A New Steganography Method for Hiding Text into RGB Image

AL-Hasan Amer Ibrahim[1], Ruaa Shallal Abbas Anooz[2],
Mohammed Ghassan Abdulkareem[3], Musatafa Abbas Abbood Albadr[4]*,
Fahad Taha AL-Dhief[5]*, Yaqdhan Mahmood Hussein[6], Hatem Oday Hanoosh[7], Mohammed Hasan Mutar[8]

Department of Petroleum Project Management-College of Industrial Management of Oil and Gas,
Basrah University for Oil and Gas, Al-Basrah, Iraq[1, 4]
Technical Engineering College, Al-Furat Al-Awsat Technical University (ATU), Kufa, 54003, Iraq[2]
Department of Oil and Gas Management and Marketing-College of Industrial Management of Oil and Gas,
Basra University for Oil and Gas, Al-Basrah, Iraq[3]
Faculty of Engineering-School of Electrical Engineering, Universiti Teknologi Malaysia (UTM), Johor Bahru 81310, Malaysia[5]
Department of Electronic and Communication-College of Engineering, Al Muthanna University, Iraq[6, 7]
Department of Computer Technical Engineering-College of Information Technology,
Imam Ja'afar Al-Sadiq University, Al-Muthanna 66002, Iraq[8]

***Abstract*—Now-a-days, the network has significant roles in transferring data and knowledge quickly and accurately from sender to receiver. However, the data is still not secure enough to transfer quite confidentially. Data protection is considered as one of the principal challenges in information sharing over communication. So, steganography techniques were proposed which are the art of hiding information that prevents secret text message detection from intruders. Nevertheless, most steganography methods use low bits number of secret messages. Moreover, these methods applied a single logic gate for encrypting the secret message. Therefore, this paper proposes a new method for the encryption of secret messages based on the Huffman technique to reduce the secret message dimensions. In addition, the proposed method uses two different logic gates namely XOR and XNOR for increasing the message security. The RGB Lena image is used as the cover image of the secret message. There are six different experiments conducted with respect to various lengths of the secret messages in bits. The experimental results show that when using the highest number of bits (i.e., 66288), the proposed method achieved 0.0233 MSE, 64.4589 PSNR, 0.9999998 SSIM, and 8.2383 encryption time. The proposed method has the ability to encrypt the secret message with a high number of bits.**

Keywords—Steganography techniques; color images; XOR gate; NOR gate; huffman technique

I. INTRODUCTION

Nowadays, communication is quite necessary for transmitting information quickly and accurately from the sender to the receiver [1]. Meanwhile, the internet in this modern era provides high convenience in transferring big amounts of data in several parts of the world. Everyone needs safety and secrecy in communicating data [2]. In our daily life, there are many secure pathways that we use such as internet or telephone for sharing and transmitting the information. But unfortunately, these pathways still not safe at a particular level [3]. Consequently, there are two common techniques which are widely used in hiding information and then sharing it safety. These techniques are cryptography and steganography [4, 5]. In the cryptography technique, the message or the text is adjusted in an encrypted form and the encryption key is known only to both sender and receiver. However, the transmission of an encrypted message in such a type of technique may lead to easily excite the attacker's suspicion, and hence this encrypted message will be intercepted, attacked and then decrypted [6]. Therefore, steganography techniques have been proposed and developed in order to overcome the insufficiencies of the cryptographic technique [7].

