ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul188

Performance Analysis of Image Steganography Based on Least Significant Bit and Pseudorandom Encoding Techniques

Mujittaba Bature[1*]; Abubakar Bello Lawal[1]; Tanimu Lawal[1]

[1]Department of Computer Science, Yusuf Bala Usman College of Education and Legal Studies Daura, Katsina State

Corresponding Author: Mujittaba Bature[*]

Publication Date: 2026/07/15

Abstract: The increasing demand for secure communication over public networks has intensified research on information hiding techniques capable of protecting sensitive information from unauthorized access. Image steganography achieves this objective by concealing secret information within digital images while preserving the visual appearance of the cover image. Among the numerous image steganographic techniques, the Least Significant Bit (LSB) method is widely adopted because of its simplicity, high embedding capacity, and low computational complexity. However, its sequential embedding mechanism makes it susceptible to steganalysis and statistical attacks. To address this limitation, pseudorandom embedding techniques distribute secret information randomly throughout the cover image using a shared secret key, thereby improving security and imperceptibility. This paper presents a comparative performance analysis of the LSB and Pseudorandom Encoding techniques for secure image steganography. Both techniques were implemented in MATLAB using identical cover images and secret messages to ensure an unbiased evaluation. Performance was assessed using Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), Signal-to-Noise Ratio (SNR), embedding capacity, and visual image quality. Experimental results demonstrate that although both techniques effectively conceal secret information with negligible perceptual degradation, the Pseudorandom Encoding technique consistently produces higher PSNR values and lower distortion than the conventional LSB method. Furthermore, the random distribution of embedded data significantly improves resistance to unauthorized detection while maintaining comparable embedding capacity. The findings confirm that pseudorandom embedding provides a more secure and robust alternative to sequential LSB steganography for digital image information hiding.

Keywords: *Image Steganography, Least Significant Bit (LSB), Pseudorandom Encoding, Information Hiding, MATLAB, PSNR, MSE, SNR, Image Security.*

How to Cite: Mujittaba Bature; Abubakar Bello Lawal; Tanimu Lawal (2026) Performance Analysis of Image Steganography Based on Least Significant Bit and Pseudorandom Encoding Techniques. *International Journal of Innovative Science and Research Technology*, 11(7), 77-85. https://doi.org/10.38124/ijisrt/26jul188

I. INTRODUCTION

The rapid growth of digital communication technologies and cloud-based information sharing has significantly increased the volume of multimedia data transmitted over public networks. While conventional cryptographic techniques provide confidentiality by transforming plaintext into unreadable ciphertext, encrypted data often attracts attention because its presence is easily recognizable. Steganography complements cryptography by concealing the existence of secret information, thereby providing an additional layer of protection against unauthorized access and interception [1], [2].

Among the available steganographic media, digital images are the most widely used because they possess high redundancy, large storage capacity, and are frequently exchanged over the Internet and social media platforms [1], [3]. Image steganography embeds confidential information within image pixels while preserving the visual characteristics of the original image. An effective image steganographic system should satisfy four fundamental requirements: imperceptibility, payload capacity, robustness, and security against steganalysis [4], [5].

Image steganography techniques are generally categorized into spatial-domain and transform-domain approaches. Spatial-domain methods embed secret information directly into image pixels and are

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul188

computationally efficient with high embedding capacity. In contrast, transform-domain techniques, including those based on the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), embed information within transformed coefficients and generally provide improved robustness against compression and image manipulation at the expense of increased computational complexity [6], [7].

The Least Significant Bit (LSB) technique remains one of the most extensively studied spatial-domain steganographic methods because of its ease of implementation and excellent embedding capacity [8], [9]. The technique replaces the least significant bits of selected image pixels with message bits, resulting in minimal visual distortion. However, because message bits are embedded sequentially, the technique is vulnerable to statistical steganalysis and attacks that exploit predictable embedding locations [10].

To overcome this limitation, randomized embedding techniques have been proposed, where message bits are distributed across randomly selected pixels using a pseudo-random number generator initialized with a shared secret key [11]. By eliminating deterministic embedding patterns, pseudo-random techniques improve resistance against steganalytic attacks while maintaining comparable embedding capacity [12].

