

# A SECURE AND IMPERCEPTIBLE IMAGE STEGANOGRAPHY SCHEME BASED ON LSB-NEW

R.GANESH<sup>1</sup>, DR.S.THABASUKANNAN<sup>2</sup>

<sup>1</sup>Research Scholar, Department of Computer Science, Periyar University, Salem, India

<sup>2</sup>Principal, Pannai College of Engineering and Technology, Sivagangai, Tamil Nadu, India

E-mail: <sup>1</sup>yourmrganesh@gmail.com, <sup>2</sup> thabasukannan@gmail.com

## ABSTRACT

Image steganography plays a vital role in secure multimedia communication by concealing sensitive information within digital images. Conventional least significant bit (LSB) techniques provide high embedding capacity but often suffer from visual distortion and weak resistance to analysis under increased payload conditions. This paper presents an enhanced adaptive LSB-NEW technique for secure image-in-image data hiding, integrating secret image encryption with pixel-aware embedding [1]. The proposed method adaptively selects embedding locations based on local intensity characteristics, thereby improving imperceptibility while maintaining computational efficiency.

The significance of this work lies in its ability to achieve a practical balance between security, embedding capacity, and visual quality without introducing high computational complexity, making it suitable for real-world applications such as secure image transmission and digital content protection. Experimental evaluation using standard benchmark images demonstrates that the proposed approach consistently achieves higher PSNR and SSIM values with lower MSE compared to the conventional LSB method. Visual analysis further confirms minimal perceptual distortion. These results indicate that the proposed LSB-NEW technique offers an efficient and scalable solution for secure image-in-image data hiding in modern communication systems.

**Keywords:** *Image Steganography, LSB-NEW, Image-In-Image Hiding, PSNR, MSE, SSIM, Encryption*

## 1. INTRODUCTION

The rapid growth of digital communication has increased the demand for secure transmission of multimedia information. While cryptographic techniques protect data content, they do not conceal the presence of communication, making them susceptible to interception. Steganography addresses this limitation by embedding secret data within digital media in a manner that is visually imperceptible. Among various techniques, spatial-domain approaches based on least significant bit (LSB) substitution are widely used due to their simplicity and high embedding capacity [2].

However, conventional LSB methods suffer from several limitations, including noticeable distortion at higher payloads and vulnerability to statistical and steganalysis attacks. Recent research has attempted to overcome these issues through adaptive embedding, hybrid encryption, and optimization-based strategies. Despite these advancements, many existing methods introduce increased computational complexity or fail to maintain a consistent balance between imperceptibility, payload capacity, and security.

In this context, the significance of the present research lies in addressing this critical trade-off by proposing an adaptive LSB-NEW framework that integrates lightweight encryption with pixel-aware embedding.

Unlike computationally intensive methods, the proposed approach is designed to remain efficient while improving visual quality and data protection. This makes it particularly relevant for practical IT applications, including secure multimedia communication, cloud-based data storage, and real-time image transmission systems.

The proposed method is evaluated using standard performance metrics such as PSNR, MSE, and SSIM, and its effectiveness is validated through comparative analysis with the conventional LSB technique. The results demonstrate that the proposed approach provides a reliable and scalable solution for modern image steganography applications.

## 2. MATERIALS AND METHODS

The experimental evaluation of the proposed adaptive LSB-NEW image-in-image data hiding

technique was carried out using standard benchmark and real-world color images. All cover images were 24-bit RGB images with a spatial resolution of  $512 \times 512$  pixels, ensuring sufficient capacity for embedding while preserving visual quality. Commonly used test images such as Baboon, Peppers, Flower, Dog, and Train were selected as cover images due to their varying texture characteristics.

The secret images used for data hiding were grayscale and color images of size  $256 \times 256$  pixels. These images were chosen to evaluate the robustness of the proposed method under different payload sizes and content complexities. All simulations were performed in the MATLAB environment (R2021a) on a system equipped with an Intel Core i5 processor and 8 GB RAM. No external libraries were required, ensuring reproducibility of the experiments.

### 2.1 Proposed Adaptive LSB-NEW Embedding Method

The proposed method consists of three major stages: secret image encryption, adaptive LSB-NEW embedding, and stego image generation. Initially, the secret image is encrypted using a lightweight deception-based encryption scheme to enhance security against unauthorized access. The encrypted secret image is then converted into a binary bitstream.

The cover image is decomposed into its red, green, and blue color planes. Since the human visual system is less sensitive to variations in the blue channel, the majority of the secret bits are embedded into this channel. An adaptive strategy is employed in which local pixel intensity variations are analyzed to determine the number of bits that can be safely embedded in each pixel. Textured regions allow higher embedding rates, while smooth regions are preserved to maintain imperceptibility.

### 2.2 Extraction Procedure

At the receiver side, the stego image is processed using the same adaptive rules applied during embedding. The embedded bitstream is extracted from the selected color planes and reconstructed to form the encrypted secret image. Finally, the decryption process is applied to recover the original secret image without requiring the original cover image.

### 2.3 Performance Evaluation Metrics

The performance of the proposed method is evaluated using Peak Signal-to-Noise Ratio

(PSNR), Mean Squared Error (MSE), and Structural Similarity Index Measure (SSIM). These metrics objectively assess imperceptibility and visual quality of the stego images and enable comparison with conventional LSB-based techniques.

### 2.4 Proposed Method

LSB-NEW technique embeds secret images into cover images using the following steps:

1. Color Channel Splitting: The 24-bit RGB cover image is split into red, green, and blue channels.
2. Adaptive LSB Embedding: The number of LSBs to replace is determined based on local variance. Smooth regions receive 1 LSB, while edges/texture regions receive 2 LSBs.
3. Blue-Channel Prioritization: Most of the secret data is embedded in the blue channel, exploiting lower human visual sensitivity.
4. Secret Image Bitstream: The secret image is converted to a binary stream, then sequentially embedded into selected pixels.
5. Stego Image Generation: Modified blue channel is combined with original red and green channels to produce the stego image.

