A Multilayer Secure Image Steganography Framework Using Edge-Adaptive Embedding and Pre-Encryption

A F M Zainul Abadin[1], Rossilawati Sulaiman[2]*
Center for Cyber Security-Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia, Bangi, Selangor, 43600, Malaysia[1, 2]
Dept. of Information and Communication Engineering, Pabna University of Science and Technology, Pabna-660, Bangladesh[1]

***Abstract*—High-capacity image steganography aims to conceal large volumes of data while preserving imperceptibility and resistance to statistical and visual detection. This study proposes a multilayer secure image steganography framework using edge-adaptive embedding and pre-encryption. The method utilizes multiple edge detectors, namely Canny, Laplacian of Gaussian (LoG), and Prewitt, to accurately classify edge and non-edge regions, enabling efficient use of high-tolerance embedding areas. A Bee Colony Footprint Edge Optimization (BCFEO) algorithm is employed to select optimal embedding locations through a distortion-aware adaptive process, improving payload distribution under varying capacity conditions. For enhanced security, the secret message is encrypted prior to embedding using AES in Counter (CTR) mode, ensuring confidentiality without altering payload size and allowing exact recovery. A 5-LSB filtering mechanism is applied during preprocessing to reduce redundancy and control embedding distortion. The proposed framework is evaluated on a set of several 256×256 resized RGB images, including benchmark images from the USC-SIPI database and independently captured natural images, using standard performance metrics such as PSNR, SSIM, NCC, UIQI, and statistical steganalysis techniques. Experimental results demonstrate that the method achieves high embedding capacity with minimal visual degradation and improved performance compared to conventional edge-based approaches. The integration of adaptive optimized embedding and pre-encryption provides an efficient and reliable solution for secure image-based communication systems. The broader validation using larger datasets, different image resolutions, and more diverse image categories remains a future research direction.**

Keywords*—Image steganography; AES-CTR encryption; hybrid edge detection; edge-adaptive embedding; BCFEO nature-inspired optimization; statistical steganalysis

I. Introduction

With the rapid growth of digital communication, protecting sensitive information has become critical. While cryptography secures content, it does not hide the presence of communication, making it vulnerable to suspicion [1],[2]. Image steganography addresses this limitation by embedding data imperceptibly within images for covert communication [3]. A key challenge in image steganography is achieving a high payload capacity without compromising visual imperceptibility and statistical security [4]. Conventional least significant bit (LSB)-based schemes offer simplicity, but suffer from limited robustness and vulnerability to steganalysis when embedding capacity is increased [5]. To address this limitation, edge-based steganography has been widely investigated, as edge regions exhibit higher intensity variations and can tolerate larger embedding distortions compared to smooth areas. However, many existing edge-based methods rely on a single edge detector or fixed embedding rules, which restrict adaptability and lead to suboptimal payload distribution [6].

Another critical limitation in existing approaches is the insufficient integration of optimization-driven embedding strategies and cryptographic security. While several methods focus on either improving capacity or enhancing security, relatively few frameworks jointly optimize embedding locations while simultaneously encrypting the payload prior to embedding [7], [8]. As a result, such systems remain vulnerable to payload leakage or performance degradation under high embedding loads.

To address these challenges, this study proposes a high-capacity edge-adaptive image steganography framework with multilayer security. It integrates Canny, LoG, and Prewitt operators for accurate edge detection, while a Bee Colony Footprint Edge Optimization (BCFEO) algorithm adaptively selects optimal embedding locations for efficient payload distribution. Additionally, AES-CTR encryption is applied prior to embedding to ensure confidentiality even under partial data extraction.

The main contributions of this work are summarized as follows:

- A multilayer secure image steganography framework using edge-adaptive embedding and pre-encryption, integrating AES-CTR encryption with adaptive embedding to ensure confidentiality, exact payload length preservation, and reliable recovery.
- A hybrid edge detection and preprocessing strategy, combining Canny, Laplacian of Gaussian (LoG), and Prewitt operators with 5-LSB filtering to achieve accurate edge classification and controlled embedding distortion.
- A Bee Colony Footprint Edge Optimization (BCFEO) algorithm for distortion-aware and adaptive selection of

*Corresponding author

embedding pixels, enabling efficient payload distribution under varying capacity requirements.

- Comprehensive experimental evaluation, demonstrating high embedding capacity, improved imperceptibility, and strong resistance to statistical steganalysis compared to conventional methods.

The rest of the study has been structured as follows: Literature review in Section II discusses similar work on image steganography. Section III explains the recommended methodology. Experimental data and performance analysis are presented in Section IV, and Section V wraps up the study.

II. Literature Review

Over the past two decades, image steganography has progressed from simple spatial-domain methods to adaptive, edge-aware, and security-enhanced frameworks [9]. Existing studies mainly focus on improving capacity, imperceptibility, or robustness [10]. This section briefly reviews LSB-based, edge-adaptive, optimization-driven, and secure steganographic methods, highlighting key contributions and limitations.

Least significant bit (LSB) substitution is one of the earliest and most widely used image steganography techniques due to its simplicity and high embedding capacity [11]. Chan and Cheng [12] proposed an LSB-based embedding scheme with pixel adjustment to reduce visual distortion; however, the method remains vulnerable to statistical steganalysis as the payload increases. More recently, Rahman et al. [13] enhanced LSB steganography using a Magic Matrix and multi-level encryption to improve payload reliability and security in RGB images, but the reliance on fixed LSB substitution patterns limits scalability under high-capacity embedding and increases detectability against advanced steganalysis.

To improve imperceptibility, several studies have explored edge-based steganography, exploiting the higher distortion tolerance of edge and textured regions [14]. Sultana et al. [15] combined Sobel Canny edge detection with adaptive LSB embedding to increase payload while preserving visual quality; however, static edge fusion and limited bit-depth adaptation restrict scalability and robustness at higher payloads. Similarly, Habiban et al. [16] employed LoG-Wavelet and LoG-Canny edge detectors with LSB embedding and GIFT encryption, but the use of fixed 1-bit embedding and predefined edge rules constrains adaptability and resilience against modern steganalysis.

Recent works have further investigated adaptive and content-aware steganography to support higher payloads. The study [17] proposed a spatial-domain Fuzzy-graded method based on local texture complexity for adaptive pixel selection, achieving improved imperceptibility at moderate payloads; however, the absence of explicit edge prioritization leads to performance degradation at higher embedding rates. Further, Daiyrbayeva et al. [18] introduced an adaptive reversible data-hiding method for medical X-ray images using region segmentation and interpolation-based embedding, achieving high PSNR and reversibility, but at the cost of increased computational complexity and limited scalability for large-resolution images.

Edge-adaptive strategies have also been enhanced using hybrid detectors and learning-based models [19]. Several studies have employed Sobel, Canny, and Laplacian-based edge guidance to improve imperceptibility [15], [20], but reliance on single or static edge maps limits robustness across diverse image characteristics. The work [21] combined LoG edge detection with pixel-value differencing in RGB images to enhance capacity, but the method is irreversible, restricted to color images, and achieves acceptable quality only at moderate PSNR levels.

