



# Hiding Secret Message into Gray Image Using 2-Bit Plan Slicing

Zahraa Abbas Al-zubaydi<sup>1\*</sup>, Layth kamil Almajmaie<sup>2</sup>, Israa Ali Al-Neami<sup>3</sup>, Maisa'a Abid Ali Khodher<sup>4</sup>

<sup>1</sup>Computer Engineering Department/ University of Technology-Iraq,Baghdad, Iraq

<sup>2</sup>Computer Engineering Department/ University of Technology-Iraq,Baghdad, Iraq

<sup>3</sup>Computer Engineering Department/ University of Technology-Iraq,Baghdad, Iraq

<sup>4</sup>Computer Engineering Department/ University of Technology-Iraq,Baghdad,Iraq

<sup>1</sup>Zahraa.A.Alzubaydi@uotechnology.edu.iq, <sup>2</sup>layth.k.adday @uotechnology.edu.iq,

<sup>3</sup>Israa.A.Alshaikhli@uotechnology.edu.iq, <sup>4</sup>110044@uotechnology.edu.iq

DOI: <https://doi.org/10.33103/uot.ijccce.25.1.4>

## ARTICLE HISTORY

**Received:** 08/January/2025

**Revised:** 02/February/2025

**Accepted:** 15/February/2025

**Available online:** 30/April/2025

## Keywords:

Steganography, Bit plane slicing BPS, Mean Square Error, Peak Signal to Noise Ratio.

## ABSTRACT

*The comprehensive utilization of the Internet has grown significant and widespread in contemporary times. Thus, the necessity for a robust method to facilitate the secure dissemination of data has emerged as a significant barrier for network users in the realm of data transmission. The proposed system comprises four stages: the first stage employs two-bit plane slicing (2-BPS) to partition the image into four sub-images (covers), the second stage transforms a secret message from ASCII to binary format; the third stage produces a random secret key; and the four stage conceal the secret message into the covers(2BPS) images. The results obtained the metrics: The Peak Signal-to-Noise Ratio(PSNR), mean square error (MSE), entropy, correlation, and histogram. This results of tests are efficient, resilient, transparent, capacious, and offer good security without the discovery of the secret message by adversaries. contribution to this research includes using the two-bit plane slicing (2-BPS) method, but this time by dividing the cover image into four images instead of eight followed by traditional methods.*

## I. INTRODUCTION

One of the biggest problems facing modern society is the efficient and secure transportation of data while preserving its anonymity until it reaches its intended receiver [1]. Ciphering is the process of converting data into a format that enhances security and enables its widespread use across network devices. It reflects the most recent advancements in digital methods, where digital data is a significant amount of information transmitted across multiple networks [2]. Techniques for image processing systems are numerous. one of these techniques is steganography. "Stego," meaning to conceal, and "graphical," meaning to write, are the Greek terms from which the phrase "information hiding" is derived. The act of hiding writing or information is frequently referred to by one of these phrases. With this technique, a secure link can be established [3]. The embedding procedure entails the careful selection of various materials, such as images, audio, and videos, with the purpose of creating a steganographic folder, or a folder that houses the hidden data. The matter of security poses a substantial problem in the realm of digital communications on a regular basis. Data can be guaranteed to be secure when transmitted over networks or to another person. To get access to confidential information, it is important to utilize a data concealment method that exhibits enhanced resistance against concealment attacks. We are currently in search of a secure connection in order to investigate the latest developments in steganography techniques [4]. one of these techniques utilizes the bit plane slicing method that partitions an image into its constituent binary planes. In Section IV, a comprehensive account of the approach is presented.

## II. RELATED WORKS

Data security is considered one of the important issues that has occupied the minds of researchers in the past years and up to the present time. Therefore, they have been constantly trying to find techniques and solutions to ensure the safety and security of data across internet networks [5].

**(R. Roshini et al., 2020)** [6] examined the importance of picture security and the overview of the existing body of research pertaining to diverse picture Steganographic and encryption methodologies.

**(Özdemir et al., 2022)** [7] introduced a novel method for the purpose of concealing messages within a color image. The developed algorithm incorporates bit-plane slicing and double XOR operation as its main elements. The first phase in the process entails the encryption of the message prior to its concealment. The aim of this strategy is to obtain a data concealment technique that is more secure.

**(Maheshwari et al., 2019)** [8] presented a novel methodology for the diagnosis of glaucoma, employing bit-plane slicing (BPS) and local binary pattern (LBP) approaches. Initially, the input color fundus image was separated into the red (R), green (G), and blue (B) channels, and then segmented into bit planes. Furthermore, we extracted comprehensive statistical characteristics from each bit plane of the various channels using Linear Binary Patterns (LBP). Moreover, we separately fed the acquired attributes from each channel into three separate support vector machines (SVMs) for classification purposes. At the decision level, the outputs produced by several Support Vector Machines (SVMs) are aggregated to classify the input fundus image as either normal or glaucoma.

**(Nezami et al., 2022)** [9] designed a system that utilized steganography techniques, where it had been encrypting text inside an image, replaced the 4 least significant bits (LSB) of the plain text with the cover image using a hash function.

**(Marwa and, Ghadah, 2024)** [10] introduces a new color-based face segmentation image that uses the spectral and spatial information of the image by encoding it using Bit Plane Slicing (BPS) and Block Truncation Coding (BTC), respectively.

### III. STEGANOGRAPHY

Steganography is a crucial technique that conceals data transmitted over networks. The primary objective is to uphold the privacy and protection of data by implementing and advancing methods that hinder unauthorized third-party access to send data via wireless internet and networks [5].

Steganography, which is known as "covered writing", is one of the techniques used to hide confidential and sensitive information and make it undetectable by attackers [11] [3]. This technology utilizes multimedia, including images, videos, audio, and other computer files, as carriers to convey the secret message. Once the message is embedded within one of these media, such as an image, we can refer to this image as a Stego image [12]. Fig. 1 illustrated the basic model of steganography, which includes a cover image, secret message, secret key, and Stego image [13].

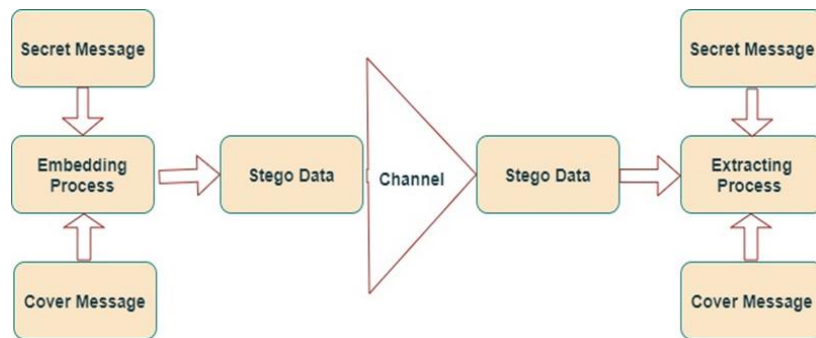


FIG. 1. BLOCK DIAGRAM OF STEGANOGRAPHY [13].