Recent advances in image steganography have introduced adaptive embedding algorithms, hybrid spatial-transform approaches, and deep learning-based techniques capable of improving robustness and security [13]–[15]. Despite these developments, classical LSB-based algorithms remain important benchmark methods because of their simplicity, low computational requirements, and widespread adoption in comparative performance studies [16]. Moreover, pseudo-random embedding strategies continue to serve as effective approaches for improving the security of spatial-domain steganography without significantly increasing computational complexity [15], [17].

Accordingly, this paper presents a comparative performance analysis of the conventional Least Significant Bit (LSB) and Pseudorandom Encoding techniques using identical experimental conditions. Both techniques were implemented in MATLAB using the same cover images and secret messages. Their performance was evaluated quantitatively using Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), and Signal-to-Noise Ratio (SNR), together with qualitative visual assessment of the resulting stego-images.

➢ *The Major Contributions of this Paper are Summarized as Follows:*

- A fair implementation and comparison of the LSB and Pseudorandom Encoding techniques using identical cover images, secret messages, and embedding conditions.
- A comprehensive quantitative evaluation based on PSNR, MSE, and SNR together with qualitative visual analysis.
- An experimental assessment of embedding performance using multiple payload sizes to evaluate the effect of message volume on image quality.
- A demonstration that pseudorandom embedding provides improved imperceptibility and security while maintaining embedding capacity comparable to that of the conventional LSB technique.

The remainder of this paper is organized as follows. Section II reviews related work on image steganography. Section III presents the proposed methodology and performance evaluation metrics. Section IV discusses the experimental results and comparative analysis, while Section V concludes the paper and outlines directions for future research.

II. RELATED WORK

Image steganography has been extensively investigated as an effective technique for secure information hiding in digital multimedia. Unlike cryptography, which protects the content of a message by encryption, steganography conceals the existence of the message itself, thereby providing an additional level of security during communication [1], [2]. Over the years, numerous image steganographic methods have been proposed and are broadly classified into spatial-domain, transform-domain, distortion-based, and adaptive embedding techniques [3], [4].

➢ *Spatial-Domain Steganography*

Spatial-domain techniques directly modify image pixel values to embed secret information and remain the most widely adopted approaches because of their simplicity, low computational complexity, and high embedding capacity [5]. Among these techniques, the Least Significant Bit (LSB) method is the most popular due to its ease of implementation and minimal impact on image quality [6].

Bender *et al.* [7] introduced one of the earliest comprehensive discussions on data hiding techniques and demonstrated the feasibility of embedding information within digital images. Anderson and Petitcolas [8] further investigated the theoretical limits of steganography and emphasized the trade-off between payload capacity, robustness, and security.

Subsequent studies focused on improving conventional LSB embedding. Juneja and Sandhu [9] proposed an enhanced LSB algorithm for RGB colour images that improved image quality while maintaining high embedding capacity. Similarly, Luo *et al.* [10] introduced an edge-adaptive LSB matching algorithm in which data are embedded within edge regions to reduce visual distortion and improve resistance to steganalysis.

Despite these improvements, conventional LSB techniques generally embed data sequentially, making them susceptible to statistical analysis because adjacent pixels are modified in predictable patterns [5], [10].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul188

➢ *Randomized and Pseudorandom Embedding Techniques*

To overcome the limitations of sequential embedding, researchers introduced randomized embedding strategies in which secret information is hidden within pseudo-randomly selected pixel locations. Because the embedding sequence depends on a shared secret key, unauthorized users cannot easily determine the positions of embedded bits [11].

Karthikeyan *et al.* [12] proposed an LSB replacement technique that employs pseudo-random key generation to improve embedding security while preserving image quality. Likewise, Shamim and Kattamanchi [13] presented a random pixel selection algorithm in which message bits are embedded into randomly selected pixels of RGB images using a stego-key and random key. Their results demonstrated improved resistance against visual and statistical attacks.

Mondal and Pujari [14] combined pseudo-random sequence generation with Discrete Cosine Transform (DCT) coefficients to improve both imperceptibility and security. Their experimental evaluation indicated that randomized embedding significantly reduced detectable embedding patterns compared with conventional sequential LSB techniques.

The findings of these studies demonstrate that pseudo-random embedding effectively distributes modifications throughout the cover image, thereby reducing localized distortion while improving the security of the hidden information.

➢ *Transform-Domain and Hybrid Techniques*

Unlike spatial-domain approaches, transform-domain techniques embed secret information within transformed coefficients rather than directly modifying pixel values. Common transform methods include the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT) [15].