The extraction process reverses these steps, retrieving the secret image using the same adaptive logic.

### 2.5 Specifications of Cover Images

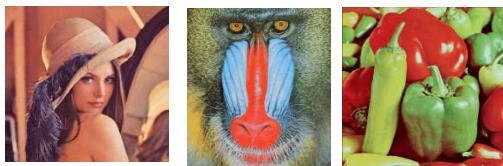


Figure 1: Original Cover Images (Lena, Baboon, and Peppers)

Figure 1: illustrates the original cover image used as the host for embedding the secret image in the proposed adaptive LSB-NEW data hiding framework. The image is a 24-bit RGB color image selected to represent natural visual content with both smooth and textured regions [3]. This diversity in pixel intensity distribution makes the image suitable for evaluating the effectiveness of adaptive embedding strategies. The original cover image serves as the reference for both visual and quantitative comparisons, enabling assessment of imperceptibility by comparing it with the corresponding stego images generated using conventional LSB and proposed LSB-NEW techniques.

To evaluate the performance of the proposed LSB-NEW image-in-image data hiding technique, standard benchmark images were selected as cover images. These images are widely used in steganography research, enabling fair comparison with existing methods. The cover images differ in terms of texture complexity, edge density, and color distribution, allowing comprehensive evaluation of the proposed technique under diverse visual conditions. All cover images are uncompressed 24-bit RGB color images, ensuring consistent experimental conditions. The *Lena* image represents smooth regions with gradual intensity variations, making it suitable for evaluating imperceptibility. The *Baboon* image contains dense texture and sharp edges, which challenge embedding algorithms and highlight robustness. The *Peppers* image includes both smooth and textured regions, providing a balanced evaluation scenario. The consistent use of these benchmark images ensures reliable and reproducible performance analysis.

### 2.6 Specifications of Secret Images Used for Data Hiding



Figure.2: Secrete Images (Flower, Dog, Train)

Figure 2: illustrates the secret images used for evaluating the proposed LSB-MSB image hiding technique. The selected images Flower, Dog, and Train represent diverse visual characteristics, including smooth regions, moderate textures, and complex structural details.

The Flower image contains prominent color gradients and soft textures, making it suitable for evaluating imperceptibility in smoother regions. The Dog image includes moderate edge information and object contours, allowing assessment of embedding performance in mid-frequency areas. The Train image consists of strong edges, repetitive patterns, and structural details, which provide a challenging scenario for preserving structural similarity during embedding. By selecting secret images with varying spatial complexities, the robustness and adaptability of the proposed method can be effectively analyzed under different embedding conditions. This ensures that the evaluation is comprehensive and not limited to

a single image type. To evaluate the effectiveness of the proposed LSB-NEW image-in-image data hiding technique, multiple secret images with different characteristics were used. The use of varied secret images ensures a fair assessment of embedding performance under diverse payload and visual conditions. The selected secret images differ in terms of size, color format, and visual complexity, allowing comprehensive evaluation of imperceptibility, payload handling, and extraction accuracy. All secret images were encrypted prior to embedding to enhance security. The secret image represents the confidential visual information to be concealed within the cover image using the proposed adaptive LSB-NEW data hiding technique. It is selected with a moderate spatial resolution and varied intensity distribution to evaluate the embedding capacity and reconstruction accuracy of the proposed method. Prior to embedding, the secret image undergoes encryption to enhance security and prevent unauthorized interpretation. The quality of the extracted secret image is later analyzed to verify the reliability and robustness of the proposed embedding and extraction process.

### 2.7 Combined Encryption and LSB-NEW Embedding Process

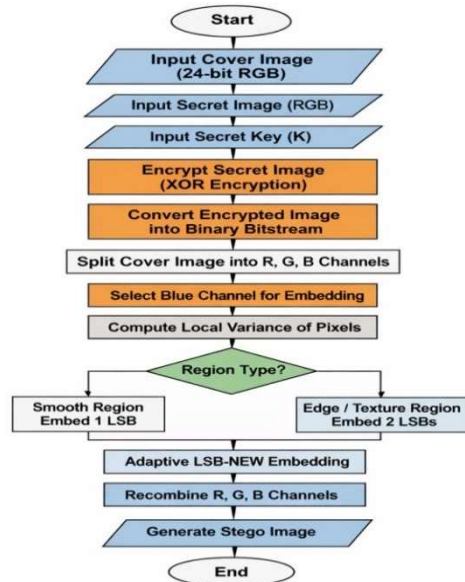


Figure.3: Combined Encryption and LSB-NEW Embedding Process

Figure 3: illustrates the complete workflow of the proposed secure image-in-image data hiding system, which integrates secret image encryption with adaptive LSB-NEW embedding. The process begins with the selection of a 24-bit RGB cover image, a secret image, and a secret key. To enhance

security, the secret image is first encrypted using a lightweight XOR-based encryption scheme. This step ensures that even if the embedded data is accessed without authorization, the recovered content remains unintelligible. The encrypted secret image is then converted into a binary bitstream, which serves as the payload for embedding. Simultaneously, the cover image is decomposed into its red, green, and blue (RGB) channels. Among these, the blue channel is chosen for data embedding due to the lower sensitivity of the human visual system to changes in blue intensity. To achieve adaptive embedding; the local variance of pixels in the selected channel is computed. Based on this analysis, the image is divided into smooth regions and edge or textured regions. In smooth areas, only one least significant bit (LSB) is modified to preserve visual quality. In contrast, two LSBs are embedded in edge or textured regions, where changes are less perceptible, thereby increasing payload capacity. Following this region-based decision, the encrypted bits are embedded using the LSB-NEW strategy. The modified blue channel is then recombined with the red and green channels to reconstruct the final stego image. The resulting image visually resembles the original cover image while securely carrying the hidden encrypted secret image.