To improve embedding efficiency, optimization-based steganography has been widely explored. Singh and Bedi [22] applied particle swarm optimization (PSO) to select embedding pixels, achieving improved imperceptibility, but at the expense of high computational cost and lack of edge prioritization. The authors in [23] employed genetic algorithms for adaptive embedding; however, convergence instability and limited robustness evaluation restrict practical deployment. Omar et al.in [24] combined LoG edge detection with Shark Smell Optimization (SSO) to select embedding pixels, but reliance on LSB substitution and block-wise processing increases overhead and limits scalability under high payload conditions.

To enhance confidentiality, several studies have integrated cryptography with steganography [25], [26]. Some of the studies emphasized encryption as a key security layer in steganographic systems, while Kumar et al. [27] combined AES encryption with adaptive spatial-domain embedding to improve secrecy. Nevertheless, these approaches largely rely on conventional LSB-based embedding, which constrains robustness and payload scalability. Hybrid security systems have also been proposed, such as the DWT-AES-LSB framework by Awadh et al. [28], which improves security and capacity but remains limited by fixed LSB allocation. Survey studies, including Varghese and Sasikala [29], further highlight that existing methods often treat capacity, imperceptibility, optimization, and security as independent objectives rather than as a unified design problem.

The review reveals that LSB methods lack robustness at high payloads, edge-based schemes have limited adaptivity, optimization approaches often ignore encryption, and secure frameworks rely on conventional embedding. Therefore, a unified framework integrating adaptive edge detection, optimization-driven embedding, and strong cryptographic security is required, motivating this work.

III. Proposed Methodology

This section presents the proposed high-capacity edge-adaptive steganography framework with multilayer security. As shown in Fig. 1, it includes preprocessing, edge detection, optimized pixel selection, encryption, embedding, and extraction stages.

Let the grayscale converted cover image, and the secret message can be denoted as Eq. (1) and Eq. (2), respectively.

$$I \in \mathbb{Z}^{M\times N}, I(i,j) \in [0,255] \quad (1)$$

$$\mathcal{M} = \{m_k\}_{k=1}^{L}, m_k \in \{0,1\} \quad (2)$$

The objective is to embed $\mathcal{M}$ into I to generate a stego image I_s, that permits maximum payload capacity, minimum visual distortion, and the payload confidentiality remains preserved. This is formulated as a constrained optimization problem such as [see Eq. (3)]:

$$\max_{\Omega} \; C(\Omega) \text{s.t.} D(I, I_s) \leq \tau \tag{3}$$

where,

- Ω = total embedding pixel set
- $C(\cdot)$ = payload capacity
- $D(\cdot)$ = distortion metric
- τ = imperceptibility threshold

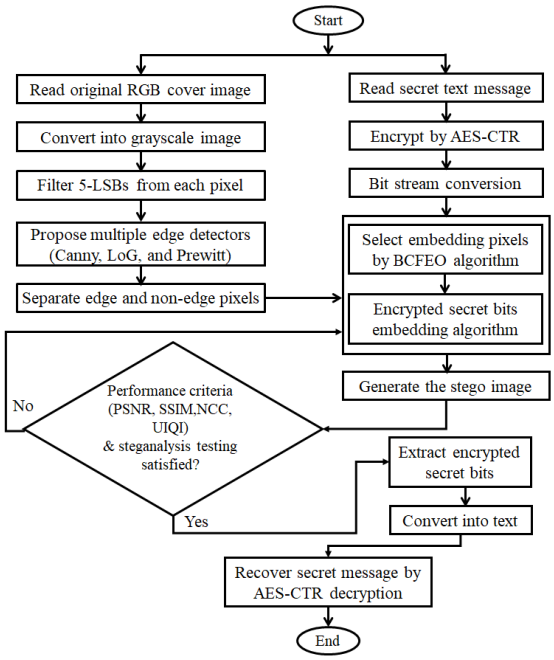

Fig. 1. Flowchart of the proposed edge-adaptive image steganography scheme with BCFEO-based optimized embedding and AES-CTR multilayer security.

A. Cover Image Preprocessing

The RGB cover image is first converted to grayscale to reduce computational complexity and ensure uniform pixel-level processing. A 5-LSB filtering operation is then applied by clearing the five least significant bits of each pixel, as expressed in Eq. (4):

$$I_n(i,j) = \left\lfloor \frac{I(i,j)}{2^5} \right\rfloor \times 2^5 \tag{4}$$

This operation quantizes each 8-bit pixel into multiples of 32, preserving the three most significant bits while discarding low-significance intensity variations. Therefore, the maximum preprocessing-induced pixel deviation is limited to 31 gray levels, while the normalized image remains structurally suitable for stable edge detection and controlled embedding. The purpose of this step is not to preserve exact pixel intensity, but to create a stable reference image in both embedding and extraction phases so that edge-map generation and bit recovery remain consistent. Its effect on image fidelity is subsequently reflected through PSNR, MSE, SSIM, and other quality metrics under different payload capacities. As payload increases, this preprocessing helps limit uncontrolled pixel fluctuation and improves robustness by reducing sensitivity to minor intensity variations.

B. Multi-Detector Edge Identification

Accurate identification of embedding regions is essential for high-capacity steganography. The proposed method employs Canny, LoG, and Prewitt detectors [15], whose outputs are fused to generate a reliable edge map for classifying pixels into edge and non-edge regions. This multi-detector approach improves robustness and adaptability across varying image textures.

1) Canny detector: The Canny method computes image gradients using Sobel operators [30], as in Eq. (5):

$$G = \sqrt{G_x^2 + G_y^2}, \quad \theta = \tan^{-1}\left(\frac{G_y}{G_x}\right) \tag{5}$$

where, G_x and G_y are horizontal and vertical gradients. Non-maximum suppression and hysteresis thresholding are then used to retain only strong, well-localized edges. Canny detector ensures strong edge localization and effective noise suppression through gradient analysis and hysteresis thresholding.

2) Laplacian of Gaussian (LoG) detector: The LoG highlights regions of rapid intensity change by convolving the image with [31], see Eq. (6):

$$\nabla^2 G(x,y) = \frac{\partial^2 G}{\partial x^2} + \quad \theta = \tan^{-1}\left(\frac{G_y}{G_x}\right) \tag{6}$$

where, $G(x,y)$ is a Gaussian-smoothed image. Zero-crossings of the result indicate edges, allowing detection of fine transitions and weak boundaries. LoG detector highlights fine intensity transitions and captures weak edges often missed by gradient-only detectors.

3) Prewitt detector: The Prewitt operator estimates gradients using convolution masks [3], as in Eq. (7):

$$G_x = I * M_x, \quad G_y = I * M_y \tag{7}$$

with M_x and M_y as horizontal and vertical masks. This operator is computationally simple and effective for detecting directional edges. Prewitt detector computes directional gradients, providing complementary information on vertical and horizontal edge structures.