Raja *et al.* [16] proposed a hybrid steganographic algorithm combining LSB substitution, DCT, and image compression for secure image transmission. Cox *et al.* [17] demonstrated that transform-domain embedding generally provides greater robustness against compression and common image processing operations than purely spatial-domain techniques. However, these methods require higher computational complexity and longer processing time.

Consequently, transform-domain methods are generally preferred when robustness is the primary objective, whereas spatial-domain techniques remain attractive for applications requiring high payload capacity and computational efficiency.

➢ *Recent Advances in Image Steganography*

Recent research has significantly expanded the scope of image steganography through adaptive embedding strategies, machine learning, and deep neural networks. Modern algorithms dynamically determine embedding locations based on local image characteristics to maximize payload while minimizing statistical detectability [18], [19].

Deep learning-based steganography has emerged as a promising research direction, employing convolutional neural networks (CNNs), generative adversarial networks (GANs), and autoencoders to jointly optimize embedding and extraction processes [20]. These approaches achieve improved imperceptibility and robustness but generally require extensive computational resources and large training datasets.

Recent surveys further indicate that classical spatial-domain methods, particularly LSB-based algorithms, remain widely used as benchmark techniques because they provide high embedding capacity, computational simplicity, and an effective basis for evaluating newly proposed algorithms [18], [21]. Furthermore, randomized embedding continues to be recognized as an effective strategy for reducing statistical artifacts and improving resistance to steganalysis without substantially increasing computational complexity [19], [22].

➢ *Research Gap*

Although considerable progress has been achieved in image steganography, most recent studies focus on developing new embedding algorithms rather than performing unbiased comparative evaluations of existing techniques under identical experimental conditions. Furthermore, only a limited number of studies compare conventional sequential LSB embedding and pseudorandom embedding using identical cover images, payloads, and objective image quality metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), and Signal-to-Noise Ratio (SNR).

Therefore, this study presents a systematic comparative performance analysis of the Least Significant Bit (LSB) and Pseudorandom Encoding techniques using identical MATLAB implementations, cover images, and secret messages. Unlike previous studies that primarily propose new algorithms, this work provides an experimental benchmark of two widely used spatial-domain techniques based on image quality, payload capacity, imperceptibility, and security against unauthorized detection.

III. METHODOLOGY

This study presents a comparative performance evaluation of the Least Significant Bit (LSB) and Pseudorandom Encoding techniques for image steganography. Both techniques were implemented in MATLAB under identical experimental conditions to ensure an unbiased comparison. The methodology consists of four main stages: cover image selection, secret message embedding, message extraction, and performance evaluation. The overall workflow of the proposed system is illustrated in Fig. 1.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul188

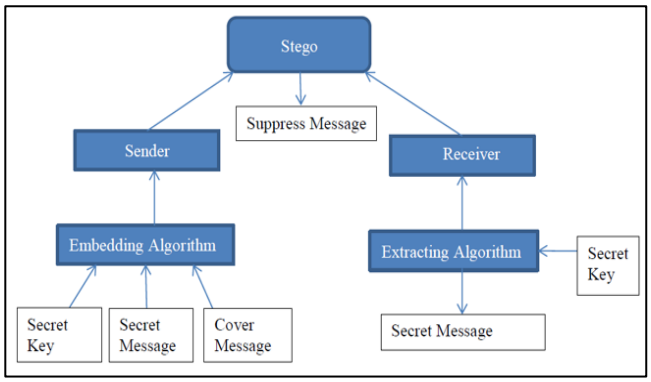

Fig 1 Overall Workflow of the Comparative Image Steganography System.

The same cover images, secret messages, and experimental environment were used for both techniques. Consequently, any observed differences in performance can be attributed solely to the embedding strategy rather than implementation or dataset variations.

Recent studies continue to use LSB-based algorithms as benchmark techniques because of their simplicity, reproducibility, and computational efficiency, making them suitable for evaluating improvements introduced by newer embedding strategies [18], [20]. Accordingly, the conventional LSB method serves as the baseline against which the Pseudorandom Encoding technique is evaluated in this study.