### IV. BIT PLANE SLICING BPS

The term "bit plane slicing" pertains to the procedure of partitioning an image into its constituent binary planes. Pixels are numerical values that are generated by the combination of multiple bits. An 8-bit image represents the intensity of each pixel using 8 bits. The 8-bit picture is comprised of eight 1-bit plane sections, as stated in reference [14]. These plane sections span from bit plane '0' (LSB) to bit-plane '7' (MSB). Fig. 2 [7] illustrates the schematic representation of bit-plane slicing. In the depicted picture, plane '0' covers the bits with the lowest order among all pixels, whereas plane '7' contains the bits with higher order. This methodology is employed to depict an image by allocating one or more bits of the byte to each individual pixel.

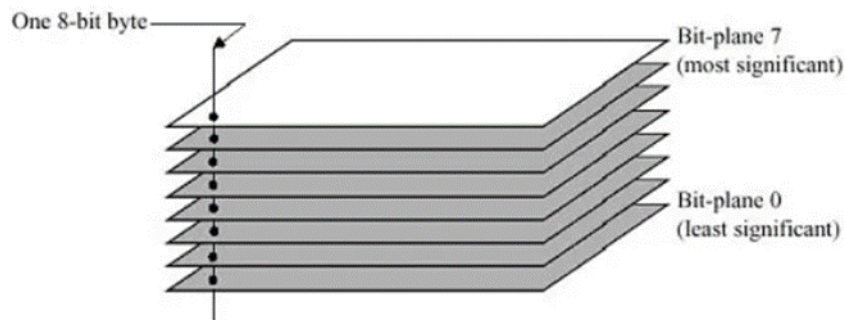


FIG. 2. BIT PLANE SLICING METHOD [7].

### V. EVALUATION SYSTEM PERFORMANCE

The system evaluation encompasses the use of several measures, such as mean square error (MSE), peak signal noise ratio (PSNR), correlation coefficient, histogram, and information entropy

[15], [16], [17]. The procurement of these metrics is crucial for the evaluation of innovative algorithms. The algorithm that has just been devised, which exceeds these measurements, can be considered a valuable algorithm.

#### A. Mean Squared Error (Mse)

The computation of Mean Squared Error (MSE) involves the comparison of byte counts between two images. Every individual pixel is composed of 8 bits, leading to a grand total of 256 levels that can be employed to depict various degrees of grey. The utilization of Mean Squared Errors (MSEs) proves advantageous in the comparison of bytes between two images. The Mean Squared Error (MSE) is calculated in (1) using the following method [18]:

$$MSE = \sum a \times b [M1(a \times b) - M2(a \times b)] / (a \times b) \quad (1)$$

#### B. Peak Signal Noise Ratio (Psnr)

The Peak Signal-to-Noise Ratio (PSNR) is a quantitative measure used to assess the degree of imperceptibility, expressed in decibels. The metric measures the numerical difference in quality between the two photographs. The presence of a high Peak Signal-to-Noise Ratio (PSNR) value indicates a negligible difference between two images. Conversely, a low peak signal-to-noise ratio (PSNR) indicates a notable degree of distortion between two images. Equation (2) calculates the Peak Signal-to-Noise Ratio (PSNR) in the following manner [19]:

$$PSNR = 1 - \log_{10} R^2(2) / MSE \quad (2)$$

#### C. Correlation Coefficient

The computation of the correlation coefficient, represented as  $r$ , is conducted in order to evaluate the magnitude and structure of the linear association between two variables that have been randomly chosen. When there is a strong association between two variables, the correlation coefficient tends to converge towards a value of 1. As the value coefficient approaches 0, it signifies the absence of a relationship between two variables. The coefficient  $r$  can be calculated using equation (3) [20]:

$$r = \sum i (x_i - \bar{x})(y_i - \bar{y}) / \sum i (\sum i (x_i - \bar{x})^2)^{1/2} (\sum i (y_i - \bar{y})^2)^{1/2} \quad (3)$$

#### D. Histogram

An image histogram is a visual depiction that showcases the dispersion of pixels across various degrees or indicators within the indexed color image. The histogram encompasses the fundamental information necessary for the process of picture normalization in situations when image pixels are of considerable length, with the aim of attaining a satisfactory degree of dissimilarity [21]. A histogram is utilized to visually represent the probable progression of the normalization technique. Normalization expanded the pixel levels to cover the entire range, hence increasing the image's dissimilarity. Equation (4) redefines the procedure of equalizing a new pixel value when implementing this technique [22].

$$P(m, n) = (\text{number of pixels with scale level}(m, n) / \text{Total number of pixels}) * (\text{maximum scale level}) \quad (4)$$

#### E. Information Entropy

Information entropy (IE) is a key measure of unpredictability in various disciplines such as lossless data compression, statistical inference, machine learning, and encryption. The present measure possesses the capacity to quantitatively assess the extent of grayscale value dispersion within a picture. A high level of information extraction (IE) leads to a uniform distribution of grey values. The security of a stenographic system is evaluated using the IE metric. Let  $m$  potential elements be represented as  $e_1, e_2, \dots, e_m$ , where each element has a probability  $P(e_1), P(e_2), \dots, P(e_m)$ . Entropy is mathematically represented by the equation (5).

$$H(e) = \sum_{i=0}^{m-1} P(e_i) \log_2 P(e_i) \quad (5)$$

This equation calculates the minimum number of bits needed to encrypt a series of bits, taking into account the frequency of the symbol [21].

## F. PROPOSED SYSTEM

This system includes the flowchart of the proposed system shown in *Fig. (3-a, b)*, which describing the proposed embedding and extraction secret message system.