C. Hybrid Edge Detection

Multiple detectors are used to leverage their complementary strengths: Canny is noise-robust, LoG enhances weak edges but may introduce false responses, and Prewitt captures gradients but is less precise in noise. Their edge maps are computed and combined as follows [see Eq. (8)]:

$$\begin{aligned} E_c &= \text{Canny}(I_n); E_l \\ &= \text{LoG}(I_n); E_p = \text{Prewitt}(I_n) \end{aligned} \tag{8}$$

By fusing their outputs with an OR operation, the system maximizes true edge coverage while minimizing the loss of embedding opportunities that would occur if a single detector were used. This hybridization ensures a richer set of candidate

pixels for embedding, leading to higher payload capacity and greater resilience without compromising imperceptibility. A fused edge map is then obtained as Eq. (9):

$$E_f(i,j) = \begin{cases} 1, & E_c + E_l + E_p \geq \theta \\ 0, & \text{otherwise} \end{cases} \quad (9)$$

Pixels are classified as:

- Edge pixels: $\mathcal{E} = \{(i,j) \mid E_f(i,j) = 1\}$
- Non-edge pixels: $\mathcal{N} = \Omega \setminus \mathcal{E}$

D. Optimized Embedding Pixel Selection Using BCFEO

To efficiently utilize the available embedding space, the proposed framework integrates the Bee Colony Footprint Edge Optimization (BCFEO) algorithm for adaptive pixel selection. BCFEO identifies suitable embedding locations by evaluating candidate edge pixels according to their local edge strength, texture variation, and distortion tolerance. Each candidate pixel $p_k \in \mathcal{E}$ is assigned a fitness score, after which the scores are normalized and ranked to categorize pixels based on their embedding suitability. Unlike iterative swarm-position update methods, the proposed BCFEO stage does not physically move pixels; instead, it performs fitness-based categorization of cover-image pixels. The optimized embedding set Ωe^* is selected from the highest-ranked edge pixels using an adaptive threshold determined by the payload requirement. If the capacity of Ωe^* is insufficient, the framework sequentially utilizes the remaining edge pixels Ω_r and, only when necessary, the non-edge pixels Ω_n. This hierarchical selection strategy enables adaptive payload distribution while preserving visual quality by prioritizing pixels with higher distortion tolerance. BCFEO-based pixel score for each candidate pixel $p_k \in \mathcal{E}$ is assigned a fitness score [see Eq. (10)]:

$$F(p_k) = \alpha \cdot | \nabla I_n(p_k) | - \beta \cdot \sigma^2(p_k) \quad (10)$$

where,

- $| \nabla I_n |$ = local gradient magnitude
- σ^2 = local variance
- α, β = weighting factors

The BCFEO iteratively updates pixel selection to maximize the fitness score as Eq. (11):

$$F(p_k)_{max} = \max \sum_{p_k \in \Omega} F(p_k) \quad (11)$$

E. Multilayer Security: AES-CTR Encryption

To enhance confidentiality, the secret message is encrypted prior to embedding using the Advanced Encryption Standard in Counter (AES-CTR) mode. AES-CTR is selected due to its strong cryptographic security, stream-like encryption capability, and absence of padding-induced length expansion that does not impact payload efficiency. The encrypted bitstream exhibits high randomness, preventing meaningful interpretation even if partial extraction occurs. This cryptographic layer forms the first security barrier, complementing the concealment provided by steganographic embedding. The plaintext message $\mathcal{M}$ is encrypted as Eq. (12):

$$C_k = m_k \oplus \text{AES}_K(\text{CTR} + k) \quad (12)$$

where,

- K= secret key
- CTR = initial counter
- C_k= ciphertext bit

CTR mode preserves message length and prevents error propagation.

F. Secret Data Embedding

The encrypted data is converted into a binary bitstream and embedded in the red channel using an adaptive strategy based on pixel classification and optimization output. This allows high payload capacity while preserving imperceptibility and statistical security. The distortion-aware embedding modifies each pixel accordingly, as in Eq. (13):

$$I_s(p) = \begin{cases} I_n(p) + b, & \text{if } b \in \{0,1\} \\ I_n(p), & \text{otherwise} \end{cases} \quad (13)$$

where, b is the encrypted bit. Bit allocation per pixel is adaptive and is determined as [see Eq. (14)]:

$$\eta(p) = \begin{cases} 2, & p \in \Omega_e^* \\ 1, & p \in \Omega_r \\ 0, & p \in \Omega_n \end{cases} \quad (14)$$

The well-defined algorithm for secret data embedding is presented in Algorithm 1.

Algorithm 1: Optimized Edge-Adaptive Embedding with Multilayer Security

Input: Cover image I, secret message $\mathcal{M}$, secret key K, initial counter CTR_0, embedding parameters (edge detectors, BCFEO parameters, payload length L)

Output: Stego image I_s

1: Input cover image I of size $M \times N$

2: Convert I to grayscale image Ig

3: Apply 5-LSB normalization to Ig:

$$I_n(i,j) = floor(\frac{I_g(i,j)}{2^5} 2^5)$$

4: Compute edge maps:

$$E_c \leftarrow Canny(I_n)$$

$$E_l \leftarrow LoG(I_n)$$

$$E_p \leftarrow Prewitt(I_n)$$

5: Fuse edge maps to generate consolidated edge map E_f:

$$E_f(i,j) = 1 \; if \; Ec(i,j) + El(i,j) + Ep(i,j) \geq \theta$$

$$0 \; otherwise$$

6: Classify pixels:

$$Edge \; pixel \; set \; \mathcal{E} \leftarrow \{(i,j) | E_f(i,j) = 1\}$$

$$Non-edge \; pixel \; set \; \mathcal{N} \leftarrow \Omega \setminus \mathcal{E}$$

7: Initialize Bee Colony Footprint Edge Optimization (BCFEO)

8: For each candidate edge pixel $pk \in \mathcal{E}$, compute its local fitness score $F(pk)$ using:

$$F(pk) = \alpha|\nabla In(pk)| - \beta\sigma^2(pk)$$

9: Perform BCFEO-based pixel fitness categorization:

For each candidate edge pixel $pk \in \mathcal{E}$, compute its fitness score $F(pk)$ based on edge strength, local texture variation, and embedding suitability.

Normalize all fitness scores and rank candidate pixels in descending order.

Select optimized embedding pixels as:

$$\Omega e^* = \{ pk \in \mathcal{E} | F_{norm}(pk) \geq \tau \}$$

where τ is an adaptive threshold determined by the required payload length L.

If $|\Omega e^*| < L$, include the next highest-ranked pixels until the payload requirement is satisfied.