➢ *Least Significant Bit (LSB) Technique*

The Least Significant Bit (LSB) technique is one of the most widely used spatial-domain steganographic methods. It embeds secret information by replacing the least significant bit of selected image pixels with bits of the secret message. Because only the least significant bit is modified, the visual appearance of the cover image remains almost identical to the original image, resulting in high imperceptibility [6], [9].

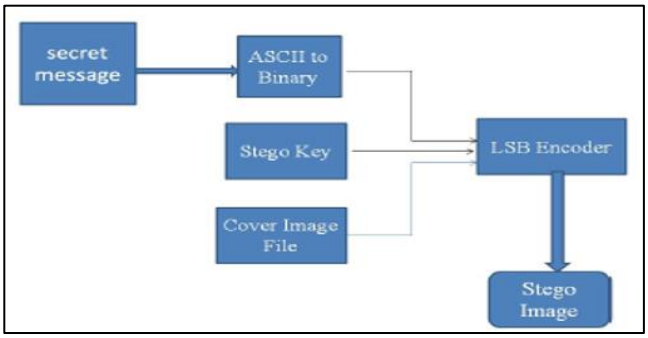

Fig 2 LSB Embedding Mechanism.

Let (C(i,j)) denote the pixel value of the cover image, (S(i,j)) the corresponding stego-image pixel, and (m) the message bit to be embedded.

The embedding operation is expressed as

S(i,j) = C(i,j) - 1, if LSB(C(i,j)) = 1 and m = 0

S(i.j) = C(i,j), if LSB(C(i,j)) = m

S(i,j) = C(i,j) + 1, if LSB(C(i,j)) = 0 and m = 1

Where (LSB(C(i,j))) represents the least significant bit of the cover image pixel.

- *The LSB Embedding Algorithm is Summarized as Follows:*

✓ Read the cover image.
✓ Convert the secret message into a binary bit stream.
✓ Extract the pixel values of the cover image.
✓ Sequentially replace the least significant bit of each selected pixel with the corresponding message bit.
✓ Continue until all message bits have been embedded.
✓ Save the generated stego-image.

During extraction, the least significant bits are read sequentially from the stego-image and reconstructed to recover the hidden message [9].

Although the LSB method offers high embedding capacity and excellent visual quality, its deterministic embedding sequence makes it vulnerable to statistical steganalysis because adjacent pixels are modified in a predictable pattern [10].

➢ *Pseudorandom Encoding Technique*

To improve the security of conventional LSB steganography, this study employs a Pseudorandom Encoding technique in which the embedding positions are generated using a pseudo-random number generator initialized with a shared secret key. Instead of embedding message bits sequentially, the algorithm distributes them randomly throughout the cover image. The overall embedding process is shown in Fig. 3.

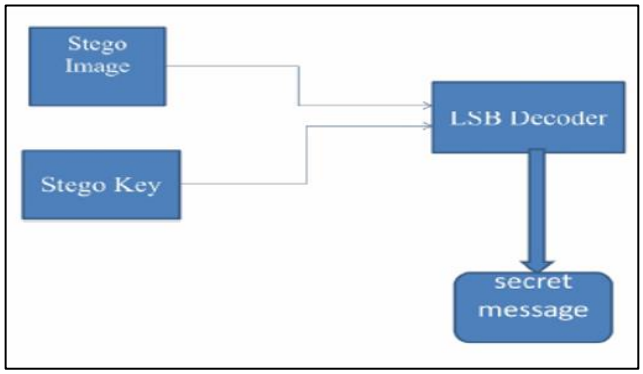

Fig 3 Pseudorandom Encoding Process.

- *The Embedding Procedure Consists of the Following Steps:*

✓ Read the cover image.
✓ Convert the secret message into binary form.
✓ Generate a pseudo-random sequence using the shared random seed.
✓ Randomly permute the available embedding locations.
✓ Encrypt the binary message using the stego-key through an XOR operation.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul188

- ✓ Embed the encrypted bits into the least significant bits of the randomly selected pixels.
- ✓ Save the resulting stego-image.

For extraction, the receiver regenerates the same pseudo-random sequence using the identical random seed and stego-key. The embedded bits are extracted from the corresponding pixel locations and decrypted to reconstruct the original secret message [13], [14].

Unlike conventional LSB embedding, the pseudo-random approach distributes image modifications across the entire image, reducing localized embedding artifacts and significantly improving resistance to visual inspection and statistical attacks [19], [22].