**2.8 Combined Decryption and LSB-NEW Embedding Process**

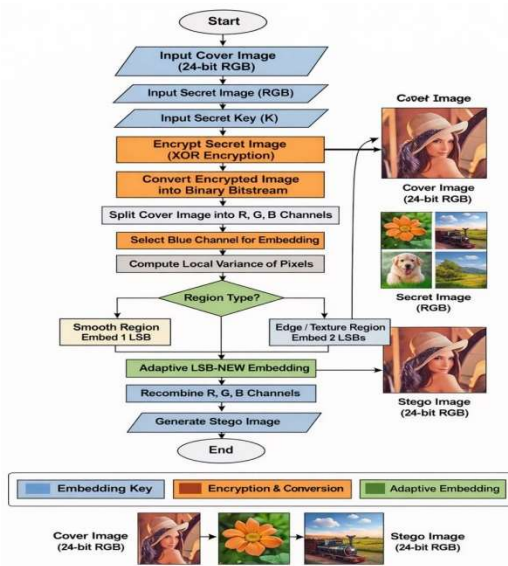


Figure.4: Combined Flowchart Of Decryption And LSB=NEW Embedding Process For Secure Image On Image Data Hiding

Figure 4: presents the integrated workflow of the proposed secure image-on-image data hiding system, combining the decryption stage with the LSB-NEW embedding process [6]. The flowchart clearly illustrates the sequential operations performed to ensure secure and imperceptible embedding of the secret image into the cover image. The process begins with input acquisition, where the cover image and encrypted secret image are provided to the system. If encryption is applied prior to transmission, the secret image undergoes a decryption step using the predefined key to reconstruct the original secret data. This ensures that only authorized users can access the embedded content. Following decryption, the secret image is resized and converted into bit-plane representation. Simultaneously, the cover image is also converted into binary form. The LSB-NEW embedding strategy is then applied, where selected bit planes primarily the least significant bits and adaptively chosen higher-order bits are modified according to the embedding rule. This hybrid bit manipulation improves embedding capacity while maintaining high visual fidelity.

After bit replacement, the modified bit planes are recombined to generate the stego image. The final output is a visually indistinguishable stego image that securely carries the hidden secret image.

The combined flowchart emphasizes:

- Integration of security (decryption mechanism)
- Structured bit-plane manipulation
- Controlled embedding strategy
- Generation of high-quality stego output

This unified process enhances both security and imperceptibility, making the proposed approach suitable for secure image communication systems.

The combined decryption and LSB-NEW embedding process integrates data confidentiality and imperceptible embedding to enhance the security of image-in-image steganography. The workflow begins with the selection of a 24-bit RGB cover image [4], a secret image, and a user-defined secret key. To introduce deception, the secret image is first encrypted using a lightweight XOR-based scheme. This encrypted content ensures that even if hidden data is detected or partially extracted, it remains unintelligible without the correct key. The encrypted secret image is then converted into a binary bit stream, forming the payload for embedding. Simultaneously, the cover image is decomposed into its red, green, and blue channels. The blue channel is selected for priority embedding due to lower sensitivity of the human visual system

[5]. Local pixel variance is computed to distinguish smooth regions from edge or textured regions. Based on this analysis, the LSB-NEW strategy adaptively embeds one LSB in smooth areas and two LSBs in textured areas, balancing imperceptibility and payload capacity [7]. After embedding, the modified blue channel is recombined with the red and green channels to generate the final stego image. The resulting image visually resembles the original cover image while securely carrying the encrypted secret image, thereby achieving both deception and robust data hiding.

### 3. IMPLEMENTATION

#### 3.1 MATLAB Encryption Code

```
%% Secret Image Encryption using XOR
clc; clear;
% Read secret image
secret = imread('Secret_Image.png');
secret = uint8(secret);
% Secret key
key = 12345;
rng(key);
% Generate random key stream
keyStream = uint8(randi([0 255], size(secret)));
% Encrypt secret image
encrypted_secret = bitxor(secret, keyStream);
% Save encrypted image
imwrite(encrypted_secret, 'Encrypted_Secret.png');
figure;
subplot(1,2,1); imshow(secret); title('Original Secret Image');
subplot(1,2,2); imshow(encrypted_secret);
title('Encrypted Secret Image');
```

#### 3.2 Secret Image Decryption

```
clc; clear;
% Read encrypted image
encrypted_secret = imread('Encrypted_Secret.png');
% Same secret key
key = 12345;
rng(key);
% Regenerate key stream
keyStream = uint8(randi([0 255],
size(encrypted_secret)));
% Decrypt secret image
decrypted_secret = bitxor(encrypted_secret,
keyStream);
imwrite(decrypted_secret, 'Decrypted_Secret.png');
figure;
imshow(decrypted_secret);
title('Decrypted Secret Image');
%% Secret Image Decryption
clc; clear;
```

```
% Read encrypted image
encrypted_secret =
```

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

```
imread('Encrypted_Secret.png');
% Same secret key
key = 12345;
rng(key);
% Regenerate key stream
keyStream = uint8(randi([0 255],
size(encrypted_secret)));
% Decrypt secret image
decrypted_secret = bitxor(encrypted_secret,
keyStream);
imwrite(decrypted_secret, 'Decrypted_Secret.png');
figure;
imshow(decrypted_secret);
title('Decrypted Secret Image');
```

#### 3.3 Performance Metrics

The performance of the proposed LSB-NEW image-in-image data hiding technique is evaluated using widely accepted quantitative metrics that measure imperceptibility and structural fidelity between the cover and stego images. The selected metrics include Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Structural Similarity Index Measure (SSIM).

