Iraqi Journal of Information and Communications Technology(IJICT)
Vol. 8, Issue 3, December 2025
www.ijict.edu.iq
ISSN:2222-758X
e-ISSN:2789-7362

SECURE INFORMATION EMBEDDING USING A FOUR-SLICE 2-BPS TECHNIQUE IN IMAGE STEGANOGRAPHIC

Zahraa Abbas Hassan[1]
[1] College of Computer Engineering, University of Technology, Baghdad, Iraq
Zahraa.A.Alzubydi@uotechnology.edu.iq[1]
Corresponding Author: **Zahraa Abbas Hassan**
Received:26/07/2025; Revised:05/09/2025; Accepted:05/10/2025
DOI:10.31987/ijict.8.3.347

***Abstract*- The heavy reliance on the internet for secure data transmission require strong and efficient methods to ensure confidentiality. This study suggests an enhanced steganographic method that embedded secret messages into grayscale images using a four slice Two Bit Plane Slicing (2-BPS) technique, random key generation and XOR-based embedding. The proposed method minimize complexity by dividing the cover image into four segments, thereby improving efficiency and security, unlike the traditional bit-plane slicing methods that depend on eight planes. The method was analyzed using the metrics performance like: Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), entropy, correlation, and histogram analysis. The results show high degree of non-perceptually, low deformation and flexibility against statistical and visual steganalysis. Furthermore, execution time tests confirm the method's computational efficiency, making it suitable for real-time applications. This approach provides a practical balance between visual quality, data security, and processing speed, with potential extensions to color and high-resolution images.**

keywords: **Image steganography, Plane slicing, Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Grayscale image.**

I. INTRODUCTION

The recent digital society faces a major challenge, that is finding a secure and efficient transfer of data along the keeping the anonymity of information until reaching to the recipient [1]. Encryption is the process of transforming data into a format that allows only authorized access and enables safe and secure communication between devices on networks. It's equivalent to present development in digital communication, where huge amount of data is being frequently transferred over multiple platforms [2]. One of the successful techniques for inserting information within an image processing is Steganography. This name is originated from the Greek word "Steganos" which mean "hide" and "graphing" which mean "to write" [3]. This technique includes hiding sensitive information within seemingly safe digital formats, likes images, audio recordings, or movies. The purpose of creating a secret communication path is to cover and hide the presence of the message. An image or other confidential material is used to covert channel for transmitting confidential information. Security is a major concern in digital communications system, especially when transmitting sensitive data over shared or public networks. Effective steganography techniques are essential, especially those that provide high protection against steganography and other concealment attempts [4]. A successful steganography technique must ensure that the embedded information is difficult for unauthorized individuals to discover or extract. Analyzing recent developments in steganography techniques requires the establishment of secure communication channels. Bit-Level Segmentation (BPS) divides a grayscale image into eight separate binary levels, known as bit levels. Secret data can be inserted into lower order level, frequently least significant bits, to decrease visual distortion and maintain the safety of embedded message [5][6].

ISSN:2222-758X
e-ISSN:2789-7362

Despite their effectiveness, standard steganography techniques exhibit several limitations. Methods that embed data into fixed positions, particularly the Least Significant Bit (LSB), are highly vulnerable to statistical attacks and simple detection algorithms. Embedding into higher-order bit planes often leads to visible distortions, reducing imperceptibility. Moreover, conventional eight-plane slicing increases complexity and reduces efficiency. These weaknesses highlight the need for a modified approach. The proposed system addresses these issues by applying a four-slice 2-BPS method combined with random key generation and XOR operations, which enhances confidentiality while reducing computational overhead.

II. RELATED WORKS

The security of the data is constantly considered as remarkable challenge which also attracted the considerable interest for the specialists involve in the research of novel digital field [7]. Consequently, it leads to a huge development to guarantee a secure data transmission via the network of the internet by employing many techniques for this purpose.

To emphasize the importance of picture security the author [8] examined a number of steganographic and encryption techniques designed to protect visual data. In [9] introduced a new method for hiding messages in color graphics by combining bit-plane slicing with a double XOR operation.

The security average witnessed a significant increase for the data equipped under the surface, if a technique involves a prime coded process has been engaged with the applied technology. An approach based on both (Local Binary Pattern (LBP) and Bit-Plane Slicing (BPS)) algorithms has been used to detect glaucoma was demonstrated by [10]. The characteristic of LBP help to color fundus images. Next to that, the images is distributed in to clarified channels (red, green and blue) and categorized to planes of bit. Triple Support Vector Machines (SVMs) were employed to categorize both decision-level fusion as well as decision-level fusion which was exploited to hit the last diagnosis.