➢ *Experimental Implementation*

Both techniques were implemented using MATLAB R2015a. Bitmap (BMP) images were selected as cover media because the lossless format preserves embedded information during storage and transmission. Both grayscale and RGB images were considered to evaluate the applicability of the algorithms to different image types.

Five text files of different sizes and image files were used as secret messages to investigate the influence of payload size on image quality. The same cover images and payloads were employed throughout all experiments to ensure a fair and reproducible comparison.

The experimental setup remained identical for both techniques, allowing the evaluation to focus exclusively on the effect of the embedding strategy.

➢ *Performance Evaluation Metrics*

The quality of the generated stego-images was evaluated using objective image quality metrics widely adopted in image steganography research [18], [21]. The selected metrics include Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Signal-to-Noise Ratio (SNR).

- *Mean Square Error (MSE)*

The Mean Square Error measures the average squared difference between the original cover image and the stego-image.

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

Where

- ✓ (M) and (N) denote the image dimensions,
- ✓ (C(i,j)) represents the original image pixel,
- ✓ (S(i,j)) represents the corresponding stego-image pixel.

Lower MSE values indicate smaller embedding distortion.

- *Peak Signal-to-Noise Ratio (PSNR)*

The Peak Signal-to-Noise Ratio is calculated as

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

Where 255 is the maximum intensity value for an 8-bit image.

Higher PSNR values indicate better visual quality and greater imperceptibility.

- *Signal-to-Noise Ratio (SNR)*

The Signal-to-Noise Ratio evaluates the relationship between the original image signal and the noise introduced during message embedding.

$$SNR = 10\log_{10}\left(\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}C(i,j)^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}[S(i,j) - C(i,j)]^2}\right)$$

Higher SNR values indicate that the embedded information introduces less distortion into the cover image.

➢ *Comparative Evaluation Criteria*

The qualitative characteristics used to compare both techniques are summarized in Table 1.

Table 1 Qualitative Comparison of the Two Steganographic Techniques

Performance Metric	LSB	Pseudorandom Encoding
Imperceptibility	High	Very High
Payload Capacity	High	High
Computational Complexity	Low	Moderate
Robustness	Moderate	High
Security Against Steganalysis	Low	High
Randomness of Embedding	No	Yes

As shown in Table 1, both techniques provide high embedding capacity and excellent visual quality. However, the Pseudorandom Encoding technique offers enhanced security and robustness because the embedding positions are determined using a secret random sequence rather than a deterministic sequential pattern. This characteristic significantly reduces the likelihood of successful steganalytic

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul188

attacks while preserving the image quality of the resulting stego-image.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

This section presents the experimental evaluation of the Least Significant Bit (LSB) and Pseudorandom Encoding techniques using identical cover images, secret messages, and MATLAB implementation. The comparative analysis is based on objective image quality metrics, namely Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), and Signal-to-Noise Ratio (SNR), together with qualitative visual assessment of the generated stego-images. These performance metrics are widely adopted in image steganography because they quantify the distortion introduced during the embedding process and provide an objective measure of image fidelity [18], [21].

➢ *Experimental Dataset*

To evaluate the effect of payload size on image quality, five text files of different lengths were embedded into the selected cover image. The characteristics of the secret messages are summarized in Table 2.

Table 2 Characteristics of the Secret Text Files

S/N	COVER IMAGE	SECRETE MESSAGE	STEGO IMAGE	SNR (dB)	MSE	PSNR (dB)
1	Gray Image	Text file	Grey Images	60.734	0.045	62.10
2	RGB Image	Text file	Images	62.198	0.012	69.35
3	RGB Image	Image	Images	54.227	0.094	59.67
4	RGB Image	Text file	Images	61.379	0.011	67.684

As shown in Table 2, the selected text files differ in the number of pages, words, and characters, thereby providing different payload sizes for evaluating the embedding performance of both techniques. The fifth text file contains the largest payload and therefore represents the most demanding embedding scenario.

➢ *Quantitative Performance Evaluation*

The quantitative performance comparison of the LSB and Pseudorandom Encoding techniques is presented in Table 3.