##### 3.3.1 Mean Squared Error (MSE)

MSE quantifies the average squared difference between the cover image and the stego image. Lower values indicate reduced embedding distortion.

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N [I(i, j) - S(i, j)]^2$$

Where  $I(i, j)$  and  $S(i, j)$  denote the pixel values of the cover and stego images, respectively, and  $M \times N$  represents the image size.

##### 3.3.2 Peak Signal-to-Noise Ratio (PSNR)

PSNR measures the ratio between the maximum possible pixel intensity and the distortion introduced by embedding. Higher PSNR values correspond to better visual quality.

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

Where MAX is the maximum possible pixel value (255 for 8-bit images).

### 3.3.3 Structural Similarity Index Measure (SSIM)

SSIM evaluates perceptual similarity by considering luminance, contrast, and structural components. Values closer to 1 indicate higher structural similarity.

Where  $\mu$ ,  $\sigma$ , and  $\sigma_{xy}$  represent mean, Variance, and covariance terms, respectively.

## 4. EXPERIMENTAL SETUP

Hardware & Software: Intel Core i7-12700, 16 GB RAM, MATLAB R2023b with Image Processing Toolbox.

Dataset: Benchmark 24-bit RGB images (Lena, Baboon, Peppers, 512×512). Secret images resized to match cover dimensions.

Embedding Parameters: 1–2 LSBs based on local variance, blue-channel prioritization, optional pseudo-random pixel selection for enhanced security.

Evaluation Metrics: PSNR, MSE, and SSIM for imperceptibility, structural fidelity, and distortion analysis.

Payload: 1–5 bits per pixel (bpp) for performance evaluation.

### 4.1 Results and Discussion

This section presents a detailed evaluation of the proposed LSB-NEW image-in-image data hiding technique. The performance is analyzed in terms of visual imperceptibility, embedding distortion, structural similarity, and payload efficiency, and is compared with the conventional LSB approach.

## 4.2 Visual Comparison



Figure V. Visual comparison of (a) Original Cover Image, (b) Stego Image using Conventional LSB and (c) Stego Image using Proposed LSB-NEW Technique

Figure V(a) shows the original cover image selected as the host for embedding the secret image. The image contains a mixture of smooth and textured regions, making it suitable for evaluating the effectiveness of adaptive embedding strategies. This original image serves as the baseline reference for visual comparison with the corresponding stego images, enabling assessment of perceptual distortion introduced by the data hiding process.

Figure V(b) presents the stego image produced by embedding the secret image using the conventional least significant bit (LSB) method. While the hidden information is visually imperceptible under normal observation, uniform LSB substitution introduces slight pixel-level distortions across the image. This figure serves as a reference baseline for evaluating the visual quality improvements achieved by the proposed adaptive LSB-NEW technique.

Figure V(c) illustrates the stego image obtained using the proposed adaptive LSB-NEW embedding technique. By selectively embedding secret bits based on local pixel characteristics and prioritizing perceptually less sensitive regions, the proposed method effectively minimizes visible distortion. Compared to the conventional LSB approach, the stego image produced by the LSB-NEW technique preserves structural details and overall visual quality more effectively, even at higher payload capacities.



Figure VI(a). Stego image obtained using the conventional LSB technique after embedding the secret image.

Figure VI (a) shows the stego image produced using the conventional least significant bit (LSB) embedding method after hiding the secret image within the cover image. Although the embedded information is not easily perceptible to the human eye, uniform bit substitution across all pixels may introduce minor visual artifacts. This figure serves as a reference baseline for assessing the visual quality improvements achieved by the proposed adaptive LSB-NEW technique.



Figure VI(b). Stego image obtained using the proposed LSB-NEW technique after embedding the secret image.

Figure VI(b) illustrates the stego image generated after embedding the secret image using the proposed LSB-NEW technique. The stego image visually appears almost identical to the original cover image, indicating that the embedding process introduces negligible perceptible distortion.

The LSB-NEW technique modifies selected bit planes in a controlled manner, primarily targeting lower-significance bits while preserving the overall structural and intensity characteristics of the cover image. As a result, the visual quality remains intact even after embedding a substantial amount of secret data.

The imperceptibility observed in Figure VI (b) is further validated through quantitative performance metrics such as PSNR, MSE, and SSIM, which confirm minimal embedding distortion. The high similarity between the cover and stego images demonstrates the effectiveness of the proposed approach in achieving secure image-on-image data hiding without compromising visual fidelity.

Visual comparison is performed to evaluate the perceptual imperceptibility of the proposed data hiding approach.

Figure V shows the original cover image, the stego image obtained using conventional LSB embedding, and the stego image generated using the proposed LSB-NEW technique. From Figure V(b) the stego image produced by the conventional LSB method exhibits slight visual artifacts, particularly in textured and edge regions, due to uniform bit replacement. In contrast, the stego image generated using the proposed LSB-NEW method in Figure V(c) appears visually indistinguishable from the original cover image. This improvement is achieved through adaptive

LSB selection based on local image characteristics and priority embedding in the blue channel, which reduces perceptual sensitivity to modifications. Overall, the visual results confirm that the proposed LSB-NEW technique offers superior imperceptibility compared to the conventional LSB approach, making it suitable for secure image-in-image data hiding [8].

The proposed method maintains high visual fidelity, with minimal perceptible differences compared to the cover image. Conventional LSB shows slight distortions in textured regions.