Steganography is the science of communicating in such a method that it covers and hides the presence of the communication [8]. Thus, there is no one that can detect the existence of a message because the steganography technique hides its presence. On other words, the steganography technique is hiding the message inside multimedia content such as video, audio and image files, where the message will be embedded with one of these multimedia contents [9]. Steganography technique is consisting of two main terms which are the data or the message and cover image [10]. The message is the secret information that needs to be hidden. While the cover image is referred to the carrier that hides or covers the message. Fig. 1 shows the steganography diagram. Steganography's word has been taken from Greek words, where "stegos" indicates to "cover" and "grafia" indicates to "writing" and these two words are defining together as "covered writing" [11]. There are many different techniques of steganography such as spatial domain methods, spread spectrum technique, statistical technique, transform domain technique, and distortion technique [12]. Also, there are different measurements which determine the performance efficiency of steganography techniques such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Structural Similarity Index Measure (SSIM) and Signal to Noise Ratio (SNR) [13, 14]. Steganography technique is quite valuable and it can be applied in many domains such as communication and secret data storing, e-commerce, database systems, data alteration protection, and media [15]. As we mentioned previously that the steganography technique has different categories for hiding information which are embedding the information in text, images, audios, videos, or protocol. The images are considered the most common cover objects which have used for steganography technique [16]. Due to the digital images are broadly proliferated on the Internet and also due to provide a large number of excessive bits in the digital image. The picture steganography is considered as a method for secret and ambiguity correspondence that intends to transfer many of mystery information. Generally, to the cover picture extent among conveying parties. Besides, it aims to avoid the suspicion for non-conveying gatherings in such type of correspondence [17].

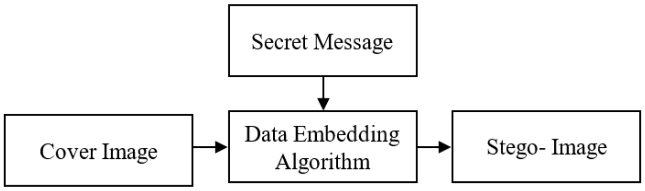


Fig. 1. The steganography diagram.

The image in the computer is a set of numbers that form various light intensities in different image areas. This numeric representation is constituted individual points and a grid which are referred to as pixels [18]. On the Internet, most images are consisting of a rectangular map for the image's pixels which are represented as bits. These pixels are presented horizontally and displayed row by row. The bits number in a color image named the bit depth that belongs to the bits number utilized for every pixel. In present color images, the smallest bit depth is 8 (i.e., there are 8 bits used for representing each pixel color) [19]. Grayscale and monochrome images use 8 bits for every pixel and these pixels are able to present 256 various colors or grey shades.

The digital color images are usually stored in files of 24-bit and use the pattern of RGB color that is known as true color as well. All colors for pixels with 24-bit picture are derived from three essential colors which are Red, Green and Blue (RGB). Each color is produced with 8 bits. Hence, in every pixel, there are 256 different amount of RGB colors as well as to more than 16-million combinations that lead to producing more than 16-million colors in the image [20]. With regards to images, hiding the message in the image is performed by taking the cover object as an image that is indicated as image steganography. The pixel intensities in image steganography are used in order to hide the message [21]. In steganographic images, the Least Significant Bit (LSB) is considered a widely known technique due to its high advantages in encrypting texts in images [22-24]. However, the conventional LSB technique still needs more enhancements in the steganographic technology [25, 26].

Moreover, recent steganography techniques used in the image are yet suffering from the small amount of data that required to be hidden in the cover image. Also, these techniques are showing some negative effects and wasting some of the hidden data. Moreover, there is an urgent need to find a method that is able to hide data without distinguishing between the hidden data and the original covering data. Therefore, the aims of this paper are as follow:

- In this work, we propose the Huffman technique in order to reduce the dimensionality of the secret message.
- Propose two different logic gates called XOR and XNOR for increasing the encryption security of the secret message.
- The proposed method is performed based on six different experiments with respect to various lengths of the secret messages in bits.
- The performance of the proposed method is evaluated in terms of MSE, PSNR, and execution time.

The remainder of this paper is organized as follows: Sections II shows the related works in the steganography technique for hiding information in images. Section III presents the proposed method in terms of the Huffman technique and two logic gates. Section IV discusses the experimental results. Finally, Section V presents the conclusion of this paper.