In a separate piece of research, [11] developed a method that makes use of a hash function to replace the four least significant bits of the plaintext by the LSBs of a cover picture. This was done with the intention of embedding encrypted data within an image. A color-based facial segmentation approach was presented in [12]. This method combines spectral and spatial data by encoding images with Block Truncation Coding (BTC) and Bit-Plane Slicing (BPS). A steganography technique was proposed in [5] to enhance robustness and embedding capacity by adopting Bit Plane Slicing with Catalan Lucas sequence number. In [6] proposed more enriched techniques for image steganography by merging bit plane slicing with elliptic curve cryptography and wavelet transformation. To maximize protection against visual and statistical attacks a hybrid multi domain strategy using wavelet, spatial and ECC scrambled MSB planes was developed by [13]. Another strategy that helps in reducing the amount of distortion and detectability that appears in LSB based embedding and enhance the quality of stego image using Fibonacci bit plane was proposed by [14].

Recent advancements in image steganography have emphasized deep learning-based and hybrid frameworks for improving robustness and payload capacity [15][16][17]. For instance, [16] introduced CRoSS, a diffusion model for secure image steganography, while [17] applied hybrid crypto-steganography for efficient wireless communication security. Similarly, [18] proposed a color image segmentation method combining bit-plane slicing with block truncation coding. However, these approaches are often computationally intensive, making them unsuitable for lightweight or real-time applications.

ISSN:2222-758X
e-ISSN:2789-7362

This gap underscores the importance of developing efficient yet secure methods, such as the proposed four-slice 2-BPS technique.

III. STEGANOGRAPHY OVERVIEW

The method of hiding data inside cover media to make sure that the presence of the hidden data stays undetectable when it's transmitted through wireless and network channels is known as Steganography [7]. The hidden data can be transmitted by different media types like: video, audio, picture and any other computer files, the outcome of hiding a message into an image is known as "Stego image" [14][19]. Fig. 1 shows the major model of steganography, which typically includes a cover image, secret message, secret key and the resulting Stego image [20]. Moreover, the conceptual formula used to describe this process is shown in Eq. (1):

$$\text{Stego-medium} = \text{Cover medium} + \text{Secret message} + \text{Stego key} \tag{1}$$

Recent systems encrypt data before embedding it to improve security and strength [21]. In addition, a key component of

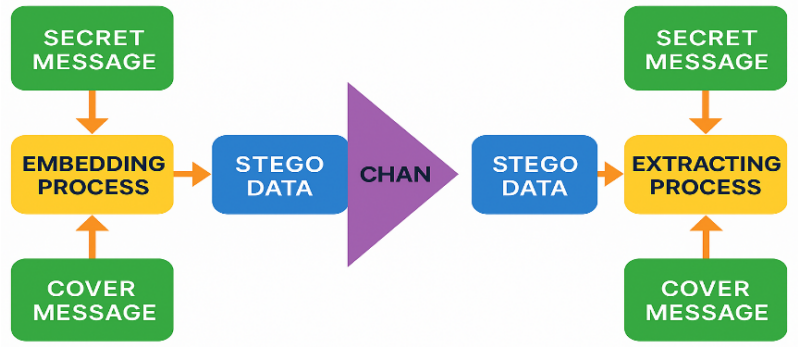

Figure 1: Block Diagram of Steganography.

successful steganographic systems is still finding and changing redundant bits in the cover media, which is the focus of current advancements in AI-driven steganography [15]. Furthermore, hybrid crypto-steganographic frameworks are increasingly used to protect data, especially in wireless communication environments [16].

IV. BIT PLANE SLICING (BPS)

It's a basic image analyzing method that splits an 8-bit grayscale image to eight separate binary images [1]. From bit plane 0 the least significant bit to bit plane 7 the most significant bit, each binary images represents a distinct bit position within the binary representation of the pixel [17],[22]. Selective data embedding at different significance levels is made easier by this hierarchical breakdown [23].

The visual clarity of the cover image is usually preserved and covert communication is made possible by embedding secret information in lower-order bit planes (such as LSBs) with negligible discernible deformation [21]. On the other hand, embedding in higher-order bit planes improves resilience to image processing attacks, although it may result in observable

ISSN:2222-758X
e-ISSN:2789-7362

image quality reduction [22]. A schematic illustration of bit plane slicing is shown in Fig. 2, where the MSBs are stored in bit-plane 7 while the LSBs of all pixels are contained in bit-plane 0. By precisely controlling the data embedding and extraction procedures in steganographic and digital watermarking applications, this technique efficiently portrays a picture by separating each bit of every pixel into distinct binary planes [20].