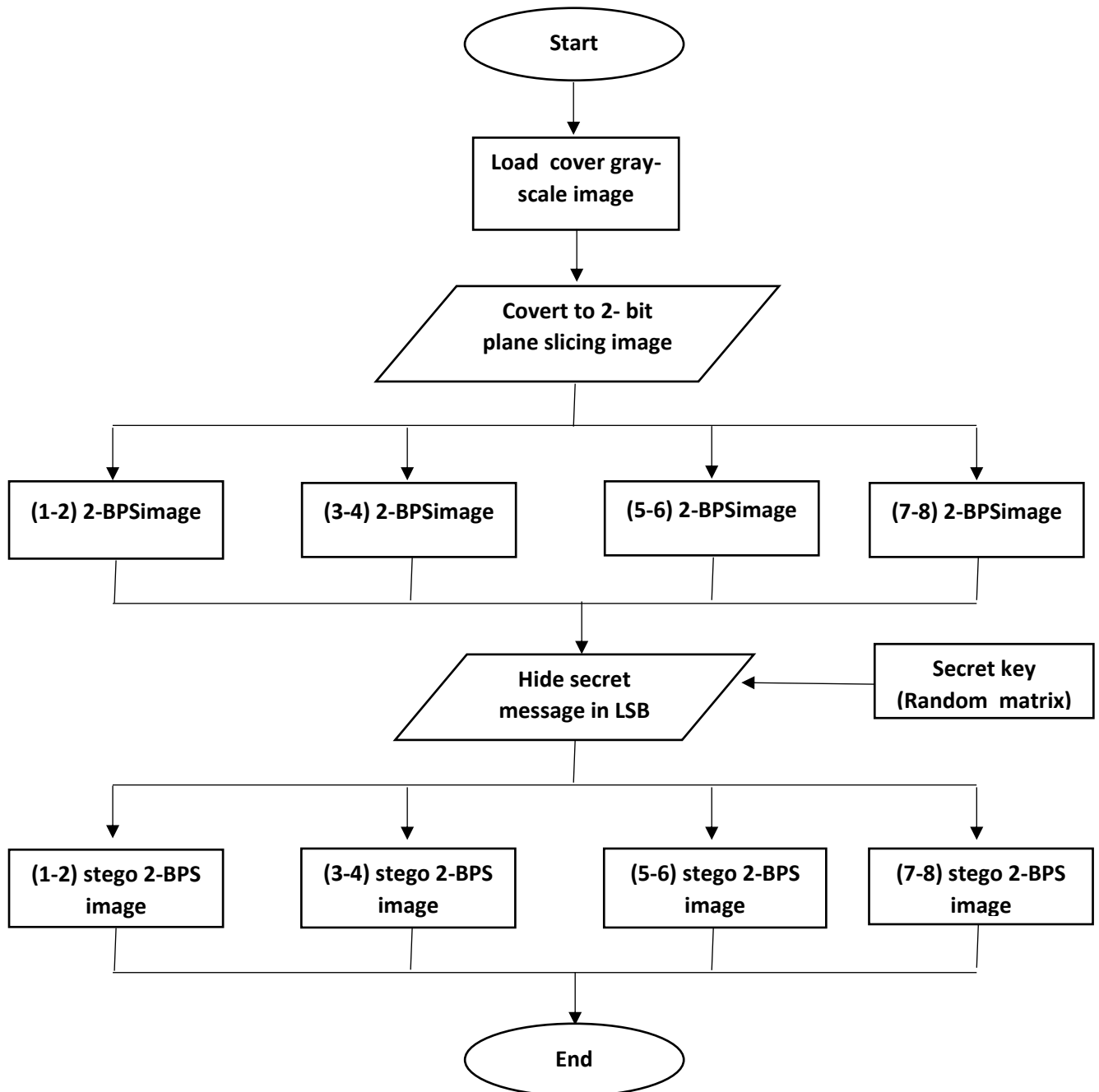


FIG. 3. (A) EMBEDDING SYSTEM EXTRACTION SYSTEM.

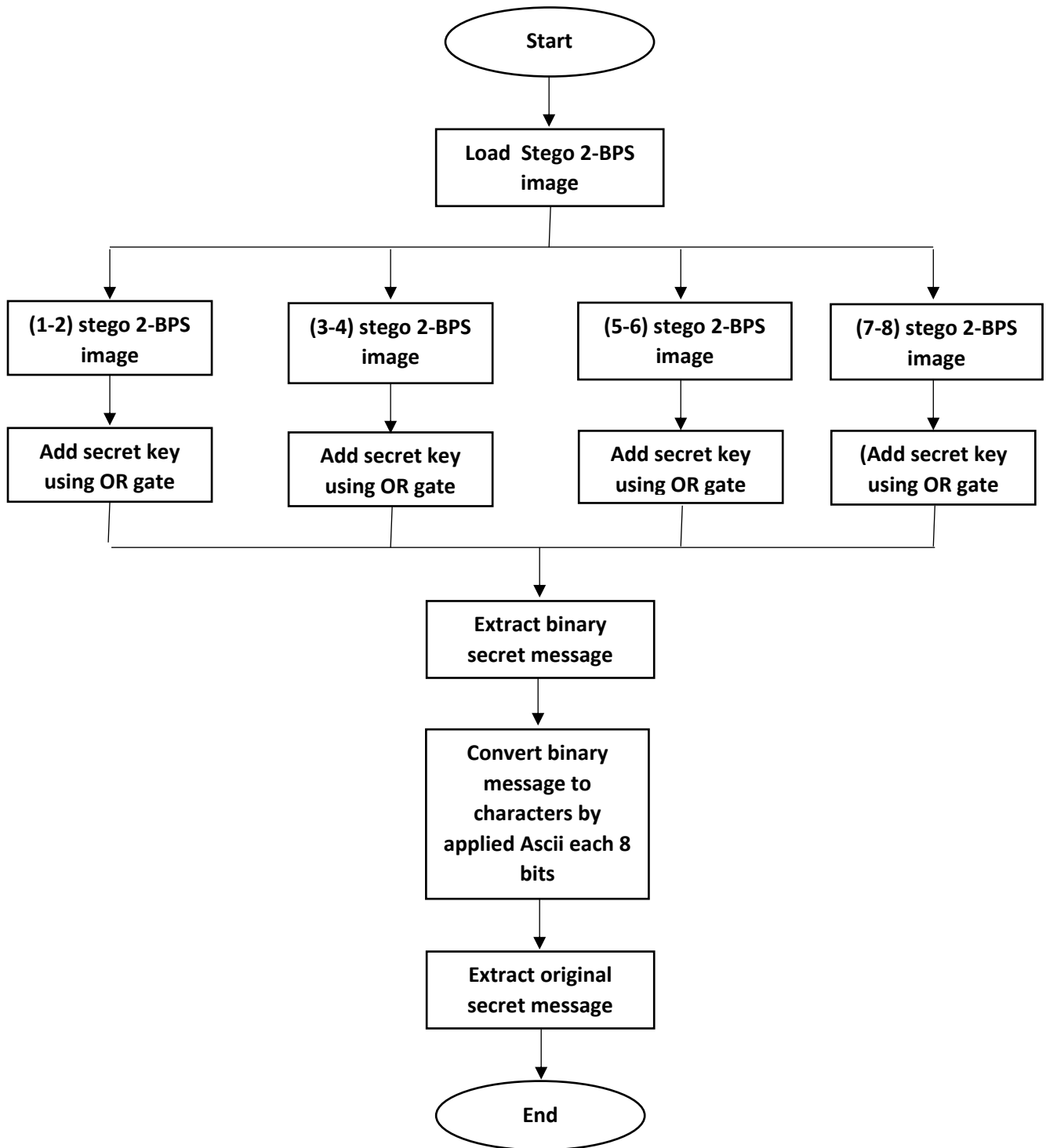


FIG. 3. (B) EMBEDDING SYSTEM).

- The proposed system involving four steps:

**Step 1:** In this step, the BPS methodology requires the use of an 8-bit slicing algorithm to include hidden information into a set of four slices. This methodology employs each number pixel represents by 8-bit binary, and each new image take 2- bit binary from 8-bit binary to generate four 2-bit plane images, as shown in *Fig. 4*. The value and function of individual bits in an image can be ascertained

by partitioning the digital image into separate bit-planes. The aforementioned technique, which has demonstrated comparable effectiveness in image compression, computes the total number of bits required to quantize each individual pixel.