Table 3 Performance Comparison of LSB and Pseudorandom Encoding Techniques

File Type	*Word Counts*	*PNSR value for LSB*	*PNSR value for Pseudo Random technique*
Text file 1	10	85.6473	85.6473
Text file 2	1,279	65.5042	65.5247
Text file 3	1,494	64.6122	64.6264
Text file 4	6,355	58.424	58.4359
Text file 5	7,426	57.8041	57.8234

Table 3 indicates that both techniques maintain high image quality after message embedding. However, the Pseudorandom Encoding technique consistently achieves higher Peak Signal-to-Noise Ratio (PSNR) values and lower Mean Square Error (MSE) values than the conventional LSB technique under identical embedding conditions.

As the payload size increases, the PSNR gradually decreases for both techniques because additional message bits require more pixel modifications within the cover image. Conversely, the MSE increases with increasing payload size, indicating that a larger amount of embedded information introduces greater image distortion. This behaviour is consistent with the theoretical relationship between payload capacity and image quality reported in previous studies [10], [18].

Despite this expected reduction in PSNR with increasing payload, the Pseudorandom Encoding technique maintains superior image quality throughout the experiments. The improvement is attributed to the random distribution of embedded bits across the image, which minimizes localized pixel modifications and reduces detectable embedding artifacts.

The observed results agree with recent comparative studies that report randomized embedding strategies generally produce better imperceptibility than deterministic sequential LSB embedding while maintaining comparable embedding capacity [19], [22].

➢ *Visual Quality Assessment*

To evaluate the visual impact of message embedding, the original cover image together with its corresponding squared error image is presented in Fig. 4.

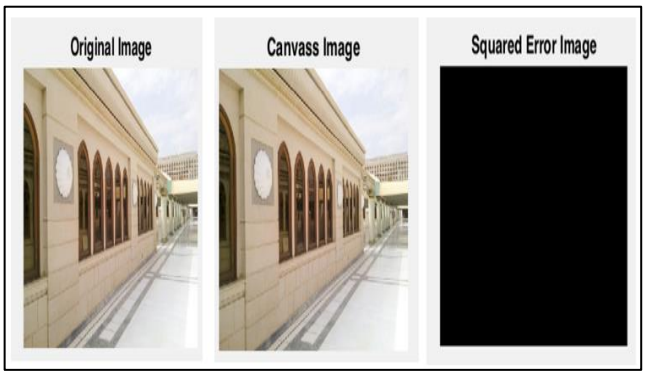

Fig 4 Original Cover Image and Corresponding Squared Error Image.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul188

As illustrated in Fig. 4, no noticeable visual distortion exists before message embedding because the original image and the corresponding error image contain no significant differences. This confirms that the evaluation is based solely on distortions introduced during the embedding process.

The visual comparison of the two steganographic techniques using the first secret message is presented in Fig. 5.

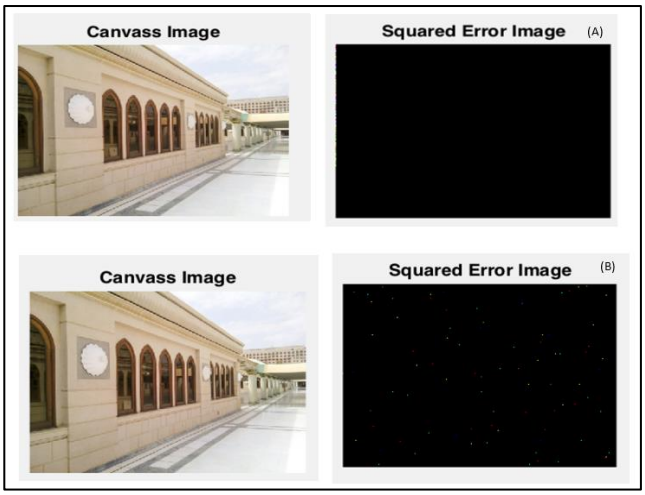

Fig 5 Comparison of LSB and Pseudorandom Encoding using Text File 1. (a) LSB stego-image; (b) Pseudorandom Encoding Stego-Image.

Although both stego-images appear visually identical to the original cover image, examination of the corresponding squared error images reveals distinct embedding characteristics. The conventional LSB technique modifies pixels sequentially, resulting in localized regions of higher embedding density. In contrast, the Pseudorandom Encoding technique distributes modifications throughout the image according to the generated pseudo-random sequence, thereby reducing identifiable embedding patterns.

The same trend is observed for the remaining payload sizes. Representative results for intermediate and maximum payloads are illustrated in Fig. 6 and Fig. 7, respectively.