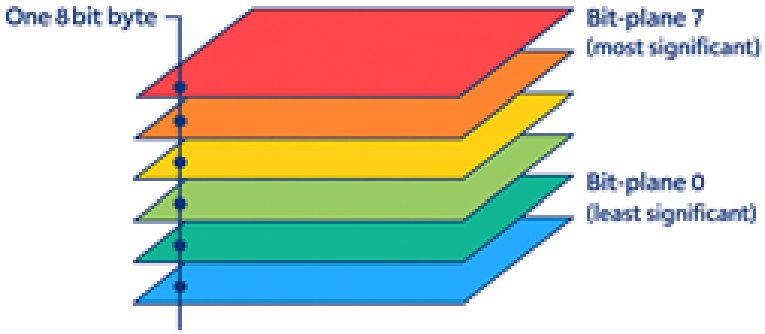

Figure 2: Bit Plane Slicing Method.

V. SYSTEM PERFORMANCE EVALUATION METRICS

A. *Mean Square Error (MSE)*

The mean squared difference among corresponding pixels in the original and stego images. It is calculated by Eq. (2), which is adopted from [23]:

$$\text{MSE} = \frac{1}{a+b} \sum_{i=1}^{a} \sum_{j=1}^{b} [M_1(i,j) - M_2(i,j)]^2 \tag{2}$$

Where:

- $a \times b$ is the image dimension (total number of pixels),
- $M_1(i,j)$ represents the pixel value at position (i,j) in the original image,
- $M_2(i,j)$ represents the pixel value at position (i,j) in the stego image.

A lower MSE value shows higher similarity between the two images.

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

PSNR calculating image quality and hidden data imperceptibility. Higher PSNR indicates better quality, it's calculated by Eq. (3) according to [24].

$$\text{PSNR} = 10 \log_{10} \left(\frac{\text{MAX}^2}{\text{MSE}} \right) \tag{3}$$

Where:

- MAX represents the maximum pixel value of the image,
- MSE represents the Mean Square Error between the original and stego images.

ISSN:2222-758X
e-ISSN:2789-7362

C. Coefficient of Correlation

The coefficient of correlation, denoted as r, is calculated to evaluate the direction and strength of the linear relation between two randomly selected parameters. A value of r near 0 suggests little to no linear association between the variables, whereas a value near to 1 shows a strong positive linear correlation. The correlation coefficient is computed by Eq. (4) as in [25]:

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\,\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}} \tag{4}$$

Where:

- x_i and y_i represent the values of the two parameters at instance i,
- $\bar{x}$ and $\bar{y}$ represent the mean values of x and y,
- n represents the total number of data points.

D. Histogram Analysis

An image histogram illustrates the distribution of pixel intensities in an indexed color image. It plays a key role in normalization by adjusting pixel values to span the full intensity range, thereby enhancing image contrast. This process improves visual differentiation with minimal distortion. The normalized pixel value $P(m, n)$ is computed by Eq. (5) as in [26]:

$$p(m,n) = \left(\frac{\text{Number of pixels at scale level } (m,n)}{\text{Total number of pixels}}\right) \times \text{Maximum scale level} \tag{5}$$

E. Entropy of Information

Measures the randomness of grayscale values in the image, indicating resistance to statistical attacks.
Let m be the number of possible grayscale levels, with each level e_i occurring with probability $P(e_i)$. The entropy is calculated by Eq. (6) according to [27]:

$$H(e) = \sum_{i=0}^{m-1} P(e_i)\,\log_2\big(P(e_i)\big) \tag{6}$$

VI. PROPOSED EMBEDDING AND EXTRACTION SYSTEM

A. Embedding Steps

1) **Image Slicing:** The grayscale image is divided into four 2-bit plane slices.
2) **Message Conversion:** The secret message is converted from ASCII to binary.
3) **Secret Key Generation:** A pseudo-random 6×6 matrix generated in MATLAB is scaled, rounded, and used to locate the embedding positions.
4) **Data Embedding:** Each 2-bit segment of the binary message is XORed with the corresponding 2-BPS images using the secret key.