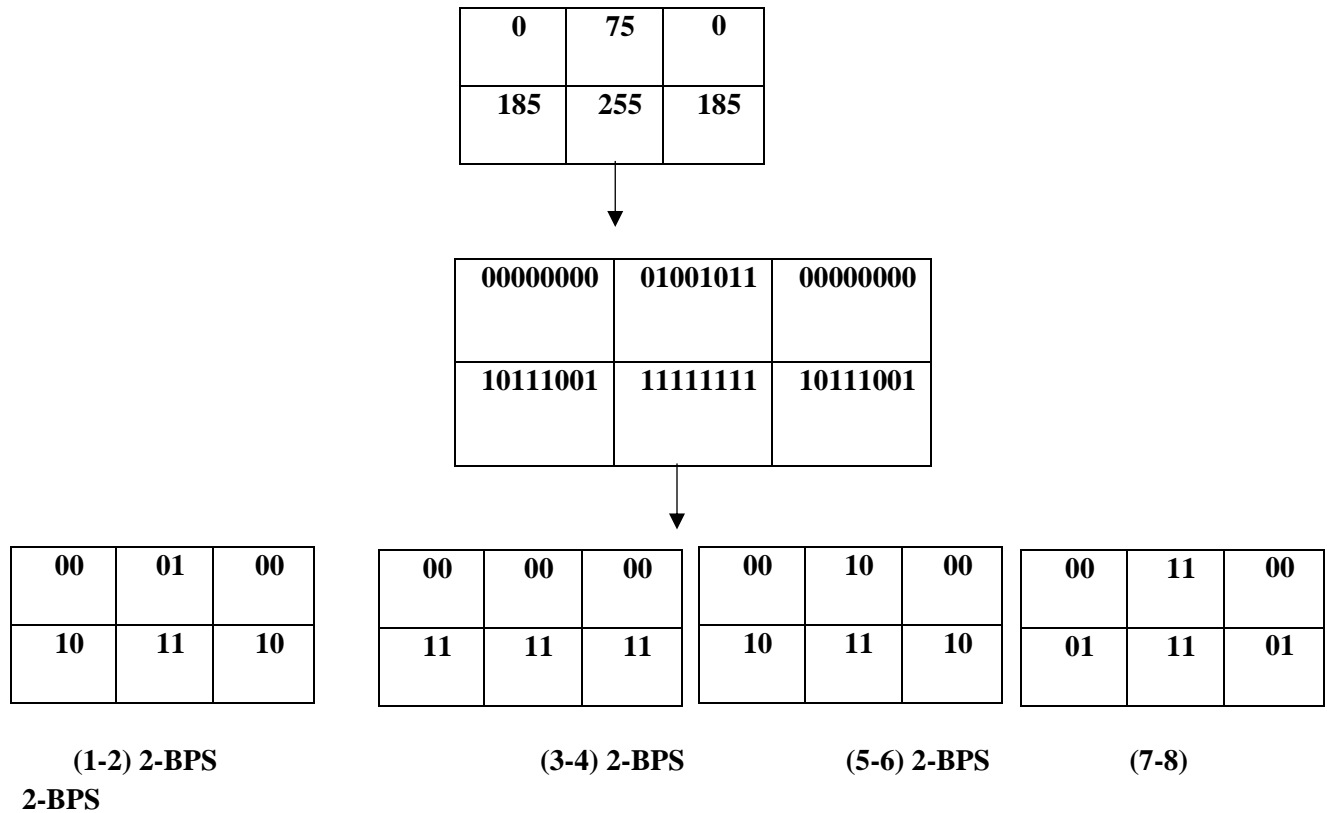

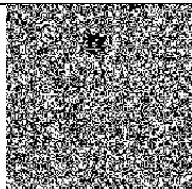

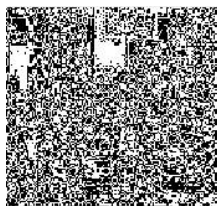


FIG. 4. DIVIDING GRAY SCALE IMAGE TO FOUR 2- BIT PLANE SLICING IMAGES.

- as shown in Table I, that are considered to cover gray image to hide a secret message into image 2-bit plan slicing.

TABLE I. CONVERT BINARY IMAGE TO FOUR 2-BPS IMAGES (COVERS)

Original image	2 bit plan
	
	1-2
	





**Step 2:** Convert the secret message characters from ASCII codes to binary format. *Fig. 5* demonstrates the typical process of translating ASCII letters into binary notation:

**The Computer Engineering is Very Good Study**

1010100 1101000 1100101 100000 1000011 1101111 1101101 1110000 1110101 1110100 1100101  
 1110010 100000 1000101 1101110 1100111 1101001 1101110 1100101 1100101 1110010 1101001  
 1101110 1100111 100000 1101001 1110011 100000 1010110 1100101 1110010 1111001 100000  
 1000111 1101111 1101111 1100100 100000 1010011 1110100 1110101 1100100 1111001

FIG. 5. SECRET MESSAGE CONVERSION FROM ASCII TO BINARY NOTATION.

Every character is given a distinct ASCII code. The character "T" corresponds to an ASCII number of 84, facilitating its translation into binary as an efficient approach to convert the complete secret message into binary notation.

**Step 3:** Generating the secret key from a random array using a MATLAB application, where the secret key determines the locations where the secret text is hidden within the cover (four 2-BPS images), Here is an array of size 6x6 that is generated using the instruction (rand): X= rand (6)

X=

0.2760	0.9597	0.5060	0.1493	0.9293	0.3517
0.6797	0.3404	0.6991	0.2575	0.3500	0.8308
0.6551	0.5853	0.8909	0.8407	0.1966	0.5853
0.1626	0.2238	0.9593	0.2543	0.2511	0.5497
0.1190	0.7513	0.5472	0.8143	0.6160	0.9172



<b>0.4984</b>	<b>0.2551</b>	<b>0.1386</b>	<b>0.2435</b>	<b>0.4733</b>	<b>0.2858</b>
---------------	---------------	---------------	---------------	---------------	---------------

The matrix is multiplied by 10 and then rounded (round instruction to the nearest integer to generate the secret key, which identifies the locations where the secret message is hidden.

$Z = 10 * (x)$

$Z =$

<b>2.7603</b>	<b>9.5974</b>	<b>5.0596</b>	<b>1.4929</b>	<b>9.2926</b>	<b>3.5166</b>
<b>6.7970</b>	<b>3.4039</b>	<b>6.9908</b>	<b>2.5751</b>	<b>3.4998</b>	<b>8.3083</b>
<b>6.5510</b>	<b>5.8527</b>	<b>8.9090</b>	<b>8.4072</b>	<b>1.9660</b>	<b>5.8526</b>
<b>1.6261</b>	<b>2.2381</b>	<b>9.5929</b>	<b>2.5428</b>	<b>2.5108</b>	<b>5.4972</b>
<b>1.1900</b>	<b>7.5127</b>	<b>5.4722</b>	<b>8.1428</b>	<b>6.1604</b>	<b>9.1719</b>
<b>4.9836</b>	<b>2.5510</b>	<b>1.3862</b>	<b>2.4352</b>	<b>4.7329</b>	<b>2.8584</b>

Round(z)

Secret key =

<b>3</b>	<b>10</b>	<b>5</b>	<b>1</b>	<b>9</b>	<b>4</b>
<b>7</b>	<b>3</b>	<b>7</b>	<b>3</b>	<b>3</b>	<b>8</b>
<b>7</b>	<b>6</b>	<b>9</b>	<b>8</b>	<b>2</b>	<b>6</b>
<b>2</b>	<b>2</b>	<b>10</b>	<b>3</b>	<b>3</b>	<b>5</b>
<b>1</b>	<b>8</b>	<b>5</b>	<b>8</b>	<b>6</b>	<b>9</b>
<b>5</b>	<b>3</b>	<b>1</b>	<b>2</b>	<b>5</b>	<b>3</b>

**Step 4:** This step includes the embedding method, which conceals the secret message within the four 2-BPS images using a secret key that determines the hiding locations. After determining the replacement position, the 2 least significant bits of the hidden message are substituted with the 2-LSB of the covers to generate four Stego 2-bit plane images.