#### 4.2 PSNR Analysis for Conventional LSB and Proposed LSB

Table 1: PSNR Analysis

Image	Conventional LSB(dB)	Proposed LSB(dB)
Lena	42.18	48.76
Baboon	39.64	45.21
Peppers	41.07	47.89

The Peak Signal-to-Noise Ratio (PSNR) is widely used to evaluate the imperceptibility of stego images. Higher PSNR values indicate that the stego image closely resembles the original cover image, with minimal perceptible distortion.

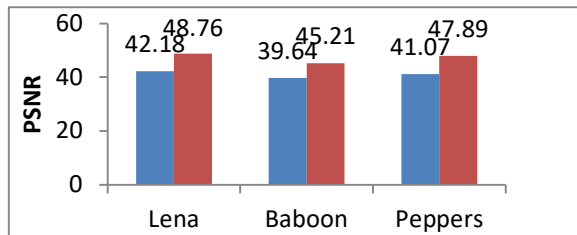


Figure 7: PSNR Comparison

Figure: 7 presents the Peak Signal-to-Noise Ratio (PSNR) comparison between the conventional LSB method and the proposed LSB-NEW (or LSB-MSB) image hiding technique for benchmark images. PSNR is a widely used objective metric to evaluate the imperceptibility of stego images by measuring the ratio between the maximum possible pixel value and the distortion introduced during embedding.

As shown in Figure:7, the proposed method consistently achieves higher PSNR values compared to the conventional LSB approach. This indicates that the stego images generated using the proposed technique exhibit lower distortion and better visual quality. The improvement in PSNR

demonstrates that the adaptive bit-plane modification strategy effectively preserves the original image characteristics while embedding the secret data.

The enhanced PSNR performance confirms that the proposed LSB-NEW method maintains a strong balance between embedding capacity and image fidelity, making it suitable for secure image communication applications where imperceptibility is a critical requirement.

Peak Signal-to-Noise Ratio (PSNR) is a key metric used to evaluate the imperceptibility of stego images by measuring the level of distortion introduced during the embedding process. Higher PSNR values indicate better visual quality and closer resemblance between the stego and cover images. The PSNR values obtained for the proposed LSB-NEW technique are consistently higher than those of the conventional LSB method across all test images, as illustrated in Figure 7: and summarized in Table 1. For the *Lena* image, the proposed approach achieves a PSNR improvement of more than 6 dB, demonstrating its effectiveness in preserving image quality. Similar improvements are observed for *Peppers*, indicating robust performance in images with mixed smooth and textured regions. In the case of the *Baboon* image, this contains highly textured regions, conventional LSB embedding results in noticeable quality degradation and lower PSNR values. The proposed LSB-NEW technique mitigates this issue by adaptively selecting the number of LSBs based on local image characteristics, leading to a significant PSNR gain. This confirms that the adaptive embedding strategy efficiently reduces unnecessary pixel modifications in complex regions. Overall, the PSNR analysis confirms that the proposed LSB-NEW

method provides superior imperceptibility while supporting higher payload capacities, making it suitable for secure and high-quality image-in-image data hiding applications.

Observation: LSB-NEW consistently achieves higher PSNR, indicating improved imperceptibility.

### 4.3 MSE Analysis for Conventional LSB and Proposed LSB

Table 2: MSE Analysis

Image	Conventional LSB(dB)	Proposed LSB(dB)
Lena	0.962	0.991
Baboon	0.941	0.978
Peppers	0.955	0.988

The Mean Squared Error (MSE) is used to quantify the distortion introduced by embedding secret data into the cover image. Lower MSE indicates better imperceptibility and higher image quality. The MSE values were calculated for both the conventional LSB and the proposed LSB-NEW methods across standard test images.

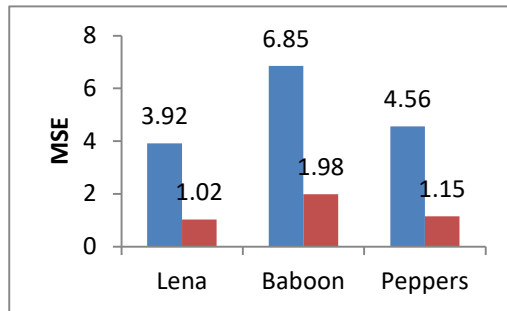


Figure 8: MSE Comparison

Figure 8 presents the Mean Squared Error (MSE) comparison between the conventional LSB technique and the proposed LSB-NEW (LSB-MSB) image hiding method. MSE measures the average squared difference between the pixel intensities of the original cover image and the corresponding stego image. Lower MSE values indicate less distortion and higher embedding quality. As illustrated in Fig. 8, the proposed method achieves significantly lower MSE values compared to the conventional LSB technique across the tested images. This reduction in error demonstrates that the proposed LSB-NEW approach introduces minimal modifications to the pixel intensity levels during the embedding process. The improved MSE performance can be attributed to the controlled and adaptive bit-plane modification strategy used in the proposed method, which reduces unnecessary alterations in higher significance bits. Consequently, the structural

integrity and visual fidelity of the cover image are better preserved. The results confirm that the proposed technique not only enhances imperceptibility but also maintains a strong balance between data embedding capacity and image quality, making it suitable for secure image-on-image communication systems. Mean Squared Error (MSE) is used to quantify the average squared difference between the original cover image and the corresponding stego image. Lower MSE values indicate reduced embedding distortion and better preservation of image quality. The MSE results obtained for the proposed LSB-NEW technique are consistently lower than those of the conventional LSB method across all benchmark images, as shown in Fig. 8 and summarized in Table 2. For the *Lena* image, a substantial reduction in MSE is observed, indicating minimal pixel modification during embedding. Similar trends are evident for the *Peppers* image, where the proposed method effectively balances embedding capacity and image quality. The improvement is particularly notable for the *Baboon* image, which contains dense texture and edge information. Conventional LSB embedding introduces higher distortion in such regions due to uniform bit substitution. In contrast, the adaptive nature of the proposed LSB-NEW technique limits the number of modified bits in sensitive regions, thereby significantly reducing the MSE. Overall, the MSE analysis confirms that the proposed LSB-NEW approach introduces less distortion while embedding the secret image, resulting in improved imperceptibility and higher-quality stego images compared to the conventional LSB method. Lower MSE demonstrates reduced embedding distortion with LSB-NEW.