Fig. 3 provides a visual overview of the proposed embedding process. It begins with preparing the grayscale image and the secret message, then proceeds through key generation and data embedding. The following steps outline each stage

ISSN:2222-758X
e-ISSN:2789-7362

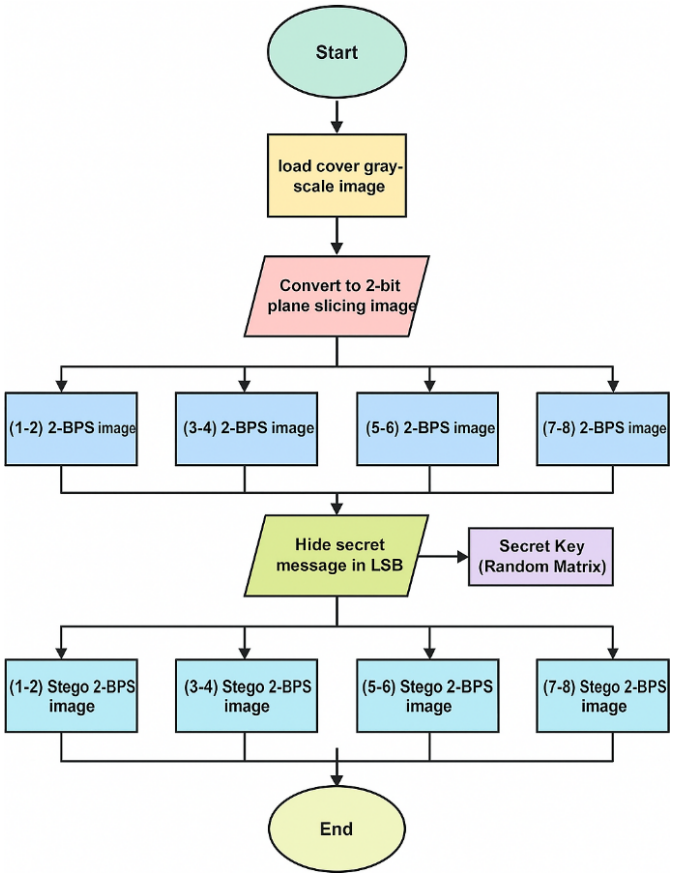

Figure 3: Embedding Steps.

in detail, illustrating how the confidential message is securely hidden within the image while preserving its quality. To illustrate the embedding process, consider the character "A," which in ASCII corresponds to the binary sequence 01000001. This sequence is divided into 2-bit parts: 01 | 00 | 00 | 01. Suppose the random key generates the sequence 11 | 01 | 10 | 00. Each 2-bit chunk of the message is XORed with the corresponding key sequence, producing 10 | 01 | 10 | 01. These encrypted parts are then embedded into the 2-BPS slices of the cover image. During extraction, the secret key is reapplied to retrieve the original binary sequence, which is then converted back to the ASCII character "A." This example shows the simplicity and strength of the embedding process.

B. Extraction Steps

1) **Image Slicing:** The grayscale image is divided into four 2-bit plane slices.
2) **Message Conversion:** The secret message is converted from ASCII to binary.
3) **Secret Key Generation:** A pseudo-random 6×6 matrix generated in MATLAB is scaled, rounded, and used to locate the embedding positions.

ISSN:2222-758X
e-ISSN:2789-7362

4) **Data Embedding:** Each 2-bit segment of the binary message is XORed with the corresponding 2-BPS images using the secret key.

Fig. 4 illustrate the process of extraction, the processes begin with restoring the stego image from the server and then use a secret key to locate the embedded bits. Following the identification of the bits, the full binary message is reconstructed and ultimately transformed into readable ASCII text. This process preserves the original image's quality and anonymity while guaranteeing an accurate recovery of the hidden information.