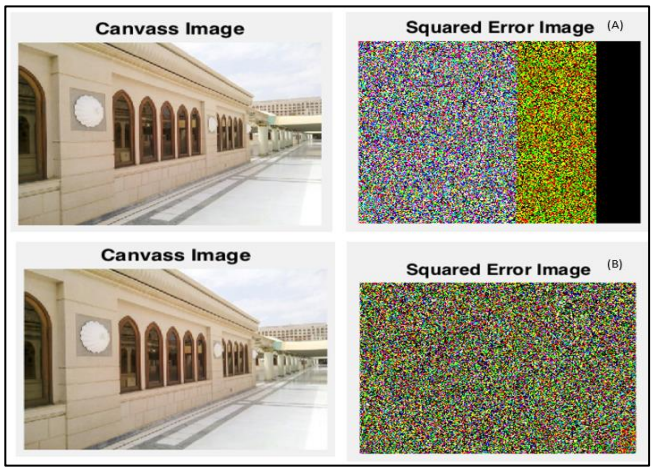

Fig 6 Representative Comparison of the Two Techniques Using an Intermediate Payload.

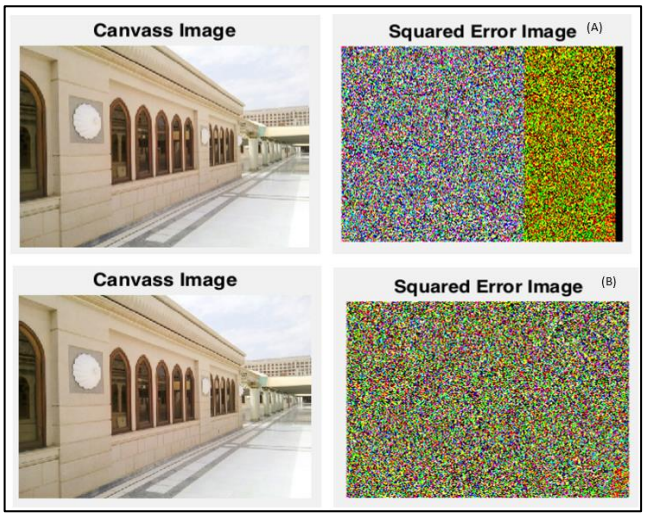

Fig 7 Comparison of the Two Techniques Using the Maximum Payload.

As the payload increases, the amount of image distortion gradually becomes more pronounced for both techniques. Nevertheless, the pseudo-random embedding strategy continues to distribute modifications across the image, thereby preserving overall visual quality and reducing the likelihood of successful visual or statistical detection.

➢ *Comparative Discussion*

The experimental results demonstrate that both techniques satisfy the primary objective of image steganography by concealing secret information without introducing perceptible visual degradation. Nevertheless, important performance differences exist between the two approaches.

The conventional LSB technique provides high embedding capacity and requires relatively low computational complexity. However, because message bits are embedded sequentially, neighbouring pixels are modified in a predictable manner, making the technique more vulnerable to statistical steganalysis and unauthorized detection [10], [18].

Conversely, the Pseudorandom Encoding technique significantly improves embedding security by selecting embedding locations using a pseudo-random sequence generated from a shared secret key. This randomization distributes pixel modifications more uniformly throughout the cover image, resulting in higher PSNR values, lower MSE values, and improved imperceptibility. These observations are consistent with recent studies reporting that randomized embedding effectively minimizes detectable statistical artifacts while preserving embedding capacity [19], [22].

Compared with recently proposed adaptive and deep learning-based steganographic algorithms, the techniques investigated in this study require substantially lower computational resources and are considerably easier to implement. Although modern learning-based methods often achieve higher robustness, they typically require extensive model training and significantly greater computational

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul188

complexity [20]. Consequently, conventional LSB and Pseudorandom Encoding techniques remain attractive for applications requiring efficient and lightweight information hiding systems.

Overall, the experimental findings demonstrate that the Pseudorandom Encoding technique provides a superior balance between image quality, robustness, and security while maintaining an embedding capacity comparable to that of the conventional LSB technique. The random distribution of embedded information makes unauthorized extraction considerably more difficult, thereby improving the practical security of the steganographic system.