10: Define pixels categories as:

$\Omega^* = \Omega e^* \cup \Omega r \cup \Omega n$; where

Ωe^* : BCFEO-optimized edge pixels

Ωr: remaining edge pixels

Ωn: selected non-edge pixels

11: Convert secret message $\mathcal{M}$ into binary bitstream $\{mk\}, k = 1 \dots L$

12: Encrypt bitstream using AES-CTR:

$$ck = mk \oplus AES_K(CTR_0 + k)$$

13: Initialize bit index $k = 1$

14: **for** each pixel $pk \in \Omega^*$ **do**

if $k > L$ **then**

break

end if

15: Determine embedding capacity $\eta(pk)$:

$$\eta(pk) = 2\ bits\ if\ pk \in \Omega e^*$$
$$1\ bit\ if\ pk \in \Omega r$$
$$0\ bit\ if\ pk \in \Omega n$$

16: Embed $\eta(pk)$ encrypted bits into pk in red channel of I :

$$I'_R(pk) \leftarrow I_R(pk) + \Sigma\ (ck \times 2^b), b \in \{0, \dots, \eta(pk) - 1\}$$

17: $Update\ k \leftarrow k + \eta(pk)$

18: end for

19: Reconstruct stego image I_s through merging I'_R and remaining two unchanged channels

20: Output stego image I_s

G. Secret Data Extraction and Message Recovery

At the receiver, extraction follows the inverse process. Using synchronized parameters, embedded bits are retrieved from the red channel and decrypted via AES-CTR to recover the original message. The extraction and recovery are given in Eq. (15) and Eq. (16):

$$\hat{b}_k = I_s(p_k) mod 2 \quad (15)$$

$$\hat{m}_k = \hat{b}_k \oplus \text{AES}_K(\text{CTR} + k) \quad (16)$$

The secret data extraction and reliable message recovery algorithm with a well-structured definition is presented in Algorithm 2.

Algorithm 2: Edge-Adaptive Extraction and AES-CTR Decryption

Input: Stego image I_s, secret key K, initial counter CTR_0, embedding parameters (edge detectors, BCFEO parameters, payload length L)

Output: Recovered secret message $\hat{\mathcal{M}}$

1: Convert I_s to grayscale image I_sg

2: Apply 5-LSB clearing to $I_sg \rightarrow I_sn$

3: Compute edge maps:

$$E_c \leftarrow Canny(I_sn)$$
$$E_l \leftarrow LoG(I_sn)$$
$$E_p \leftarrow Prewitt(I_sn)$$

4: Fuse edge maps to generate E_f:

$$E_f(i,j) = 1\ if\ Ec(i,j) + El(i,j) + Ep(i,j) \geq \theta$$
$$0\ otherwise$$

5: Classify pixels:

$$Edge\ pixel\ set\ \mathcal{E} \leftarrow \{ (i,j) | E_f(i,j) = 1 \}$$
$$Non-edge\ pixel\ set\ \mathcal{N} \leftarrow \Omega \setminus \mathcal{E}$$

6: Initialize Bee Colony Footprint Edge Optimization (BCFEO)

7: For each candidate edge pixel $pk \in \mathcal{E}$, compute fitness:

$$F(pk) = \alpha|\nabla In(pk)| - \beta\sigma^2(pk)$$

8: Perform BCFEO-based pixel fitness categorization:

$\Omega^* = \Omega e^* \cup \Omega r \cup \Omega n$; where

Ωe^* : BCFEO-optimized edge pixels

Ωr: remaining edge pixels

Ωn: selected non-edge pixels

9: Initialize empty ciphertext bitstream $\hat{\mathcal{C}} = \emptyset$

10: Select the modified red channel I'_R of stego image

11: **for** $k = 1$ to L **do**

12: Select extraction pixel $pk \in \Omega^*$

Extract encrypted bit:

13: $\hat{c}k = I_s(pk) \bmod 2$

14: Append $\hat{c}k$ to $\hat{C}$

15: end for

16: Group $\hat{C}$ into byte-aligned blocks

17: Initialize AES-CTR keystream using key K and counter CTR_0

18: **for** each encrypted bit $\hat{c}k$ **do**

Generate keystream bit:

$$zk = AES_K(CTR_0 + k)$$

Recover plaintext bit:

$$\hat{m}k = \hat{c}k \oplus zk$$

end for

19: Reconstruct original message $\hat{\mathcal{M}}$ from bitstream $\{\hat{m}k\}$

20: Output recovered message $\hat{\mathcal{M}}$

IV. Results and Analysis

The proposed framework was implemented and evaluated in Python 3.11.7 using the Anaconda distribution. Experiments were conducted on standard RGB benchmark images obtained from the USC-SIPI image database [32], together with additional natural images captured independently to introduce scene diversity beyond benchmark datasets. For consistent comparative evaluation, all color images were resized to 256×256 and converted into 8-bit grayscale images, resulting in 65,536 pixels per image for each simulation. Among the complete set of tested images, six representative samples, namely "Pepper", "F16", "Sailboat", "Boats", and two personally captured natural images, "KL Tower" and "UKM", are reported in detail due to space limitations and presentation clarity. These images were selected to cover different structural and textural characteristics, including smooth regions, strong edges, object boundaries, and complex natural backgrounds. Nevertheless, the evaluation is primarily based on fixed-resolution grayscale images; therefore, future work will extend the analysis to larger image sets with different resolutions, content categories, and statistical properties to further validate the generalizability of the proposed framework.

A. Payload Capacity Analysis

The achievable payload capacity of an image steganography system is primarily governed by the number and spatial distribution of pixels deemed suitable for embedding. In the proposed framework, payload capacity is directly influenced by the effectiveness of edge and non-edge pixel identification, which is performed exclusively on a reference intensity plane prior to data embedding. To evaluate the baseline embedding potential, edge pixels were initially identified using individual edge detectors, namely Canny, Prewitt, and Laplacian of Gaussian (LoG) and their hybridization applied to consecutive processed cover images.

TABLE I. Edge Pixels Found by Different Detectors and their Hybridization in Original and Cleared Images.

Images (65536 pixels)	Canny	LoG	Prewitt	Hybrid fused	
	Original grayscale (Org)			Org	Cleared
Pepper	7193	9284	8042	14132	21498
F16	6400	10607	9985	14246	16554
Sailboat	10774	12112	12666	20388	25362
Boats	9425	13211	11498	19515	23565
KL_tower	7151	11075	11239	17653	22798
UKM	13307	13295	12849	23442	27086

The results summarized in Table I indicate that the number of detected edge pixels varies significantly across detectors and image content. The corresponding edge pixel counts obtained from these representations are illustrated in Fig. 2, where the hybrid approach on the cleared image consistently yields a higher and more stable number of embedding candidates across all benchmark images, leading to the higher embedding capacity achieved in the adaptive mode of embedding for the proposed system.

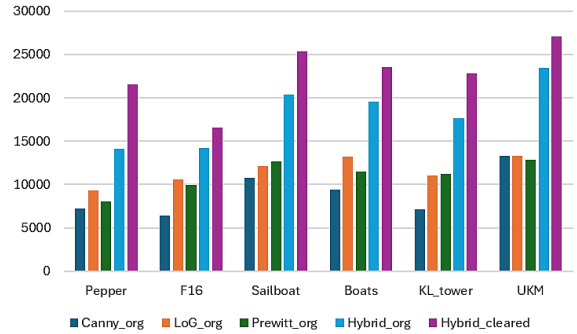

Fig. 2. Visual presentation of edge pixels found in different detectors and their hybrid fusion.