- It is possible to clarify the fourth steps in the following embedding algorithm:

#### **Embedding Algorithm 1:**

##### **Process:**

Input: Cover 2-BPS image, Secret message, Secret key.

Output: Stego 2-BPS images.

Initial:

A= Load cover 2-BPS images.

B= Load secret message.

C= Binary secret message.

D= Load Secret key

E=Load XOR operation to hide secret message

F= Stego 2-BPS images.

G= Save stego 2-BPS in server.

Step 1: Loading cover 2-BPS images in A.

Step 2: Loading secret message in B.

Step 3: Encoded a confidential message into 8-bit binary format using ASCII encoding in the C computer language.

Step 4: Find locations into cover image for select from secret key for hide each 2-LSB bits from secret message uses XOR operation in E.

Step 5: Put the Result Stego-2-BPS image in F.

Step 6: Send the Stego object to the server and store it in the G.

- The method for obtaining the secret message may also be explained using a following extraction algorithm:

### **Extraction Algorithm 2:**

#### **Process:**

Input: Secret key, Stego-object

Output: Extraction secret message from server in database.

Initial

A= Retrieve stego-object by sensor authorize.

B= Load Stego 2-BPS images.

C= Load secret key

D= Binary secret message.

E= Set character of secret message.

F= Secret Message.

Step 1: Retrieve stego-object from database in server by sensor authorize in A.

Step 2: Load Stego 2-BPS image in B.

Step 3: Load secret key in C.

Step 3: Find binary secret message bit from Stego 2-BPS image by using secret key to select locations existent into hide 2 LSB bit from secret message into each pixel using OR operation from LSB in D.

Step 4: Convert set of binary bit each 8-bit is character, and repeat all bits in E. Step 5: Put the Result secret message in F.

End

## **VI. TEST AND RESULTS OF PROPOSED SYSTEM**

This section is divided into two parts: the results section and the results discussion section.

### **A. The Results**

This section indicates the implementation of the proposed system in Table (II-a, b, c); Table (III) indicates measurements of the system between 2-bit plain and Stego-2-bit plan images, and Table (IV-a, b, c) indicates the histogram between the 2-bit plan and Stego 2-bit plain images.

TABLE (II-A) IMPLEMENTATION PROPOSED SYSTEM BETWEEN ORIGINAL IMAGE AND 2-BIT PLAN AND STEGO-2-BIT PLAN IMAGES.


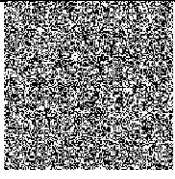
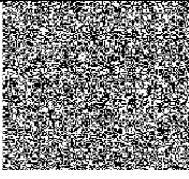

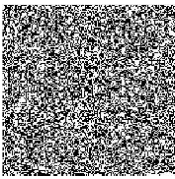
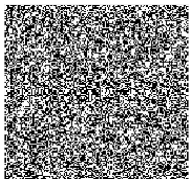

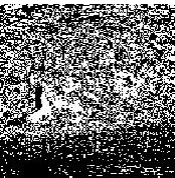
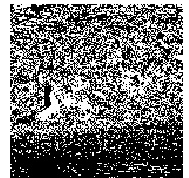


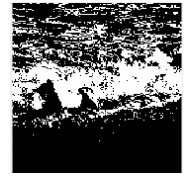

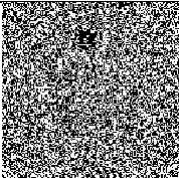
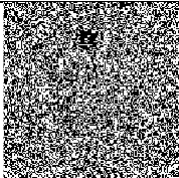

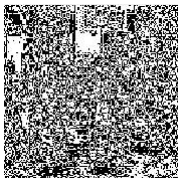
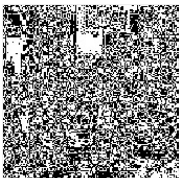
Original image	2-bit plane	Stego-2-bit plane
		
13	13-1-2	13-1-2
		
13	13-3-4	13-3-4
		
13	13-5-6	13-5-6
		
13	13-7-8	13-7-8

TABLE (II-B) IMPLEMENTATION PROPOSED SYSTEM BETWEEN ORIGINAL IMAGE AND 2-BIT PLAN AND STEGO-2-BIT PLAN IMAGES.

Original image	2 bit plan	Stego-2 bit plan
		
336	336-1-2	336-1-2
		
336	336-3-4	336-3-4

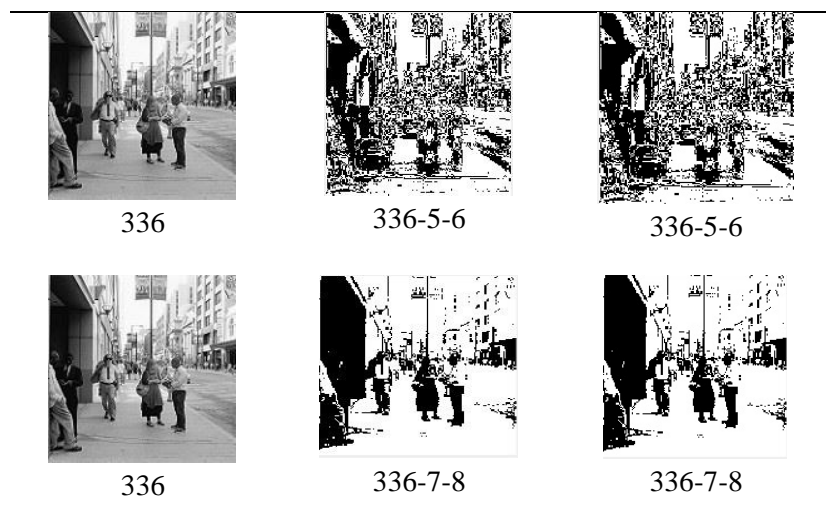
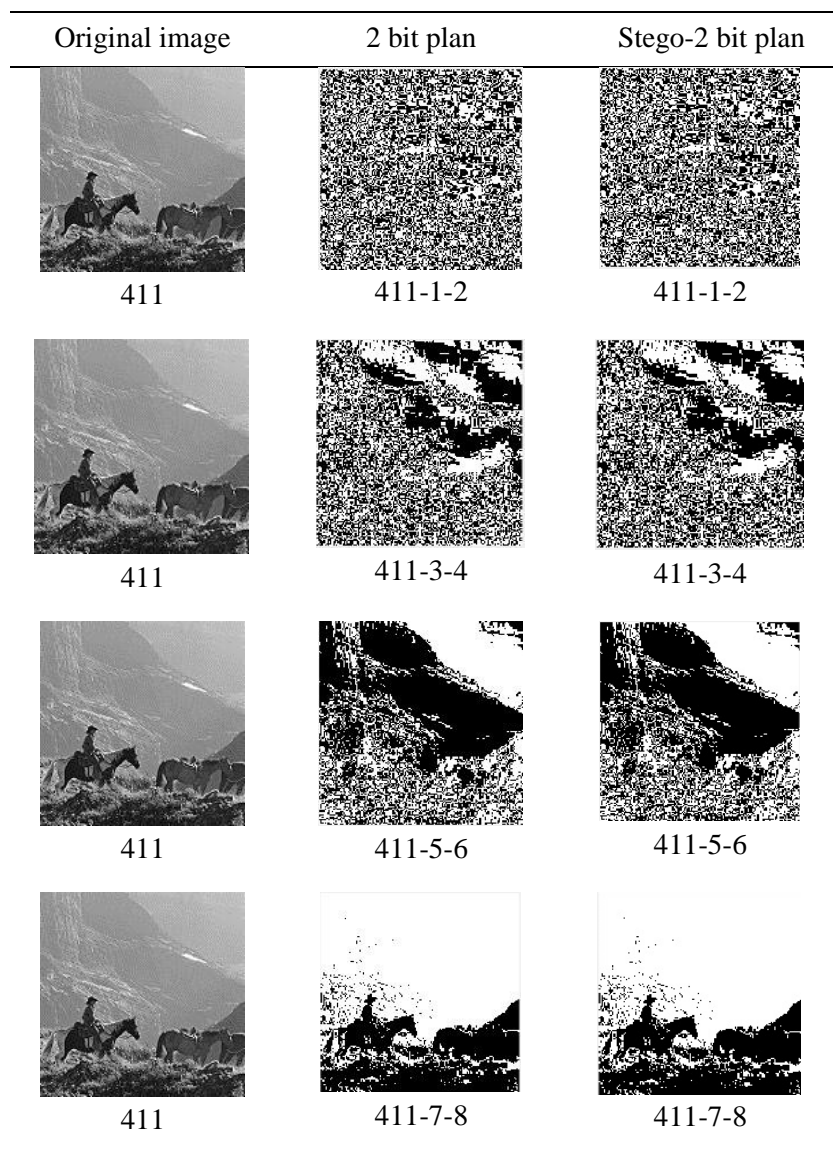