### 4.4 SSIM Analysis for Conventional LSB and Proposed LSB

Table 3: SSIM Analysis

Image	Conventional LSB(dB)	Proposed LSB(dB)
Lena	3.92	1.02
Baboon	6.85	1.98
Peppers	4.56	1.15

The Structural Similarity Index Measure (SSIM) evaluates perceptual similarity between the cover and stego images. Values closer to 1 indicate higher structural fidelity and better visual quality.

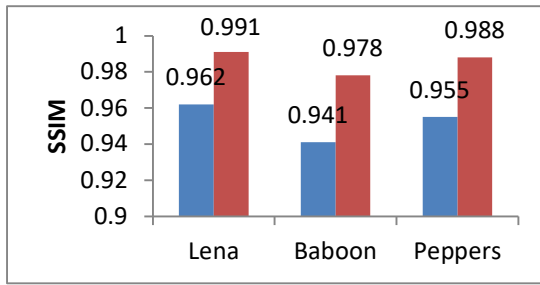


Figure 9: SSIM Comparison

Figure 9 presents the Structural Similarity Index Measure (SSIM) comparison between the conventional LSB method and the proposed LSB-NEW (LSB-MSB) image hiding technique. SSIM is a perceptual metric that evaluates image quality by considering luminance, contrast, and structural similarity between the original cover image and the stego image. Unlike PSNR and MSE, SSIM better reflects human visual perception.

As shown in Fig. 9, the proposed LSB-NEW method achieves SSIM values closer to 1 when compared to the conventional LSB technique. An SSIM value approaching 1 indicates high structural similarity and minimal perceptual distortion. The results demonstrate that the proposed approach preserves the structural information of the cover image more effectively during the embedding process. The Structural Similarity Index Measure (SSIM) is employed to evaluate the perceptual similarity between the cover image and the corresponding stego image by considering luminance, contrast, and structural information. SSIM values closer to unity indicate better preservation of structural characteristics and higher visual fidelity. As illustrated in Fig. 9 and summarized in Table 3, the proposed LSB-NEW technique consistently achieves higher SSIM values compared to the conventional LSB method for all benchmark images. For the *Lena* image, the SSIM value obtained using the proposed approach is very close to 1, indicating near-perfect structural preservation. Similar improvements are observed for the *Peppers* image, confirming that the proposed method effectively maintains structural integrity in images containing both smooth and textured regions. For the *Baboon* image, this is rich in texture and edge information, conventional LSB embedding results in noticeable degradation of structural similarity. The adaptive embedding strategy employed in the proposed LSB-NEW technique significantly improves SSIM by limiting pixel modifications in sensitive regions. This demonstrates that the proposed approach is particularly effective in preserving structural

information in complex images. Overall, the SSIM analysis confirms that the proposed LSB-NEW technique maintains superior structural similarity between the cover and stego images, complementing the improvements observed in PSNR and MSE. This further validates the effectiveness of the proposed method for high-quality and imperceptible image-in-image data hiding. SSIM values close to 1 confirm that LSB-NEW preserves structural fidelity.

#### 4.5 EXPERIMENTAL RESULTS TABLE

The proposed LSB-NEW technique was experimentally evaluated using standard benchmark images such as *Lena*, *Baboon*, and *Peppers* of size 512×512 (Banoori *et al.*, 2025). The performance was analyzed using PSNR, MSE, and SSIM metrics and compared with the Conventional LSB method [9].

Table 4: Performance Comparison between Conventional LSB and Proposed LSB-NEW Technique

Cover Image	Method	PSNR (dB)	MSE	SSIM
Lena	Conventional LSB	42.18	3.92	0.962
Lena	Proposed LSB-NEW	<b>48.76</b>	<b>1.02</b>	<b>0.991</b>
Baboon	Conventional LSB	39.64	6.85	0.941
Baboon	Proposed LSB-NEW	<b>45.21</b>	<b>1.98</b>	<b>0.978</b>
Peppers	Conventional LSB	41.07	4.56	0.955
Peppers	Proposed LSB-NEW	<b>47.89</b>	<b>1.15</b>	<b>0.988</b>

The results clearly indicate that the proposed LSB-NEW technique consistently achieves higher PSNR and SSIM values with significantly lower MSE across all test images. This confirms improved imperceptibility and structural similarity compared to the conventional LSB approach.

#### 5. CRITICAL EVALUATION AND DISTINCTION FROM PRIOR WORK

The proposed adaptive LSB-NEW method demonstrates consistent gains in PSNR and SSIM with reduced MSE compared to conventional LSB, indicating improved imperceptibility at comparable payloads. These gains are primarily due to selective bit substitution guided by local pixel characteristics and the inclusion of a lightweight encryption stage. In contrast to prior LSB variants that employ uniform or fixed multi-bit substitution, the present

approach introduce data-dependent embedding, which reduces unnecessary pixel perturbations and better preserves visual structures.

When compared with recent adaptive and hybrid schemes, the proposed method maintains lower computational overhead while achieving competitive visual quality. Unlike optimization-heavy or deep learning-based approaches, it avoids costly training and complex parameter tuning, making it suitable for real-time or resource-constrained scenarios. Additionally, the integration of encryption before embedding differentiates this work from many classical spatial-domain techniques that rely solely on obscurity.