B. Imperceptibility (Qualitative) Analysis

As an initial qualitative assessment of imperceptibility, the visual quality of the generated stego images is examined from the perspective of the Human Visual System (HVS) before proceeding to quantitative performance evaluation. Fig. 3 illustrates representative examples of four original cover images and their corresponding stego images produced at an embedding payload of 1 bpp.

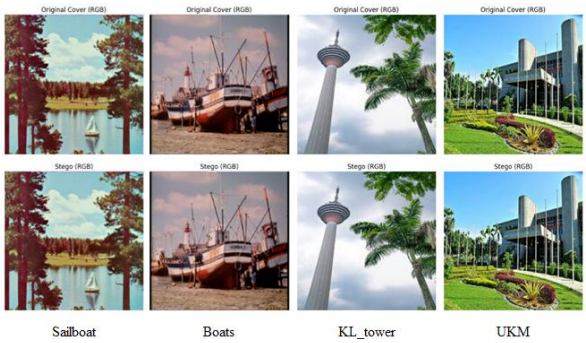

Fig. 3. Visual imperceptibility comparison between original cover images (top row) and corresponding stego images (bottom row) generated using the proposed steganography framework. Test images include Sailboat, Boats, KL_tower, and UKM.

A careful visual comparison between the cover and stego images reveals no discernible visual degradation across all evaluated test images. In particular, no visible noise patterns, color shifts, edge blurring, blocking artifacts, or contrast inconsistencies are observed in the stego images. This observation holds consistently for images with varying visual characteristics, including smooth regions, textured areas, object boundaries, natural landscapes, and human facial features. From an HVS standpoint, the stego images remain visually indistinguishable from their original counterparts.

C. Imperceptibility (Quantitative) Analysis

Imperceptibility is a critical requirement in image steganography, ensuring that the embedded payload does not introduce perceptible visual or statistical artifacts. Table II reports the detailed imperceptibility performance of the proposed method under varying payload sizes using the F-16 benchmark image, while Table III provides a cross-image summary of PSNR and SSIM values for six representative test images at selected payload capacities.

TABLE II. PRESENTATION OF PSNR, SSIM, AND NCC VALUES UNDER DIFFERENT PAYLOAD REGIMES IN F-16 IMAGE.

Payload Sizes/rates	PSNR	SSIM	NCC	UIQI	Entropy deviation
128 bits	83.91	1.0000	1.0000	1.0000	0.0000
256 bits	80.24	1.0000	1.0000	1.0000	0.0000
512 bits	77.00	1.0000	1.0000	1.0000	0.0000
1024 bits	74.07	1.0000	1.0000	1.0000	0.0000
0.031 bpp	70.91	1.0000	1.0000	1.0000	0.0000
0.063 bpp	67.81	1.0000	1.0000	1.0000	0.0000
0.125 bpp	64.96	0.9999	1.0000	1.0000	0.0000
0.25 bpp	62.01	0.9998	1.0000	1.0000	0.0001
0.50 bpp	58.92	0.9996	1.0000	1.0000	0.0001
1.00 bpp	55.91	0.9989	1.0000	1.0000	0.0008
2.00 bpp	48.90	0.9947	0.9999	0.9999	0.0012
3.00 bpp	42.61	0.9795	0.9991	0.9997	0.0141
4.00 bpp	36.67	0.9406	0.9963	0.9991	0.0333

As shown in Table II, the PSNR values for the F-16 image remain exceptionally high at low payloads, exceeding 80 dB for 128-bit embedding and gradually decreasing with increasing payload. Even at moderate payloads of 0.25-0.50 bpp, the PSNR values remain above 58 dB, which is well beyond the commonly accepted imperceptibility threshold of 40 dB. At higher payloads of 1-4 bpp, PSNR decreases as expected due to increased embedding density; however, the values remain within acceptable limits, demonstrating controlled distortion even under aggressive embedding conditions.

The SSIM values also remain extremely close to unity across most payload regimes, with only marginal degradation at higher payloads. This indicates that the proposed edge-adaptive and optimized embedding strategy effectively preserves the structural and perceptual characteristics of the cover image. Similarly, the NCC and UIQI values remain near 1.0 for all payloads, confirming strong statistical similarity between the cover and stego images. The entropy deviation remains negligible at low and moderate payloads and increases only slightly at very high embedding rates, indicating minimal disturbance to the underlying pixel distribution.

TABLE III. PRESENTATION OF PSNR AND SSIM VALUES UNDER DIFFERENT PAYLOAD REGIMES IN DIFFERENT TEST IMAGES.

Images	PSNR and SSIM for different payload rates					
	0.125 bpp		1.00 bpp		3.00 bpp	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Pepper	64.89	0.9999	55.90	0.9992	42.61	0.9761
F16	64.96	0.9999	55.91	0.9989	42.66	0.9795
Sailboat	64.97	0.9999	55.93	0.9992	42.61	0.9848
Boats	64.93	0.9999	55.93	0.9991	42.65	0.9862
KL_tower	64.97	0.9999	55.89	0.9989	42.63	0.9706
UKM	65.02	0.9999	55.91	0.9993	42.61	0.9796
Average	64.96	0.9999	55.91	0.9992	42.61	0.9795

To further address cross-image consistency, Table III summarizes PSNR and SSIM results across Pepper, F16, Sailboat, Boats, KL_tower, and UKM images at 0.125, 1.00, and 3.00 bpp. The average PSNR values are 64.96 dB, 55.91 dB, and 42.61 dB, respectively, while the corresponding average SSIM values are 0.9999, 0.9992, and 0.9795. These aggregated results confirm that the proposed method maintains high imperceptibility across different image contents, including benchmark images and independently captured natural images. The small variation among the tested images further indicates that the method is not strongly dependent on a single image structure or texture pattern.

The combined results in Table II and Table III demonstrate that the proposed method achieves a favorable capacity-imperceptibility balance across a wide range of payload capacities. The F-16 and cross-image results confirm that the proposed multi-detector edge selection and BCFEO-optimized embedding strategy maintain consistent image quality under increasing payloads across different test images.

D. Histogram Consistency Analysis

Histogram-based steganalysis evaluates whether embedding introduces noticeable changes in pixel intensity distributions. As shown in Fig. 4, the RGB histograms of the stego images closely match those of the corresponding cover images across all channels. The peak positions, intensity spread, and overall distribution shapes remain consistent, with no visible peak distortion, flattening, or abnormal clustering. This strong alignment indicates that the proposed method preserves first-order statistical properties and does not introduce detectable artifacts, even under multi-channel embedding.