TABLE (II-C) IMPLEMENTATION PROPOSED SYSTEM BETWEEN ORIGINAL IMAGE AND 2-BIT PLAN AND STEGO-2-BIT PLAN IMAGES.



## B. The Results Discussion

The analysis of the proposed system in Table (III) indicates an evaluation system for PSNR, MSE, correlation coefficient, histogram, and entropy. The PSNR in four tests is one-two to seven-eight bits. The range in the stego-2-bit plan image bit is from 93.0007 to 93.0503, and the MSE in four tests is one-two-to-seven-eight bits. The range in the stego-2-bit plan image is 3.2841 to 3.2468. Note in this test that the range of PSNR is increasing, but the range of MSE is decreasing. And the entropy in four tests of the range in the stego-2-bit plan image is from 4.4952 to 3.6512. The security and transparency of the system are very strong because using 2-bit plan slicing and hiding secret messages using random array secret keys makes it impossible for attackers to access sensitive information.

TABLE III. MEASUREMENTS OF SYSTEM BETWEEN 2-BIT PLAIN AND STEGO-2-BIT PLAN GRAY IMAGES.

Bit plan 2bit	PSNR	MSE	Entropy	Correlation
13	-	-	7.1342	0.7387
13-1-2 stego	93.0007	3.2841	4.4952	0.1615
13-3-4 stego	87.0048	1.3062	4.3496	1180.1
13-5-6 stego	92.9507	3.3220	4.2667	0.3273
13-7-8 stego	86.9550	1.3212	3.6280	0.7034
336	-	-	7.7666	0.8416
336-1-2 stego	93.0996	3.2101	4.3950	0.1268
336-3-4 stego	77.4114	0.0012	4.3191	0.2425
336-5-6 stego	81.0332	5.1660	4.1620	0.5139
336-7-8 stego	92.9005	3.3607	3.3337	0.7874
411	-	-	7.1336	0.8322
411-1-2 stego	93.0996	3.2101	4.3992	0.2104
411-3-4 stego	87.0048	1.3062	4.3676	0.3914
411-5-6 stego	93.0996	3.2101	3.7257	0.5556
411-7-8 stego	93.0503	3.2468	3.6512	0.8263

- Table (IV-a, b, c) indicates the histogram between 2-bit plan and stego gray images.



TABLE (IV-A): HISTOGRAM BETWEEN 2-BIT PLAN AND STEGO 2-BIT PLAIN IMAGES.


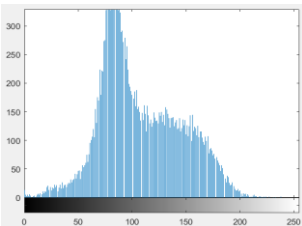
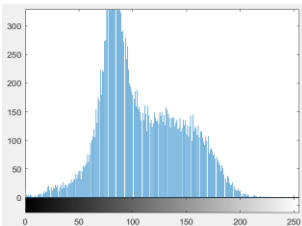
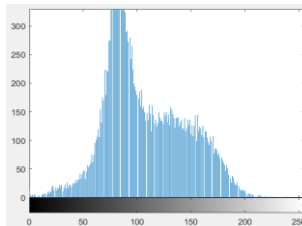
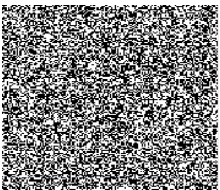
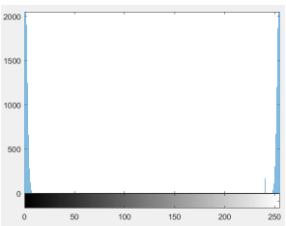
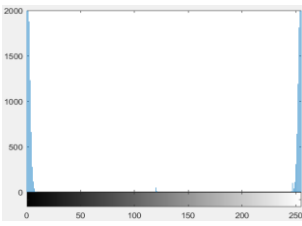
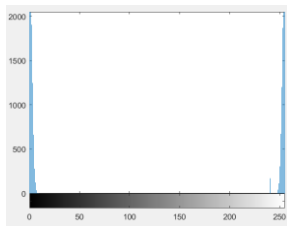
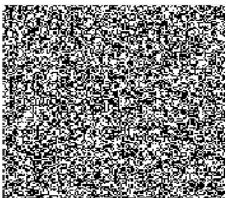
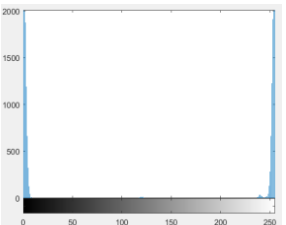
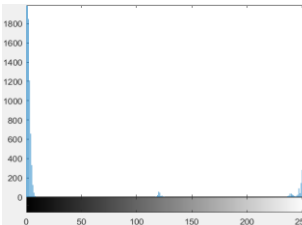
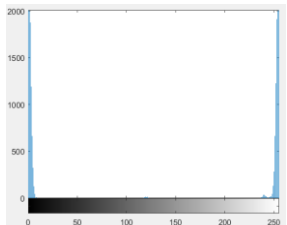