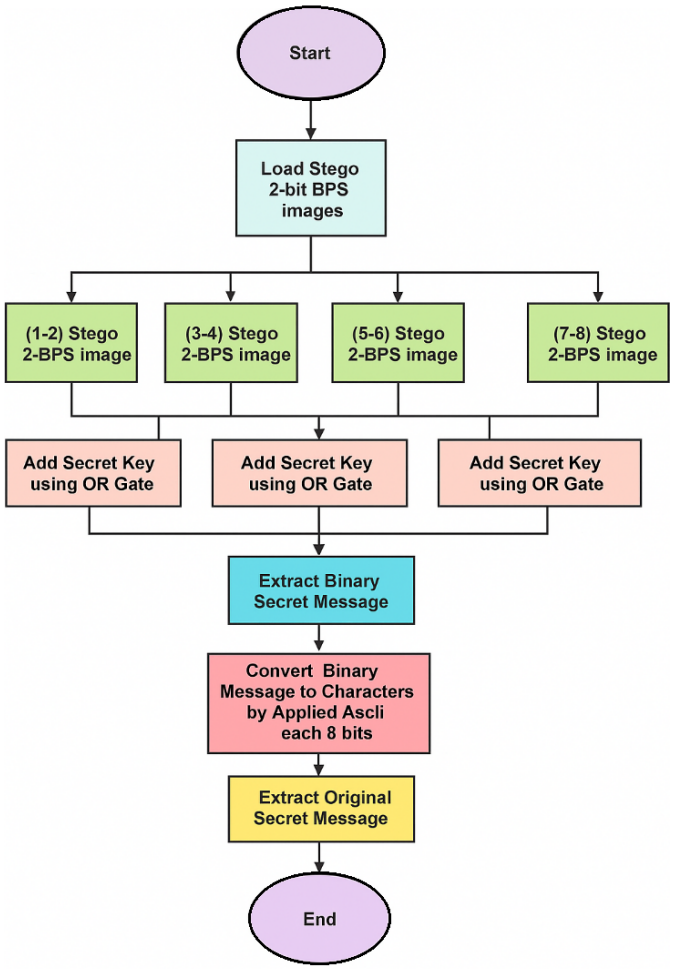

Figure 4: Extraction Steps.

VII. TEST AND RESULTS OF THE PROPOSED SYSTEM

This section shows the suggested image steganography system implementation and evaluation findings of using a sample beach image. The implementation stages are shown in Table I. The image was divided into 2-bit planes, and the secret message was embedded using random key-based OR operations. The modified stego-2-bit images were then analyzed for

ISSN:2222-758X
e-ISSN:2789-7362

visual quality, statistical integrity and histogram variation.

TABLE I
Implementation of Proposed System on Beach Image

Original Image	2-bit Plane	Stego-2-bit Plane
Beach Image	Beach-1-2	Beach-1-2-Stego
	Beach-3-4	Beach-3-4-Stego
	Beach-5-6	Beach-5-6-Stego
	Beach-7-8	Beach-7-8-Stego

Fig. 5 shows the visual outcome of the proposed system when applied to the sample beach image. Each row corresponds to a different 2-bit plane of the original grayscale image. The first column shows the unmodified original image for reference. The second column displays the extracted 2-bit plane pairs (0-1, 2-3, 4-5, and 6-7), revealing the intensity details captured at each level of bit significance. The third column presents the corresponding stego 2-bit planes after secret-message embedding. The side-by-side arrangement highlights that the stego planes maintain nearly identical visual patterns compared to their original counterparts, demonstrating that the hidden data does not introduce noticeable distortion across all bit layers.

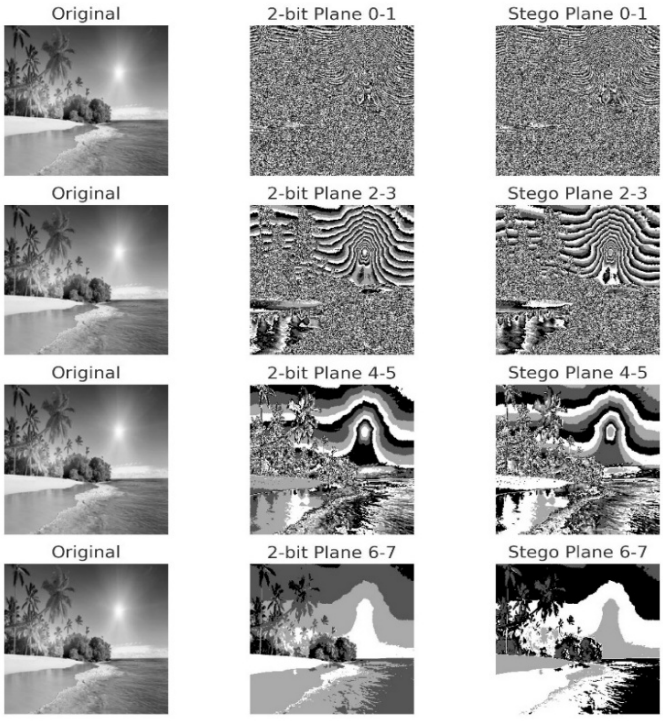

Figure 5: Implementation of Proposed System on Beach Image.

ISSN:2222-758X
e-ISSN:2789-7362

A. Evaluation Metrics

Table II summarizes the metrics evaluation such as: PSNR, MSR, Entropy Correlation. These metrics helps the imperceptibility, distortion, and security of the stego images. PSNR values remained high while MSE stayed low, indicating

TABLE II
Metric Evaluation of 2-bit vs Stego-2-bit Images (Beach Image)

Bit Plan	PSNR	MSE	Entropy	Correlation
Beach	—	—	7.7624	0.8421
Beach-1-2 S	93.1203	3.2087	4.4123	0.1543
Beach-3-4 S	87.0142	1.3015	4.3218	0.2258
Beach-5-6 S	92.9541	3.3102	4.1156	0.4076
Beach-7-8 S	86.9359	1.3354	3.6295	0.7951

minimal distortion. In addition to PSNR, MSE, entropy, and histogram analysis, execution time was measured to evaluate computational performance. The proposed method achieved an average embedding time of 0.45 seconds and extraction time of 0.39 seconds for a 512×512 grayscale image on a machine equipped with an Intel Core i7 processor and 16 GB RAM. These results indicate that the system is computationally lightweight and capable of supporting real-time applications, such as secure communication in wireless networks or real-time image sharing platforms. Entropy values suggest effective data embedding with high unpredictability, and correlation values reflect image structure integrity.