Further strengthening the histogram-based security assessment, signed Pixel Difference Histogram (PDH) plots are analyzed at the same embedding rate and presented in Fig. 5. It demonstrates a sharp, symmetric peak centered at zero for both cover and stego images, indicating that most neighboring pixel differences remain small and evenly distributed around zero. The near-perfect overlap of the signed PDH curves confirms that

the embedding process does not introduce directional bias or systematic local distortions. The combined evidence from RGB histogram comparison and PDH analysis demonstrates that the proposed steganographic framework effectively resists histogram-based steganalysis.

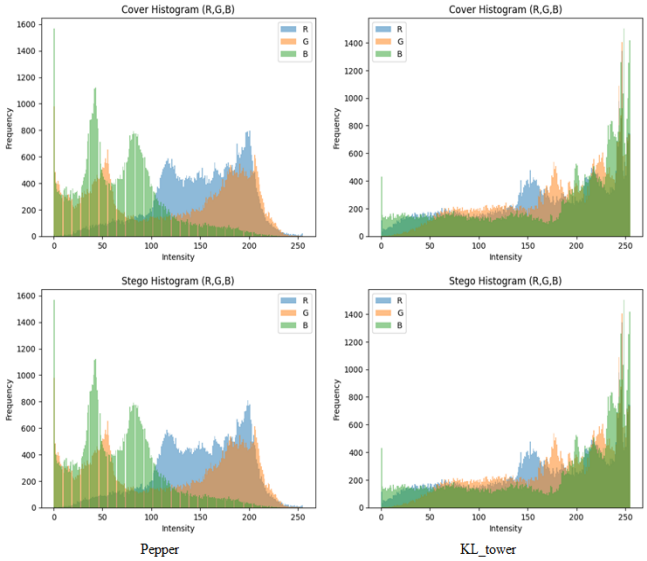

Fig. 4. RGB histogram comparison of cover (top row) and corresponding stego images (bottom row) for Pepper and KL_tower images, showing minimal statistical deviation and preservation of intensity distributions after embedding.

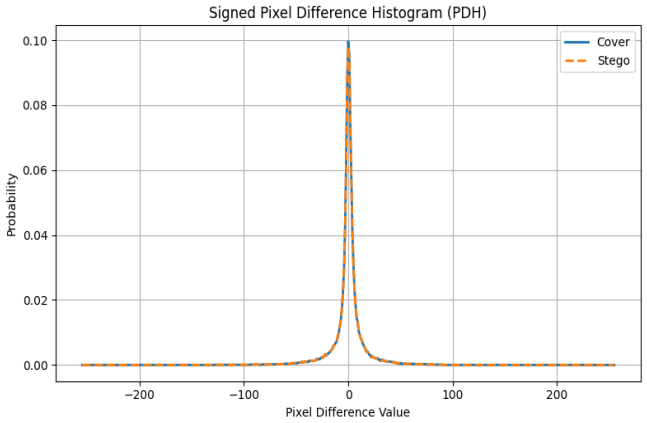

Fig. 5. PDH analysis of the cover and the stego image (F-16) at a data hiding rate of 1.00 bpp.

E. Regular-Singular (R-S) Steganalysis Evaluation

Regular-Singular (R-S) steganalysis assesses higher-order statistical changes in pixel groups under flipping masks. As shown in Fig. 6, the proportions of regular (R) and singular (S) groups for both masks $M = [1, 0, 1, 0]$ and $M = [0, 1, 0, 1]$, remain closely aligned between cover and stego images, with minimal and symmetric differences. Specifically, the relative differences between R_M and S_M, as well as between R_{-M} and S_{-M}, are minimal and symmetric across the cover-stego pairs. Additionally, the proportion of unusable groups (U) remains zero in all cases, indicating that the embedding process preserves natural image statistics without introducing detectable structural distortions.

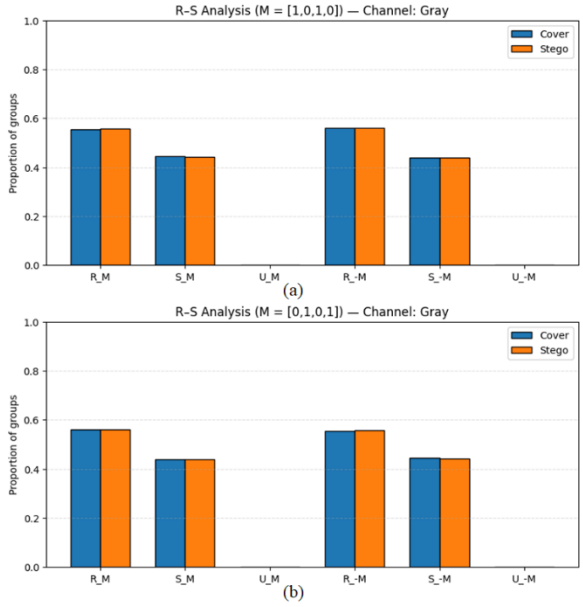

Fig. 6. Graphical presentation of Regular-Singular (R-S) steganalysis results for the grayscale converted image at an embedding rate of 1 bpp using two complementary flipping masks: (a) M=[1,0,1,0] and (b) M=[0,1,0,1].

The close correspondence between the proportions of regular (R), singular (S), and unusable (U) groups for the cover and stego images demonstrate preservation of structural statistics and resistance to R-S based steganalysis. The R-S analysis shows that the proposed embedding strategy preserves the natural imbalance between regular and singular groups across multiple flipping masks, thereby avoiding the characteristic equalization behavior exploited by R-S steganalysis.

F. Chi-Square and Pairs-of-Values (PoV) Steganalysis Evaluation

Chi-square (χ^2) steganalysis was conducted on the complete image set; representative results are shown for clarity and space efficiency. The global chi-square statistics for the grayscale converted "Sailboat" cover and stego image at 1.00 bpp embedding payload are derived from the grayscale intensity distribution after excluding low-frequency pairs is selected in an experimental simulation.

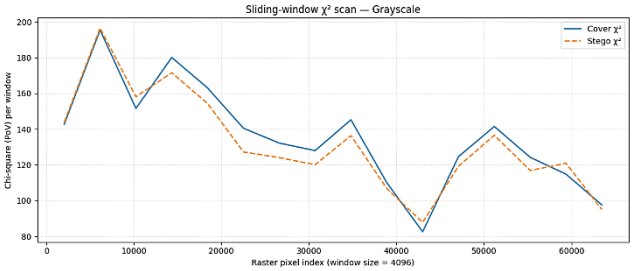

Fig. 7. Sliding-window (size=4096) chi-square ($\chi 2$) scan of the grayscale (Sailboat) cover and stego images at an embedding rate of 1 bpp.

To assess localized detectability, a sliding-window chi-square scan is performed across the rasterized grayscale image and illustrated in the sliding-window χ^2 plot shown in Fig. 7. The resulting chi-square trajectories of the cover and stego

images with 65536 hidden bits (1.00 bpp) exhibit closely aligned fluctuation patterns over all window positions and no persistent divergence or abrupt spike is observed in the stego curve relative to the cover curve. The close alignment of the chi-square trajectories indicates the absence of localized statistical anomalies introduced by the embedding process.