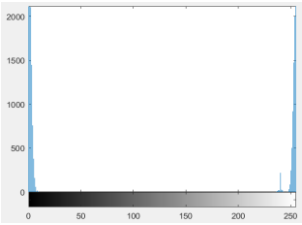
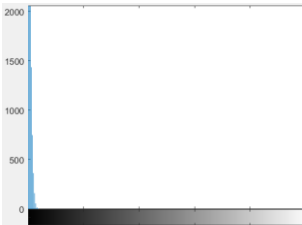
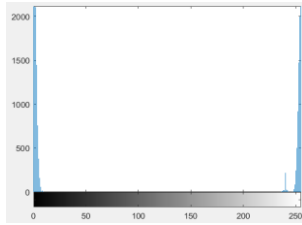
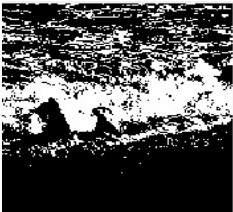
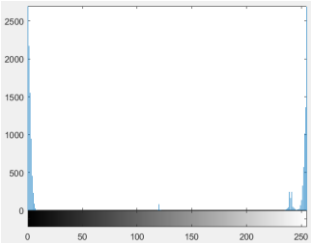
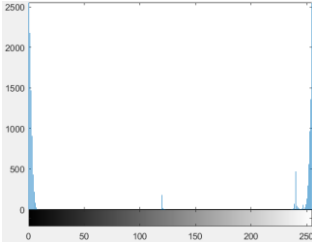
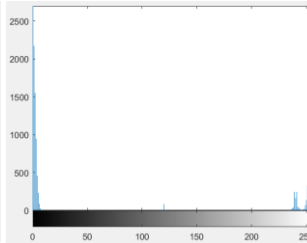
No. of Image	Histogram Original	Stego-Image Bit Plan	Cover-Bit Plan 2-bit
 13			
 13-1-2			
 13-3-4			
 13-5-6			
 13-7-8			

TABLE (IV-B): HISTOGRAM BETWEEN 2-BIT PLAN AND STEGO 2-BIT PLAIN IMAGES.


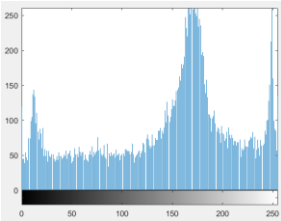
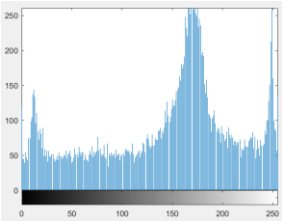
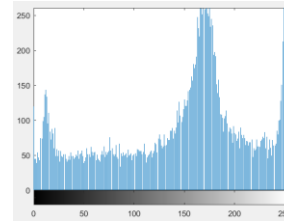
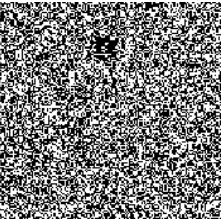
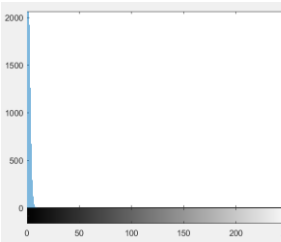
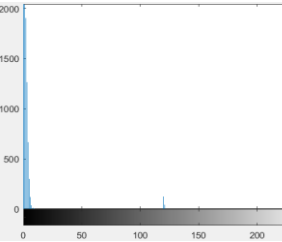
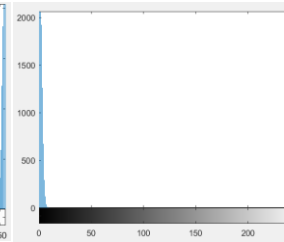
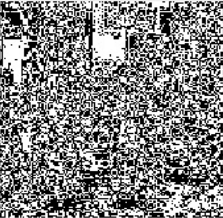
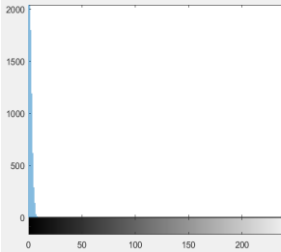
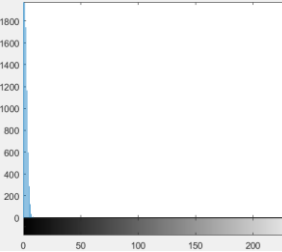
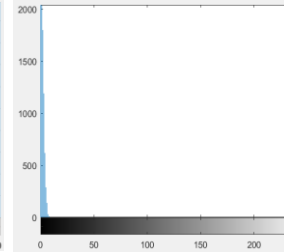

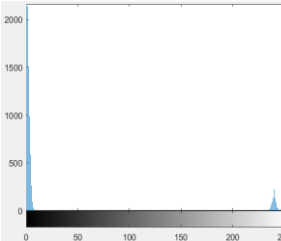
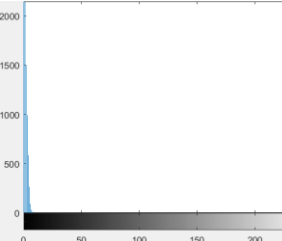
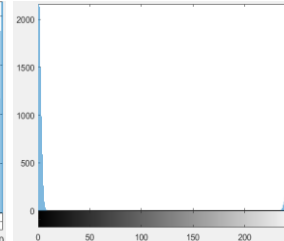

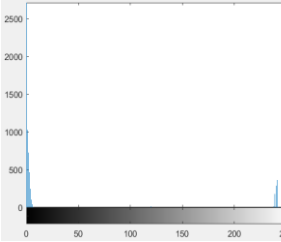
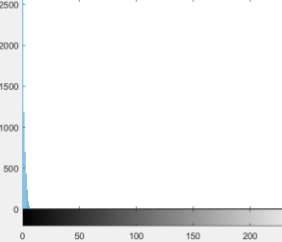
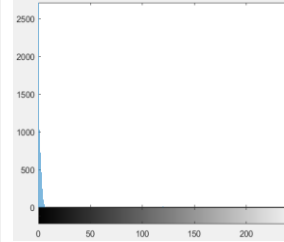

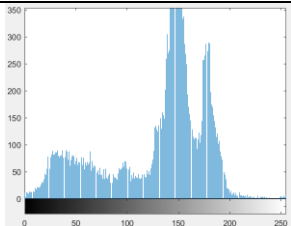
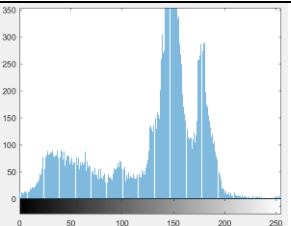
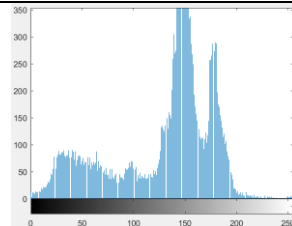
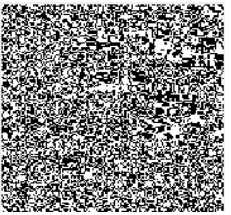
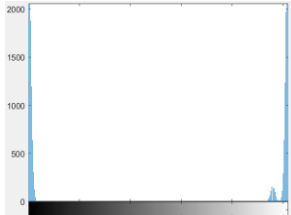

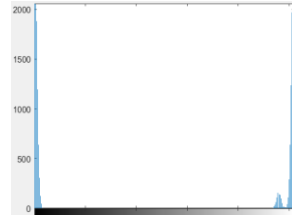
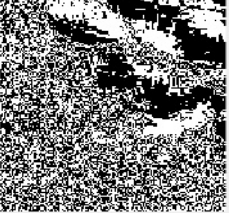