To improve the analytic clarity of the suggested method, this work presents the following graphical results based on PSNR Fig. 6, entropy Fig. 7, and correlation values from the stego images generated during the implementation phase Fig. 8.

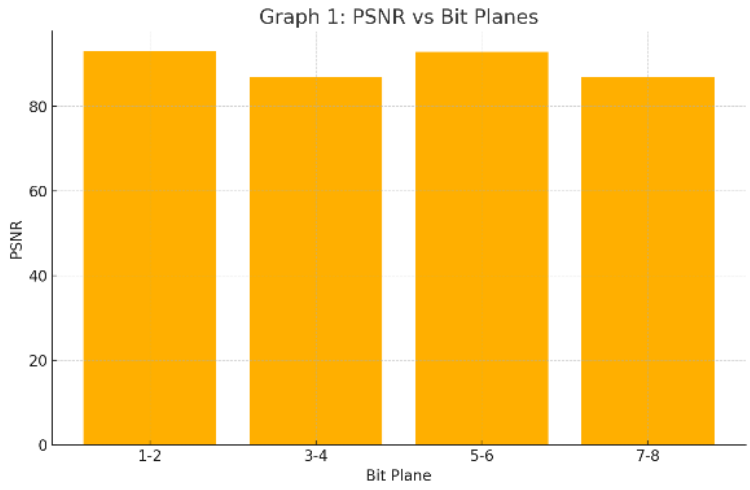

Figure 6: PSNR values across different 2-bit planes.

ISSN:2222-758X
e-ISSN:2789-7362

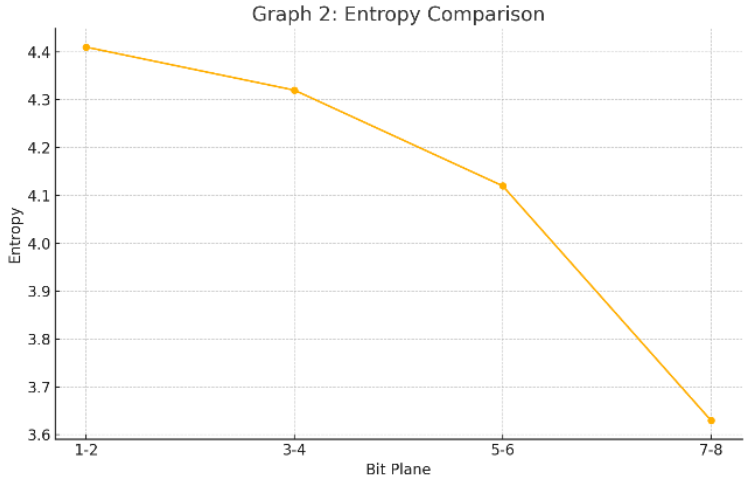

Figure 7: Entropy variation across bit planes indicating randomness and embedding strength.

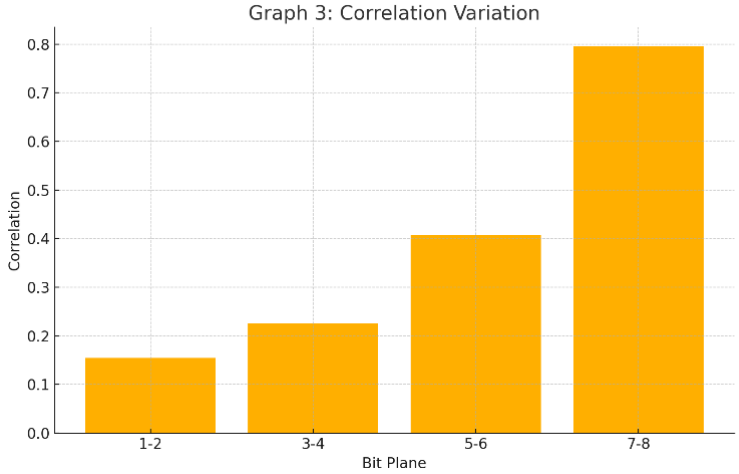

Figure 8: Correlation values showing structure similarity between original and stego images.