G. Crypto-Security and Reliability Analysis

Instead of direct plaintext embedding, the proposed system employs AES in Counter (CTR) mode to encrypt the secret message prior to bitstream generation. This ensures confidentiality while remaining independent of the embedding process. Importantly, AES-CTR preserves exact length equivalence between plaintext and ciphertext. For example, a 256-character message produces a 2048-bit stream, and the encrypted output retains the same 2048-bit length after binary conversion. As illustrated in Fig. 8, this one-to-one correspondence confirms strict length preservation throughout the process.

The results confirm that the recovered plaintext is identical to the original message, validating the reliability of the complete pipeline, including encryption, embedding, extraction, and decryption. As illustrated in Fig. 8, a 256-character message undergoes encryption, embedding, and recovery, with perfect agreement between the original and extracted plaintext, ensuring exact semantic reconstruction.

This accuracy is achieved while maintaining strict length consistency throughout all stages. The integration of AES-CTR encryption enhances security by protecting confidentiality, while its length-preserving property ensures that embedding capacity is unaffected. Consequently, the proposed framework achieves a balanced trade-off between security, capacity, and reliable recovery, reinforcing its effectiveness for secure communication.

Fig. 8. Authorized receiver validation showing end-to-end exact message (256 character) recovery, including plaintext encryption, ciphertext-to-bitstream embedding, extraction, and AES-CTR decryption.

H. Comparison with Existing Steganographic Methods

Table IV compares the proposed method with representative state-of-the-art image steganography approaches in terms of embedding capacity and imperceptibility. To ensure transparency, the comparison is interpreted in two ways based on the relative capacity-imperceptibility performances. The proposed method was evaluated under a consistent experimental setting, and the comparing values are taken from their original publications as several works do not provide complete implementation details, source codes, or identical parameter settings. Therefore, the comparison is intended to show the relative capacity-imperceptibility trend rather than a fully controlled one-to-one reproduction of all methods.

Existing hybrid edge-based methods achieve high visual quality, with PSNR values around 60.6 dB, but they operate at very low payloads, typically ≤ 0.125 bpp, which limits their applicability for high-capacity data hiding. In contrast, RGB model-based edge detection methods support higher payloads of up to 2.80 bpp but experience noticeable visual degradation, as indicated by lower PSNR and SSIM values. The IWT-PSO method provides competitive imperceptibility at low to moderate payloads, particularly within the 0.25-0.75 bpp range, where PSNR remains above 50 dB. However, its performance decreases as payload increases, and it is not extensively reported for higher-capacity embedding.

TABLE IV. COMPARISON OF THE PROPOSED METHOD TO OTHER COMPETING METHODS.

Method	Embedding rate (bpp)	PSNR (dB)	SSIM
Hybrid edge detection [16]	0.125	60.58	0.9992
RGB model-based edge detection [21]	2.80	33.51	0.8600
IWT-PSO [8]	0.25	56.53	0.9999
	0.61	52.78	0.9999
	0.75	50.68	0.9999
Proposed	0.125	64.96	0.9999
	0.25	62.01	0.9998
	0.50	58.92	0.9996
	1.00	55.91	0.9989
	2.00	48.90	0.9947
	3.00	42.61	0.9795
	4.00	36.67	0.9406

By comparison, the proposed method maintains a favorable capacity-imperceptibility balance across a wider payload range. At low payloads, it achieves high PSNR and near-unity SSIM, while at higher payloads of 1-4 bpp, it continues to preserve acceptable visual quality where many existing methods either degrade substantially or do not report results. This improvement is mainly attributed to the integration of multi-detector edge adaptivity and BCFEO-based optimized pixel selection, which prioritizes pixels with stronger edge characteristics and higher distortion tolerance. The results indicate that the proposed framework provides competitive and scalable capacity-imperceptibility trade-off for high-capacity steganographic embedding.

V. Conclusion

This study proposed a multilayer secure image steganography framework based on edge-adaptive embedding and pre-encryption for high-capacity covert communication. The framework combines hybrid edge detection using Canny, LoG, and Prewitt operators with Bee Colony Footprint Edge Optimization (BCFEO) to identify and prioritize embedding locations with high distortion tolerance. In addition, AES-CTR pre-encryption was incorporated to strengthen payload confidentiality while preserving exact message length and enabling reliable recovery. Experimental results demonstrated that the proposed method achieved high embedding capacity with controlled visual distortion, high structural similarity, and strong resistance to classical statistical steganalysis. Comparative evaluation further showed that the method provides a favorable capacity-imperceptibility trade-off over representative existing approaches, particularly at higher payloads. However, higher payloads gradually reduce imperceptibility, as indicated by lower PSNR and SSIM. The integration of adaptive edge selection, optimization-driven embedding, and length-preserving cryptographic protection makes the proposed framework an effective solution for secure image-based communication. The future work will validate the method on larger, higher-resolution, and more diverse datasets, evaluating robustness against different threats of adversarial or learning-based detection models.

Acknowledgment

This research was funded by the Ministry of Higher Education under the Fundamental Research Grant Scheme (FRGS/1/2020/ICT01/UKM/02/4), with research facilities provided by Universiti Kebangsaan Malaysia (UKM). The author, A. F. M. Zainul Abadin, gratefully acknowledges the ICT Division, the Ministry of Posts, Telecommunications and Information Technology, Bangladesh, for awarding him a PhD fellowship (FY 2022-2023, third round).

References

[1] S. Wang, J. Wang, and Z. Yu, "Privacy-preserving authentication in wireless IoT: applications, approaches, and challenges," IEEE Wirel. Commun., vol. 25, no. 6, pp. 60–67, 2019.

[2] J. Chen et al., "Fused Fuzzy Deep Learning and Information Steganography for Privacy Preservation in Medical Consumer Electronics," IEEE Trans. Consum. Electron., vol. 71, no. 2, pp. 7105–7116, 2025, doi: 10.1109/TCE.2025.3525536.

[3] A. F. M. Z. Abadin, R. Sulaiman, and M. K. Hasan, "A High-Security Image Steganography System Employing Multiple Edge Detectors," in Communications in Computer and Information Science, CCIS, vol. 2597, Springer Nature Singapore, 2026, pp. 40–55. doi: 10.1007/978-981-95-0172-4_3.

[4] M. Njoum, R. Sulaiman, Z. Shukur, and F. Qamar, "High-Secured Image LSB Steganography Using AVL-Tree with Random RGB Channel Substitution," Comput. Mater. Contin., vol. 81, no. 1, pp. 183–211, 2024, doi: 10.32604/cmc.2024.050090.

[5] A. H. Mohsin et al., "New Method of Image Steganography Based on Particle Swarm Optimization Algorithm in Spatial Domain for High Embedding Capacity," IEEE Access, vol. 7, pp. 168994–169010, 2019, doi: 10.1109/ACCESS.2019.2949622.