II. Related Work

Recently, the steganography techniques for hiding text in images have beheld a huge significance by researchers and developers due to the importance such these techniques in terms of hiding data. Furthermore, recent steganography methods of hiding data such as XOR and XNOR logic gates worked on providing a high level of security, where the intended user can only access to the secret data. In other words, the unauthorized user has no ability to detect hidden data, where this is an extremely critical issue in order to protect the sensitivity and confidentiality of information and messages being sent. Here, we will review the up-to-date techniques used in the steganography field. Besides, Table I summarizes the related works used for the encryption of secret messages in images. A steganography technique is proposed in [27] to protect information transported from attackers. This method is worked on the encryption of secret information by using the XNOR gate and the encryption key. The information that required to be encrypted is hidden in a color image by applying Least Significant Bit (LSB) algorithm. Furthermore, this method relies on chromatic channels extraction of 3 RGB channels for every pixel and 2 bits of LSB bits and then determining the channel that will hide the encryption message bit. The second LSB bit is used as an indicator that determines the channel. Meantime, the first LSB bit is replaced with the encrypted message bit, where all the encrypted message bits will be hidden in the cover image. Four different types of images have used as a carrier file which are Airplane, Peppers, Lena, and Baboon. The dimension of all these images is 512x512. Also, different amounts of information were used as secret messages to analyze and evaluate the method, where the smallest amount was 4700 bits and the largest amount was 24250 bits. The performance of this method is evaluated in terms of two measurements which are namely Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). According to the best-achieved results of the largest amount of secret information are shown that the highest PSNR and lowest MSE are 53.65 and 0.0339 respectively which have obtained from Lina image. However, the amount of hidden information is still not encouraging and a bit small.

The authors in [28] have presented a method to hide text in a color images in order for keeping the information from intruders. This method has two main stages. In the first stage, the steganography technique is used to hide the information in the transmission, where it has used the XOR operation gate for hiding the text bit in the image bit and specifies the position of the image bits according to a random key (the random key has the same length of the secret text). While in the second stage, it has used Triple data encryption standard (3DES) algorithm. This algorithm is used to encrypt the resulting image and the key. Subsequently, the key and image are sent to the receiver. In this method, two types of images have used which are Lena image (256x256 pixels) and Tree image (250x360 pixels). The results of this method have shown that Lena image has 52.0235 PSNR and 0.10024 MSE, while tree image has better performance with 55.0016 PSNR and 0.03602 MSE. However, this method has ignored the length of the confidential text in bit, where it has not taken into account. Furthermore, the steganography technique is applied in [29] to hide the text messages in 24-bit color images. In this method, two schemes have proposed which are embedding data scheme and extraction scheme. In embedding data, the text messages will be hidden in the cover image by using the LSB algorithm. In the extraction scheme, it has used XOR operation to Most Significant Bits (MSB) to recover the secret text from a stego-image. The MSB bits identify the object shape in the image. These two schemes are requiring a key that is created randomly. The experiments have carried out on six different types of images which are Toy (3264 x 2448), Mosque (767x619), Cat (645x533), Flower (551x451), View (32644x2448), and Sunset (1632x1224). The statistical analysis of this method is show that the highest value of PSNR is 63.738 that has obtained by View image, and its MSE value was 0.0026. In this regard, the LSB algorithm is used also in [30] for hiding and protecting secret text message in Image. In this work, the LSB algorithm is combined with XOR encryption techniques in order to increase the security of the text message. Four images have used to embed text messages, these images are Barbara, F16, Lena, and Soccer. All these images have a size of 256x256 pixels and it has used three different sizes (i.e., 1 KB, 2 KB, and 4 KB) of the text messages which are needed to be hidden. The experimental results have shown that the highest achieved PSNR for 1 KB, 2 KB, and 4 KB is 63.5195 (Lena image), 60.3883 (Soccer image), and 57.3182 (Soccer image), respectively. Besides, the lowest MSE for 1 KB, 2 KB, and 4 KB is 0.0289 (Lena image), 0.0595 (Soccer image), and 0.1206 (Soccer image), respectively. Also, the extracted text messages have tested by Character Error Rate (CER) and the value was 0, which proves that text messages have extracted totally. However, the embedded text messages in the cover image are small and limited. A secure model that has embedded text messages for reliable communication was proposed in [31]. Furthermore, this model has used the LSB algorithm for embedding text message bits. In this model, the LSB is based on the secret key and logistic map, this is a spatial domain technique to embed more information in color image without deteriorating the quality of the image. The logistic map method is used for embedding the message bits randomly in the image. The image type used in this work is the Lena image. According to the results, the maximum capacity text messages stored in the cover image is 29127 bytes (233016 bits) and PSNR has been achieved 55.91. A secure method for embedding secret text messages in color images is proposed in [32]. This method is used Integer Wavelet Transform (IWT) technique that is based on the LSB algorithm. The secret text messages are hidden in the LSB algorithm, and the inverse IWT is used to form the stego-image. The secret information is hidden in the approximation coefficient in the components of blue and green colors. While the actual length of the secret data and the sender signature are embedded in the LSB algorithm in the component of the red color of the cover image. In this method, six different types of images have used which are Lena, Baboon, Pepper, Airplane, House, and Tiffany. The size of each image of all these color images is 512×512 pixels. The experimental results are shown that the hybrid IWT-LSB can be embedded secret data with a size of 24 576 bits, where the highest PSNR was 55.5622 that achieved by Baboon image, and the MSE was 0.1807. However, from the studies mentioned above, we can observe some limitations that can be summarized as follow:

- Most models and methods which are used steganography techniques for embedding text messages are yet suffering from a low amount of embedding text messages.
- Majority of these methods are worked on one logic gate in the encryption of secret messages in which results in a low-security level.
- Finally, the execution time of experiments is mostly ignored.

TABLE I. THE SUMMARY OF RELATED WORKS

Years	Techniques	Images	Secret Message Size	PSNR	MSE	Ref.
2020	XNOR and LSB	Airplane, Peppers, Lena, and Baboon	24250 bits	53.65	0.0339	[27]
2020	XOR and 3DES	Lena and Tree	-	55.0016	0.03602	[28]
2019	XOR and MSB	Toy, Mosque, Cat, Flower, View, and Sunset	24 bits	63.738	0.0026	[29]
2019	XOR and LSB	Barbara, F16, Lena, and Soccer	1 KB, 2 KB, and 4 KB	63.5195, 60.3883, and 57.3182	0.0289, 0.0595, and 0.1206	[30]
2018	LSB and logistic map	Lena	29127 bytes	55.91	-	[31]
2018	IWT and LSB	Lena, Baboon, Pepper, Airplane, House, and Tiffany	24 576 bits	55.5622	0.1807	[32]

III. Proposed Method

A. Encryption Algorithm

In the proposed method, there are three main phases. Fig. 2 shows the steps of these three phases. The first phase includes four steps which are read the secret message, convert the secret message from text to decimal, implement the Huffman to compress the data (reduce the dimensionality), and convert the data from decimal to binary. While in the second phase, the secret message will be encrypted by using the following steps:

- Enter the encryption key value in binary with 8 bits.
- Implement the XNOR logic gate on every other 4 bits (i.e., first 4, third 4, fifth 4 and so on) of the secret message with the first 4 bits of the encryption key.
- Implement the XOR logic gate on every other 4 bits (i.e., second 4, fourth 4, sixth 4 and so on) of the secret message with the second 4 bits of the encryption key.