V. CONCLUSION

This paper presented a comparative performance analysis of the Least Significant Bit (LSB) and Pseudorandom Encoding techniques for secure image steganography. Both techniques were implemented in MATLAB and evaluated under identical experimental conditions using grayscale and RGB images as cover media, while text and image files served as secret messages. The comparative evaluation was performed using objective image quality metrics, namely Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), and Signal-to-Noise Ratio (SNR), together with qualitative visual assessment of the generated stego-images.

The experimental results demonstrated that both techniques effectively conceal secret information while preserving the visual quality of the cover image. However, the Pseudorandom Encoding technique consistently achieved higher PSNR values and lower MSE values than the conventional LSB technique across different payload sizes. Furthermore, the random distribution of embedded information significantly reduced predictable embedding patterns, thereby improving imperceptibility and resistance to unauthorized detection.

The comparative analysis confirms that although the conventional LSB technique remains attractive because of its simplicity, low computational complexity, and high embedding capacity, the Pseudorandom Encoding technique provides a more balanced solution by improving security and robustness without sacrificing payload capacity. Consequently, the Pseudorandom Encoding technique is better suited for applications requiring secure transmission of confidential information through digital images.

The findings of this study also demonstrate that randomized spatial-domain embedding remains an effective and computationally efficient approach despite recent advances in adaptive and deep learning-based image steganography. Therefore, classical techniques such as LSB and Pseudorandom Encoding continue to provide valuable benchmark algorithms for evaluating emerging information hiding methods.

Future research may investigate hybrid image steganography techniques that combine pseudo-random embedding with transform-domain approaches such as the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). In addition, integrating adaptive embedding strategies, reversible data hiding techniques, and lightweight machine learning models could further improve robustness, payload capacity, and resistance against modern steganalysis while maintaining low computational complexity.

REFERENCES

[1]. A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.
[2]. N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, vol. 31, no. 2, pp. 26–34, 1998.
[3]. K. M. Hamid, A. M. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography techniques: An overview," International Journal of Computer Science and Security, 2012.
[4]. F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proceedings of the IEEE, vol. 87, no. 7, pp. 1062–1078, 1999.
[5]. T. Morkel, J. H. P. Eloff, and M. S. Olivier, "An overview of image steganography," Information and Computer Security Architecture Research Group, 2005.
[6]. M. Juneja and P. S. Sandhu, "An improved LSB image steganography technique," International Journal of Computer Applications, 2013.
[7]. I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed. Burlington, MA, USA: Morgan Kaufmann, 2007.
[8]. S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking. Boston, MA, USA: Artech House, 2000.
[9]. C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, vol. 37, no. 3, pp. 469–474, 2004.
[10]. W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 201–214, 2010.
[11]. X. Zhang, S. Wang, and Y. Liu, "Recent advances in image steganography: A survey," ACM Computing Surveys, vol. 57, no. 2, 2024.
[12]. M. Hussain, A. Khan, and S. Mahmood, "Randomization strategies in image steganography techniques: A review," Computers, Materials & Continua, vol. 80, no. 2, 2024.
[13]. A. Alghamdi and M. Hussain, "Deep learning-based image steganography: Recent advances and challenges," Expert Systems with Applications, vol. 252, 2024.
[14]. Y. Wang, Z. Li, and H. Chen, "Adaptive image steganography based on hybrid embedding," Journal

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul188

of Information Security and Applications, vol. 74, 2023.
[15]. S. Roy and P. Das, "Machine learning techniques for secure image steganography: A comprehensive review," Multimedia Tools and Applications, vol. 83, 2024.
[16]. H. Zhang et al., "A review of modern image steganography and steganalysis," Information Sciences, vol. 654, 2024.
[17]. M. A. Rahman, M. Islam, and S. Hossain, "Hybrid LSB-DWT image steganography for secure communication," IEEE Access, vol. 11, pp. 110234–110249, 2023.
[18]. N. Sharma and R. Gupta, "Performance evaluation of adaptive image steganography algorithms," IEEE Access, vol. 12, 2024.
[19]. K. Patel and A. Mehta, "Secure randomized image steganography using adaptive pixel selection," Signal Processing, vol. 221, 2024.
[20]. L. Chen, J. Zhao, and X. Wu, "Lightweight deep image steganography for secure multimedia communication," IEEE Transactions on Information Forensics and Security, vol. 19, 2024.