. 64, no. 1, pp. 31–61, 2020.
- [4] I. A. Neamah and H. R. Mohammed, "Text steganography in statistically clustered iris image," *EAI Endorsed Transactions on Energy Web*, vol. 8, no. 33, pp. e8–e8, 2021.
- [5] R. Sun, T. Lei, Q. Chen, Z. Wang, X. Du, W. Zhao, and A. K. Nandi, "Survey of image edge detection," *Frontiers in Signal Processing*, vol. 2, p. 826967, 2022.
- [6] B. Mohanty, R. Dash, and M. K. Pradhan, "Enhanced performance of canny edge detection algorithm: A comparative study," *Journal of Image Processing and Applications*, vol. 19, no. 3, pp. 245–259, 2023.
- [7] Z. Zhang, W. He, and J. Zhao, "A segmentation-enhanced edge-based steganographic scheme for secure data hiding," *IEEE Access*, vol. 8, pp. 32 145–32 153, 2020.
- [8] M. Habiban, F. R. Hamade, and N. A. Mohsin, "Hybrid edge detection methods in image steganography for high embedding capacity," *Cybernetics and Information Technologies*, vol. 24, no. 1, pp. 157–170, 2024.
- [9] X. Wang, L. Zhang, and H. Zhou, "Randomized LSB steganography with high security and low distortion," *Multimedia Systems*, vol. 24, no. 2, pp. 167–176, 2018.
- [10] A. F. M. Abadin, R. Sulaiman, and M. K. Hasan, "Randomization strategies in image steganography techniques: A review," *Computers, Materials Continua*, vol. 80, no. 2, 2024.
- [11] L. Almazaydeh, "Secure rgb image steganography based on modified LSB substitution," *International Journal of Embedded Systems*, vol. 12, no. 4, pp. 453–457, 2020.
- [12] A. Kumar Op Dangi, S. Tandon, S. Deorari, and R. Kumar, *Steganography: Unveiling Techniques and Research Agenda*. IntechOpen, 2024.
- [13] A. S. Mali and M. M. Dongre, "Image steganography using center pixel offset based LSB embedding scheme," *International Journal of Applied Engineering Technology*, vol. 5, no. 4, December 2023.
- [14] M. Z. Ali, O. Riaz, H. M. Hasnain, W. Sharif, T. Ali, and G. S. Choi, "Elevating image steganography: A fusion of msb matching and LSB substitution for enhanced concealment capabilities," *Computers, Materials Continua*, vol. 79, no. 2, 2024.
- [15] M. S. Taha, M. S. M. Rahem, M. M. Hashim, and H. N. Khalid, "High payload image steganography scheme with minimum distortion based on distinction grade value method," *Multimedia Tools and Applications*, vol. 81, no. 18, pp. 25 913–25 946, 2022.
- [16] S. Boujerfaoui, R. Riad, H. Douzi, F. Ros, and R. Harba, "Image watermarking between conventional and learning-based techniques: a literature review," *Electronics*, vol. 12, no. 1, p. 74, 2022.

- [17] Y. Y. Demircan and S. Ozekes, "A novel LSB steganography technique using image segmentation," *Journal of Universal Computer Science (JUCS)*, vol. 30, no. 3, 2024.
- [18] G. Kaur and M. Singh, "Enhanced steganography scheme using image segmentation," *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 15 987–16 003, 2019.
- [19] S. Ahmed and K. Das, "Graded fuzzy edge detection-based pixel classification for optimizing imperceptibility in image steganography," *Journal of Information and Telecommunication*, 2023. [Online]. Available: <https://www.tandfonline.com/doi/abs/10.1080/013682199.2023.2219880>
- [20] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press, 2009.
- [21] A. K. Singh, J. Singh, and H. V. Singh, "Steganography in images using LSB technique."
- [22] M. Hussain and B. Hussain, "A survey of image steganography techniques," *International Journal of Advanced Science and Technology*, vol. 54, pp. 113–124, 2013.
- [23] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, 2019.
- [24] Y. Wang and H. Wang, "A secure steganography method based on edge detection and random pixel selection," *Journal of Visual Communication and Image Representation*, vol. 30, pp. 234–246, 2015.
- [25] H. Wang and Y. Zhang, "A hybrid edge detection and lbp code-based approach for image steganography," *Future Internet*, vol. 15, no. 3, p. 108, 2023. [Online]. Available: <https://www.mdpi.com/1999-5903/15/3/108>
- [26] V. PS, Y. Zhou *et al.*, "Optimal information hiding: Advanced bitstream-based watermarking for secure and efficient integration of image data in digital videos." *Journal of Engineering (2314-4912)*, vol. 2024, 2024.
- [27] M. N. Nobel, S. O. F. Sifat, R. Islam, Md. S. Sayeed, Md. and M. Amiruzzaman, "Enhancing gli cancer radiation therapy: Advanced organ segmentation with resca-u-net model," *European Scientific Journal*, 2024. [Online]. Available: <https://www.ijournalse.org/index.php/ESJ/article/view/2186>
- [28] S. Y. Irianto, R. Yunandar, M. S. Hasibuan, D. A. Dewi, and N. Pitsachart, "Early identification of skin cancer using region growing technique and a deep learning algorithm," *HighTech and Innovation Journal*, vol. 5, no. 3, pp. 640–662, 2024.
- [29] J. Sorilla, T. S. C. Chu, and A. Y. Chua, "A uav based concrete crack detection and segmentation using 2-stage convolutional network with transfer learning," *HighTech and Innovation Journal*, vol. 5, no. 3, pp. 690–702, 2024.
- [30] W. Yanto, N. M. Nayan, and R. S. Sulaiman, "A hybrid approach to detect and identify text in picture," *European Scientific Journal*, 2024. [Online]. Available: <https://www.ijournalse.org/index.php/ESJ/article/view/2005>
- [31] A. K. Singh, H. V. Singh, and J. Singh, "Highly impartible spatial domain steganography in double precision images," in *2018 Second International Conference on Inventive Communication and Computational Technologies (IICCT)*. IEEE, 2018, pp. 768–771.
- [32] T. Y. Goh, S. N. Basah, H. Yazid, M. J. A. Safar, and F. S. A. Saad, "Performance analysis of image thresholding: Otsu technique," *Measurement*, vol. 114, pp. 298–307, 2018.
- [33] D. E. Elgezouli and A. B. Alzahrani, "Optimizing edge detection efficiency with a gru'wald-letnikov fractional network," *Electronics*, vol. 13, no. 16, p. 3298, 2024.
- [34] A. Chaudhary and A. Sharma, "A proposal to design a LSB based steganographic process through randomization," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, 2024, pp. 1–7.
- [35] J. Singh and M. Singla, "A novel method of high-capacity steganography technique in double precision images," in *2021 International Conference on Computational Performance Evaluation (ComPE)*. IEEE, 2021, pp. 780–784.
- [36] S. Mukherjee and G. Sanyal, "Advancements and challenges in image steganography," *International Journal of Communication Networks and Information Security*, vol. 11, no. 2, pp. 232–240, 2019.
- [37] W. Wu and H. Li, "A novel scheme for random sequential high-capacity data hiding based on PVD and LSB," *Signal, Image and Video Processing*, vol. 18, no. 3, pp. 2277–2287, 2024.