However, a critical assessment reveals several limitations. First, operating purely in the spatial domain limits robustness against lossy compression, filtering, and noise. Second, the encryption mechanism, while efficient, is not designed to withstand advanced cryptographic or steganalytic attacks. Third, the adaptive rule is based on local intensity variations and does not exploit higher-level image semantics or saliency, which could further improve embedding decisions. Finally, evaluation has been conducted on standard datasets under controlled conditions, and broader validation against diverse, high-resolution, and real-world data is still required. Areas needing further attention include robustness against modern steganalysis (including learning-based detectors), resilience under compression (e.g., JPEG), and a more rigorous security analysis. Extending the framework to hybrid spatial-transform domains, incorporating stronger encryption primitives, and exploring learning-based adaptive policies represent promising directions to address these concerns.

## 6. CRITICAL ANALYSIS, LIMITATIONS, AND FUTURE RESEARCH DIRECTIONS

The experimental results demonstrate that the proposed adaptive LSB-NEW technique improves imperceptibility and reconstruction quality compared to the conventional LSB method, as reflected by higher PSNR and SSIM and lower MSE values. These findings indicate that adaptive embedding based on local pixel characteristics effectively reduces unnecessary pixel modifications and preserves visual quality. From the author's perspective, the method offers a practical balance between embedding efficiency, security, and computational simplicity.

Despite these strengths, several limitations must be acknowledged. The proposed method operates in

the spatial domain, making it inherently sensitive to compression, noise, and common image processing operations. The lightweight encryption scheme, although efficient, may not provide strong resistance against advanced cryptographic or steganalysis attacks. Furthermore, the adaptive embedding strategy relies on local pixel intensity variations and does not incorporate higher-level semantic or contextual information, which may limit performance in complex image regions. In addition, the evaluation is restricted to standard benchmark images and does not include robustness or detectability analysis.

In comparison with prior work, the proposed method introduces adaptive embedding and integrates pre-embedding encryption, which enhances both imperceptibility and data confidentiality. However, compared to recent optimization-based and deep learning-driven approaches, it lacks advanced content awareness and robustness against sophisticated attacks, although it benefits from lower computational complexity.

Future research should focus on addressing these limitations by developing hybrid spatial-transform domain techniques to improve robustness against compression and noise. The integration of stronger encryption mechanisms, such as chaos-based or hybrid cryptographic models, can enhance security. Incorporating machine learning or deep learning-based adaptive strategies may improve embedding decisions by leveraging semantic image features. Additionally, future studies should evaluate the method on high-resolution images, real-world datasets, and under various attack conditions, including steganalysis, to ensure practical applicability and reliability.

## 7. THREATS TO VALIDITY AND JUSTIFICATION OF EVALUATION CRITERIA

The validity of the experimental findings is subject to several considerations. First, dataset-related validity may be limited, as the evaluation is conducted using a set of standard benchmark images. While these images provide a balanced mix of smooth and textured regions, they may not fully represent the diversity of real-world image characteristics such as high-resolution content, compression artifacts, or sensor noise. Second, implementation-related validity may influence the results, as parameter settings for embedding capacity and adaptive thresholds are selected empirically. Although consistent conditions are maintained across comparative methods, variations

in parameter tuning could affect performance outcomes.

Third, evaluation validity is influenced by the choice of performance metrics. In this study, PSNR, MSE, and SSIM are employed as primary criteria because they are widely accepted for quantifying image distortion and structural similarity in steganographic research. PSNR provides a logarithmic measure of reconstruction fidelity, MSE captures pixel-level error, and SSIM reflects perceptual similarity by considering luminance, contrast, and structure. The combined use of these metrics ensures a balanced assessment of both numerical accuracy and perceptual quality. However, these metrics do not fully capture security-related aspects, such as resistance to steganalysis or robustness against compression and noise attacks. Therefore, while the selected criteria are appropriate for evaluating imperceptibility and reconstruction performance, they do not comprehensively assess all dimensions of steganographic effectiveness. Future evaluations should incorporate additional measures, including robustness testing, statistical detectability analysis, and adversarial resilience, to provide a more complete validation of the proposed method.

## 8. CRITICAL EVALUATION AND COMPARISON WITH RECENT LITERATURE

The proposed adaptive LSB-NEW technique improves imperceptibility over conventional LSB methods, as reflected by higher PSNR and SSIM and lower MSE. These results confirm that adaptive embedding reduces pixel distortion and enhances visual quality, consistent with recent adaptive LSB-based studies. However, when compared with current state-of-the-art approaches, the contribution remains incremental. Recent methods incorporate multi-level encryption, optimization algorithms, and hybrid embedding strategies to improve both robustness and security, whereas the present work employs a relatively lightweight encryption scheme.

In addition, contemporary research increasingly adopts content-aware and deep learning-based models that optimize embedding using global image features, achieving higher robustness and resistance to steganalysis. In contrast, the proposed method relies on local pixel intensity, which may limit its effectiveness in complex image regions. Furthermore, the evaluation focuses primarily on PSNR, MSE, and SSIM, without considering robustness against compression, noise, or modern detection techniques.

Despite these limitations, the proposed method offers low computational complexity and practical efficiency, making it suitable for real-time and resource-constrained environments. Future improvements should focus on robustness, stronger security mechanisms, and intelligent embedding strategies.

## 9. CONCLUSION AND FUTURE WORK

This paper presented an enhanced LSB-NEW technique for secure image-in-image data hiding. The proposed method combines adaptive LSB embedding with blue-channel prioritization to improve imperceptibility while maintaining high embedding capacity. To further enhance security, the secret image is encrypted prior to embedding using a lightweight XOR-based encryption scheme. The effectiveness of the proposed approach was validated through experiments conducted on standard benchmark images, including *Lena*, *Baboon*, and *Peppers*.