[6] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on lsb matching revisited," IEEE Trans. Inf. Forensics Secur., vol. 5, no. 2, pp. 201–214, 2010, doi: 10.1109/TIFS.2010.2041812.

[7] X. Duan, D. Guo, N. Liu, B. Li, M. Gou, and C. Qin, "A New High Capacity Image Steganography Method Combined with Image Elliptic Curve Cryptography and Deep Neural Network," IEEE Access, vol. 8, pp. 25777–25788, 2020, doi: 10.1109/ACCESS.2020.2971528.

[8] W. Wang and Q. Li, "An Image Steganography Algorithm Based on PSO and IWT for Underwater Acoustic Communication," IEEE Access, vol. 10, pp. 107376–107385, 2022, doi: 10.1109/ACCESS.2022.3212691.

[9] S. Ghoul, R. Sulaiman, and Z. Shukur, "A Review on Security Techniques in Image Steganography," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 6, pp. 361–385, 2023, doi: 10.14569/IJACSA.2023.0140640.

[10] O. Cetin and A. T. Ozcerit, "A new steganography algorithm based on color histograms for data embedding into raw video streams," Comput. Secur., vol. 28, no. 7, pp. 670–682, 2009, doi: 10.1016/j.cose.2009.04.002.

[11] A. F. M. Z. Abadin, R. Sulaiman, and M. K. Hasan, "Randomization Strategies in Image Steganography Techniques : A Review," Comput. Mater. Contin., vol. 80, no. 2, pp. 3139–3171, 2024, doi: 10.32604/cmc.2024.050834.

[12] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit., vol. 37, no. 3, pp. 469–474, 2004, doi: 10.1016/j.patcog.2003.08.007.

[13] S. Rahman et al., "A novel and efficient digital image steganography technique using least significant bit substitution," Sci. Rep., vol. 15, no. 1, pp. 1–16, 2025, doi: 10.1038/s41598-024-83147-3.

[14] A. F. M. Z. Abadin, R. Sulaiman, and M. K. Hasan, "Enhanced Predictive Pixel Deviation Frame Guided Hybrid Edge-Based Image Steganography for High Capacity and Imperceptibility," in Proc. The 10th International Conference on Electrical Engineering and Informatics, ICEEI 2025, Kuching, Malaysia, IEEE, 2025, pp. 1–6. doi: 10.1109/ICEEI68459.2025.11330299.

[15] H. Sultana, A. H. M. Kamal, G. Hossain, and M. A. Kabir, "A Novel Hybrid Edge Detection and LBP Code-Based Robust Image Steganography Method," Futur. Internet, vol. 15, no. 3, pp. 1–23, 2023, doi: 10.3390/fi15030108.

[16] M. Habiban, F. R. Hamade, and N. A. Mohsin, "Hybrid Edge Detection Methods in Image Steganography for High Embedding Capacity," Cybern. Inf. Technol., vol. 24, no. 1, pp. 157–170, 2024, doi: 10.2478/cait-2024-0009.

[17] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Graded fuzzy edge detection for imperceptibility optimization of image steganography," Imaging Sci. J., vol. 72, no. 6, pp. 693–705, 2024, doi: 10.1080/13682199.2023.2219880.

[18] E. Daiyrbayeva et al., "An Adaptive Steganographic Method for Reversible Information Embedding in X-Ray Images," Computers, vol. 14, no. 9, pp. 1–23, 2025, doi: 10.3390/computers14090386.

[19] M. Kumar, S. K. Singh, and S. Kim, "Hybrid deep learning-based cyberthreat detection and IoMT data authentication model in smart healthcare," Futur. Gener. Comput. Syst., vol. 166, p. 107711, 2025.

[20] A. F. M. Z. Abadin, M. K. Hasan, and R. Sulaiman, "An Enhanced Payload Image Steganography Employing Hybrid Edge Detection Technique and MSB Cover Image," in Communications in Computer and Information Science, CCIS, vol. 2597, Springer Nature Singapore, 2026, pp. 284–300. doi: 10.1007/978-981-95-0172-4_19.

[21] H. H. Liu and Y. T. Su, "Color Image Steganography Method Based on RGB Model and Edge Detection," Multimed. Tools Appl., no. 0123456789, 2024, doi: 10.1007/s11042-024-20008-1.

[22] S. Kumar, S. Pujari, A. Kulkarni, P. Misal, and I. R. Kale, "Image Steganography Using Particle Swarm Optimization," in International Conference on Information Science and Applications, 2023, pp. 115–130.

[23] S. M. Abdulmaged and N. M. Abdulmaged, "A new steganography technique based on genetic algorithm," Glob. J. Eng. Technol. Adv., vol. 16, no. 2, pp. 135–139, 2023.

[24] P. J. Karim, D. R. Arif, A. O. Abdalrahman, O. Y. Abdulhammed, T. S. Ali, and A. A. Saffer, "A Secure Image Steganography Using Shark Smell Optimization and Edge Detection Technique," Kurdistan J. Appl. Res., vol. 7, no. 2, pp. 11–25, 2022, doi: 10.24017/Science.2022.2.2.

[25] S. Kaur, S. Singh, M. Kaur, and H. N. Lee, "A Systematic Review of Computational Image Steganography Approaches," Arch. Comput. Methods Eng., vol. 29, no. 7, pp. 4775–4797, 2022, doi: 10.1007/s11831-022-09749-0.

[26] M. Njoum, R. Sulaiman, Z. Shukur, and F. Qamar, "A high-capacity image steganography based on random separate hashing data structure with secure CHACHA20-DRBG and AES encryption algorithms," Array, vol. 30, no. April, p. 100863, 2026, doi: 10.1016/j.array.2026.100863.

[27] A. Kumar, P. S. Sekhar, D. Khatua, D. K. Prasad, and A. A. Sekh, "Enhanced Image Steganography Using Secure Random Pixel Distribution," Secur. Priv., vol. 9, no. 1, p. e70186, 2026.

[28] [28] information security system via combination of compression, cryptography, and image steganography," Int. J. Electr. Comput. Eng., vol. 12, no. 6, pp. 6574–6584, 2022, doi: 10.11591/ijece.v12i6.pp6574-6584.

[29] F. Varghese and P. Sasikala, "A Detailed Review Based on Secure Data Transmission Using Cryptography and Steganography," Wirel. Pers. Commun., vol. 129, no. 4, pp. 2291–2318, 2023, doi: 10.1007/s11277-023-10183-z.

[30] Y. Song, C. Li, S. Xiao, Q. Zhou, and H. Xiao, "A parallel Canny edge detection algorithm based on OpenCL acceleration," PLoS One, vol. 19, no. 1, p. e0292345, 2024.

[31] S. K. Ghosal, J. K. Mandal, and R. Sarkar, "High payload image steganography based on Laplacian of Gaussian (LoG) edge detector," Multimed. Tools Appl., vol. 77, no. 23, pp. 30403–30418, 2018.

[32] "The USC-SIPI Image Database," University Southern California Signal and Image Processing Institute. [Online]. Available: https://sipi.usc.edu/database/