B. Histogram Analysis

To analyze visual uniformity and detect embedding traces, histograms that shown in Fig. 9 were generated for both original 2-bit planes and their corresponding stego images. Table III summarizes this comparison.

C. Comparative Evaluation

The performance of the proposed system is compared with previous works using key metrics, as shown in Table IV. the system introduces entropy and correlation as additional security evaluation parameters.

ISSN:2222-758X
e-ISSN:2789-7362

TABLE III
Histogram Comparison of 2-bit vs Stego Bit Planes

2-bit Plane	Stego Plane	Histogram Analysis
Beach-1-2	Beach-1-2-Stego	Slight variation, stable
Beach-3-4	Beach-3-4-Stego	No significant deviation
Beach-5-6	Beach-5-6-Stego	Visible contrast shift
Beach-7-8	Beach-7-8-Stego	Dense low-value bins

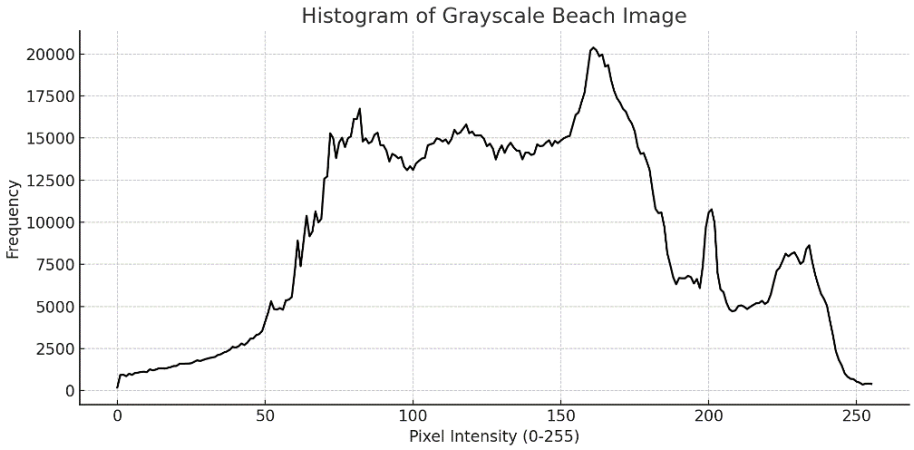

Figure 9: Histogram of Grayscale Beach Image.

TABLE IV
Comparison with Previous Works

Reference	PSNR Range	MSE Range	Entropy	Correlation
[7]	26.98 – 57.19	0.12 – 130.34	–	–
[8]	51.95 – 55.90	0.166 – 0.420	–	–
[9]	26.98 – 57.19	0.12 – 130.34	–	–
[10]	8.27 – 44.55	2.275 – 9668.1	–	–
Proposed	**86.93 – 93.12**	**1.30 – 3.31**	**3.62 – 4.41**	**0.15 – 0.79**

VIII. CONCLUSION

This study introduces a robust and efficient steganographic approach that securely embeds secret messages into grayscale images using 2-bit plane slicing combined with random key generation and XOR-based embedding. Through evaluation using metrics such as PSNR, MSE, entropy, correlation, and histogram analysis, the system demonstrated high imperceptibility and resilience against detection. The proposed method achieves an optimal balance between visual quality and data security. By integrating classical BPS techniques with modern key randomization methods, the system effectively addresses current challenges in secure data communication. Future work may explore its real-time application and extension to colored and high-resolution images. Future work may explore real-time implementation and adaptation to colored and high-resolution image contexts.

FUNDING

None.

ACKNOWLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] E. S. Hureib and A. A. Gutub, "Enhancing medical data security via combining elliptic curve cryptography and image steganography," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 20, no. 8, pp. 1–8, 2020.
[2] J. C. Maxwell, *A Treatise on Electricity and Magnetism*, 3rd ed., vol. 2. Oxford, UK: Clarendon Press, 1892, pp. 68–73.
[3] K. Mishra and R. Saharan, "Image encryption techniques using dynamic approach: An article review," *Ibn Al-Haitham Journal for Pure and Applied Sciences*, vol. 4, no. 36, 2023.
[4] U. A. Md Ehsan Ali and E. Ali, "A LSB based image steganography using random pixel and bit selection for high payload," *International Journal of Mathematical Sciences and Computing*, vol. 3, no. 2, pp. 24–23, 2021.
[5] K. Ashita and P. Smitha Vas, "Randomized steganography in skin tone images," *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, vol. 8, no. 2/3, pp. 1–8, 2018.
[6] S. Islam, M. A. Rehman, and M. S. Miah, "Steganography using bit plane slicing and Catalan–Lucas number sequence," *International Journal of Advanced Computer Science and Applications (IJACSA)*, 2022.
[7] S. Chandra and D. K. Yadav, "Efficient data hiding using bit-plane slicing for grayscale images," *International Journal of Computer Network and Information Security*, vol. 14, no. 4, pp. 41–50, 2022.
[8] M. N. Dhivya and M. S. Banupriya, "Network security with cryptography and steganography," *International Journal of Engineering Research & Technology (IJERT)*, vol. 8, no. 3, pp. 1–4, 2020.
[9] R. Roshini and C. Meena, "Review on steganography for hiding images and security issues," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 2, no. 10, pp. 424–428, Oct. 2020.
[10] B. Özdemir and N. Doğan, "Data hiding to the image with bit plane slicing and double XOR," *MANAS Journal of Engineering*, vol. 10, no. 1, pp. 66–72, 2022.
[11] S. Maheshwari, V. Kanhangad, R. B. Pachori, S. V. Bhandary, and U. R. Acharya, "Automated glaucoma diagnosis using bit-plane slicing and local binary pattern techniques," *Computers in Biology and Medicine*, vol. 105, pp. 72–80, 2019.
[12] Z. I. Nezami *et al.*, "An efficient and secure technique for image steganography using a hash function," *PeerJ Computer Science*, vol. 8, p. e1157, 2022.
[13] M. Ganavi, S. Prabhudeva, and N. P. H. Kumar, "Secure image steganography using multi domain hybrid approach," *International Journal of Computer Network and Information Security*, vol. 14, no. 4, pp. 60–68, 2022.
[14] A. A. Al Abdulla, H. Sellahewa, and S. A. Jassim, "Stego quality enhancement by Fibonacci bit plane mapping," *arXiv preprint arXiv:2004.12467*, 2020.
[15] R. Sangle *et al.*, "Unified multimedia steganography: AES-protected data concealment," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 11, pp. 1295–1305, 2023.
[16] J. Yu, X. Zhang, Y. Xu, and J. Zhang, "CRoSS: Diffusion model makes controllable, robust and secure image steganography," *arXiv preprint arXiv:2305.16936*, 2023.
[17] M. Helmy, "Audio transmission based on hybrid crypto-steganography framework for efficient cyber security in wireless communication system," *Multimedia Tools and Applications*, 2024.
[18] M. B. and G. Al-Khafaji, "A color facial image segmentation using bit plane slicing and block truncation coding techniques," *Iraqi Journal of Science*, vol. 65, no. 5, pp. 2828–2837, 2024.
[19] P. Mathur and A. K. Gupta, "A study of data hiding using cryptography and steganography," in *Proc. Int. Conf. Information Management & Machine Intelligence*. Springer, 2019, pp. 1–13.
[20] P. G. Kuppusamy *et al.*, "A novel approach based on modified cycle generative adversarial networks for image steganography," *Scalable Computing: Practice and Experience*, vol. 21, no. 1, pp. 63–72, 2020.
[21] S. Dhawan and R. Gupta, "Analysis of various data security techniques of steganography: A survey," *Information Security Journal: A Global Perspective*, vol. 30, no. 2, pp. 63–87, 2020.
[22] K. Kavitha and J. Anitha, "A survey on image steganography techniques," *International Journal of Computer Applications*, vol. 67, no. 19, pp. 6–11, 2013.
[23] B. Fesl, M. Koller, and W. Utschick, "On the mean square error optimal estimator in one-bit quantized systems," *IEEE Transactions on Signal Processing*, vol. 71, pp. 1968–1980, 2023.
[24] O. Keleş *et al.*, "On the computation of PSNR for a set of images or video," in *Proc. Picture Coding Symposium (PCS)*, Bristol, UK, 2021, pp. 1–5.
[25] T. Zheng *et al.*, "Correlation coefficients of interval-valued Pythagorean hesitant fuzzy sets and their applications," *IEEE Access*, vol. 8, pp. 9271–9286, 2020.
[26] Y. Li *et al.*, "A modified histogram equalization approach for image contrast enhancement," in *Proc. 2nd Int. Conf. Consumer Electronics and Computer Engineering (ICCECE)*, 2022, pp. 545–550.
[27] D. Xiang *et al.*, "Research on histogram equalization algorithm based on optimized adaptive quadruple segmentation and cropping of underwater image (AQSCHE)," *IEEE Access*, vol. 11, pp. 69356–69365, 2023.