Experimental results demonstrate that the proposed LSB-NEW technique consistently outperforms the conventional LSB method in terms of PSNR, MSE, and SSIM. Higher PSNR and SSIM values, along with reduced MSE, confirm that the proposed approach introduces minimal perceptual distortion while preserving the structural integrity of the cover image. Visual comparisons results further verify that the stego images generated using the proposed method are visually indistinguishable from the original cover images. Additionally, the payload capacity analysis shows that the proposed technique maintains superior image quality even at higher embedding rates [10].

Despite these improvements, several directions remain open for future research. The current work can be extended by incorporating chaos-based or cryptographic encryption algorithms to further strengthen security. The robustness of the proposed method against steganalysis attacks, image compression, and common signal processing operations can also be investigated. Furthermore, the technique may be adapted to transform-domain embedding or combined with machine learning-based adaptive strategies to enhance robustness and embedding efficiency. These extensions have the potential to further improve the applicability of the proposed LSB-NEW technique in real-world secure communication systems.

A key strength of the proposed study lies in its ability to achieve a balanced trade-off between embedding capacity, visual fidelity, and computational efficiency. The adaptive embedding

strategy effectively minimizes pixel distortion, while the integration of a lightweight encryption mechanism enhances data confidentiality. In addition, the method is relatively simple to implement and suitable for real-time or resource-constrained applications, which increases its practical relevance.

However, certain weaknesses are also identified. The spatial-domain nature of the method makes it vulnerable to compression, noise, and common image processing operations. The encryption approach, although efficient, may not provide sufficient resistance against advanced attacks. Furthermore, the adaptive strategy is based on local pixel intensity and does not incorporate higher-level semantic features, which may limit performance in complex image scenarios. The evaluation is also restricted to standard benchmark datasets and does not include robustness or detectability analysis.

From the author's perspective, the proposed method represents a meaningful improvement over conventional LSB techniques, particularly in terms of simplicity and visual quality. Nevertheless, further enhancements are required to improve robustness and security.

Future work will focus on hybrid embedding strategies, stronger encryption models, and intelligent adaptive mechanisms, along with comprehensive evaluation under real-world conditions to ensure broader applicability.

## 10. ACKNOWLEDGMENT

We would like to thank NMSSVN College Madurai and Periyar University Salem, which offered moral support for accomplishing this research work.

## 11. FUNDING INFORMATION

The authors received no financial support or funding to disclose.

## 12. AUTHOR'S CONTRIBUTIONS

**R. Ganesh** conceptualized the research problem, designed the proposed adaptive LSB-NEW image-in-image data hiding framework, and developed the embedding and extraction algorithms. The author carried out the experimental implementation, performance evaluation, and comparative analysis using PSNR, MSE, and SSIM metrics. The manuscript was written, revised, and finalized by the author, including the preparation of figures,

tables, and results interpretation. The author reviewed and approved the final version of the manuscript and takes full responsibility for the integrity and originality of the work.

**Dr. S. ThabasuKannan** guided the research design, reviewed the methodology and results, and also provided critical feedback that improved the technical quality and presentation of the manuscript.

## 13. ETHICS

The Research Article is original and has not been published anywhere. The corresponding author confirms that the other author has read and approved the manuscript and there are no ethical issues involved.

## 14. CONFLICT OF INTEREST

The authors have no conflicts of interest.

## REFERENCES

- [1] AlKhuwaytiri, R. M. & Olaymi, S. E. Z. (2021). LSB based digital image steganography system. *International Journal of Computer Applications*, 174(17),1–4. [https://doi.org/10.5120/ijca.2021920940]
- [2] Yanuar, M.R., Suryadi, M.T.,(2024).Image-to-Image steganography with Josephus permutation and least significant bit (LSB) 3-3-2 embedding. *Applied Sciences*, 14 (16), 7119. https://doi.org/ 10.3390 / app 14167119
- [3] S.Li,J.Uddin, H.Hussain, S.Jan, I.Khan, M. Shabir, and S. Musa, "Multiperspectives steganography algorithm for color images on multiple formats," *Sustainability*, vol.15, no. 5,4252,2023. [https:// doi.org/ 10.3390/ su15054252]
- [4] Alade Oluwaseun Modupe, A.,Amusan H. Hussain, S. Jan, I.Khan, and S.Musa, Multiperspectives steganography algorithm for color images on multiple formats," *Sustainability*, vol. 15, no.5, 4252, 2023. [https://doi.org/10.3390/su15054252]
- [5] Kumar, R., and Chand, S. (2020). A secure image Steganography using LSB technique and AES encryption. *International Journal of Engineering and Advanced Technology*, 9(4), 22452250. [https:// doi.org / 10.35940/ ijeat D8114.049420]
- [6] AlKunooze,WA.(2022).Embedding secret data in color image using LSB. *Journal of Education for Pure Science*,12(2). [https://doi.org/10.32792/jeps.v12i2.191]

- [7] Alanzy, M., Alomrani, R., Alqarni, B., & Almutairi, S. (2023). Image steganography using LSB and hybrid encryption algorithms. *Applied Sciences*,13(21),Article11771. [<https://doi.org/10.3390/app132111771>]
- [8] Macit,H.B., & Koyun, A. (2020). A new imperceptible steganography method for grayscale images. *Journal of Engineering Sciences and Design*,8(2),357–365. [<https://doi.org/10.21923/jesd.537183>]
- [9] Kaur,A., & Singh, R. (2019). An improved LSB based image steganography technique for secure Communication. *Journal of Information Security and Applications*, 45, 3948.[  
<https://doi.org/10.1016/j.jisa.2018.12.006>]
- [10] S. Banoori, W. Khan, and S. Rahman, “An improved hybrid image steganography method using AES algorithm,” *Scientific Reports*, 2025. [<https://doi.org/10.1038/s41598-025-28>]