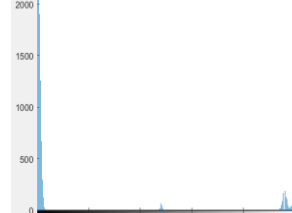



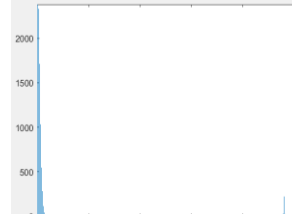


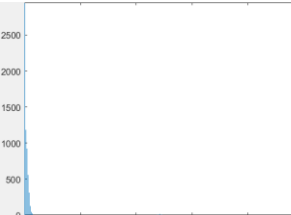
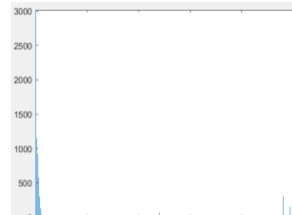
No. of Image	Histogram Original	Stego-Image Bit Plan	Cover-Bit Plan 2-bit
 336			
 336-1-2			
 336-3-4			
 336-5-6			
 336-7-8			



TABLE (IV-C): HISTOGRAM BETWEEN 2-BIT PLAN AND STEGO 2-BIT PLAIN IMAGES.

No. of Image	Histogram Original	Stego-Image Bit Plan	Cover-Bit Plan 2-bit
 411			
 411-1-2			
 411-3-4			
 411-5-6			
 411-7-8			

Finally, to evaluate the robustness of this work, the proposed system was compared with other related works mentioned in the literature, as listed in Table V.

TABLE V. COMPARISON BETWEEN PROPOSED SYSTEM AND RELATED WORKS

Reference no.	PSNR	MSE	Entropy	Correlation
[7]	57.19- 26.98	0.12- 130.34	/	/
[8]	55.903- 51.95	0.166- 0.420	/	/
[9]	57.19- 26.98	0.12- 130.34	/	/
[10]	44.5599- 8.2774	2.2756- 9668.1	/	/
<b>Proposed system</b>	<b>93.0007- 93.0503</b>	<b>3.2841-3.2468</b>	<b>4.4952 - 3.6512</b>	<b>0.1615-0.8263</b>

From the table, the proposed method involved a new two metrics represented by entropy and correlation for system evaluation that were not included in the previous methods. In addition, the results show that the proposed system gets a higher evaluation in bold results in terms of PSNR and MSE compared to the other listed methods.

## VII. CONCLUSION

Due to the urgent need confidentiality of information and data during its transmission over the Internet, a robust system for hiding data. contribution to this research includes using the two-bit plane slicing (2-BPS) method, but this time by dividing the cover image into four images instead of eight which is followed by traditional methods. It was concluded that it is an efficient method in terms of confidentiality of information, and it is undetected by attackers over the Internet through a set of measures (PSNR and MSE); when PSNR increases, MSE decreases, and vice versa, when PSNR decreases, MSE increases. This provides high confidentiality for data into images. Additionally, the capacity of hidden data is less the stronger the secrecy. Regarding the histogram in the original image compared to the hidden images, it was found to have a strong similarity, which makes it impossible for the attacker to manipulate with the hidden data, in addition to the difficulty of being detected visually by the attacker.

## REFERENCES

- [1] E. S. Hureib and A. A. Gutub, "Enhancing medical data security via combining elliptic curve cryptography and image steganography," *Int. J. Comput. Sci. Netw. Secur.(IJCSNS)*, vol. 20, no. 8, pp. 1–8, 2020.
- [2] 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.
- [3] U A Md Ehsan Ali, and Emran Ali, "A LSB Based Image Steganography Using Random Pixel and Bit Selection for High Payload," *I. J. Mathematical Sciences and Computing*, vol. 3, no. 2, pp. 24–23, 2021.
- [4] K. Ashita and P. Smitha Vas, "Randomized Steganography in Skin Tone Images," *International Journal of Computer Science, Engineering and Information Technology (IJCEIT)*, vol. 08, no. 2/3, pp. 1–8, 2018.
- [5] 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.
- [6] 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. 02, no. 10, pp. 424–428, Oct. 2020.
- [7] 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.
- [8] 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," *Comput Biol Med*, vol. 105, pp. 72–80, 2019.
- [9] Z. I. Nezami, H. Ali, M. Asif, H. Aljuaid, I. Hamid, and Z. Ali, "An efficient and secure technique for image steganography using a hash function," *PeerJ Comput Sci*, vol. 8, p. e1157, 2022.

- [10] 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.
- [11] P. Mathur and A. K. Gupta, "A Study of Data Hiding Using Cryptography and Steganography," in *International Conference on Information Management & Machine Intelligence*, Springer, 2019, pp. 1–13.
- [12] P. G. Kuppusamy, K. C. Ramya, S. S. Rani, M. Sivaram, and V. Dhasarathan, "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.
- [13] 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.
- [14] Y. Bao, C. Li, F. Meng, Y. Liang, W. Liu and K. Liu, "Mbb: A Multi-Scale Method For Data Based On Bit Plane Slicing," 2021 IEEE International Conference on Image Processing (ICIP), pp. 859-863, 2021.
- [15] L. Jiangjing, Z. Jun, F. Chunliang and G. Linhua, "Performance Evaluation Model of Human Resource Management in Public Institutions Based on Improved Decision Tree," 2020 International Conference on Wireless Communications and Smart Grid (ICWCSG), pp. 310-315, 2020.
- [16] T. Pan, "Performance Evaluation Method of Enterprise Human Resource Management Based on Machine Learning," 2021 IEEE International Conference on Industrial Application of Artificial Intelligence (IAAI), pp. 100-105, 2021.
- [17] A. ALabaichi, M. A. A. K. Al-Dabbas, and A. Salih, "Image steganography using least significant bit and secret map techniques," *International journal of electrical & computer engineering* (2088-8708), vol. 10, no. 1, 2020.
- [18] B. Fesl, M. Koller and W. Utschick, "On the Mean Square Error Optimal Estimator in One-Bit Quantized Systems," in *IEEE Transactions on Signal Processing*, vol. 71, pp. 1968-1980, 2023.
- [19] O. Keleş, M. A. Yılmaz, A. M. Tekalp, C. Korkmaz and Z. Doğan, "On the Computation of PSNR for a Set of Images or Video," 2021 Picture Coding Symposium (PCS), Bristol, United Kingdom, pp. 1-5, 2021.
- [20] T. Zheng, M. Zhang, L. Li, Q. Wu and L. Zhou, "Correlation Coefficients of Interval-Valued Pythagorean Hesitant Fuzzy Sets and Their Applications," in *IEEE Access*, vol. 8, pp. 9271-9286, 2020.
- [21] D. Xiang et al, "Research on Histogram Equalization Algorithm Based on Optimized Adaptive Quadruple Segmentation and Cropping of Underwater Image (AQSCHE).," in *IEEE Access*, vol. 11, pp. 69356- 69365, 2023.
- [22] Y. Li, R. Sun, C. Luo and Y. Zhou, "A modified Histogram Equalization approach for Image Contrast Enhancement," 2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE), pp. 545-550, 2022.