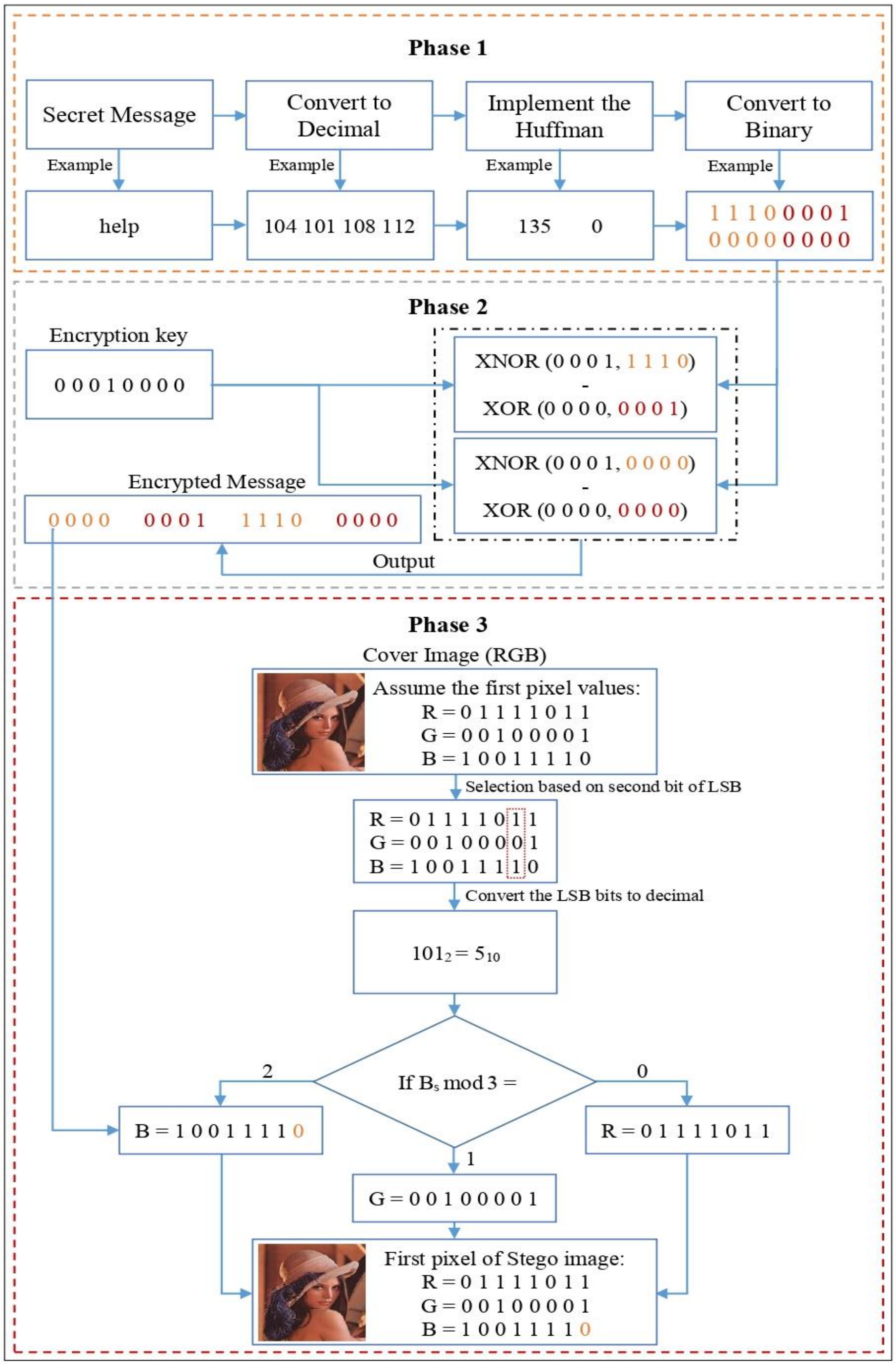


Fig. 2. The three phases of the proposed method.

Furthermore, the third phase includes the following steps:

1. Read the cover image.
2. Selection of one of three RGB channels based on second bit of LSB bits of three channels in decimal and return in B_s.

a. If (B_s mod 3) = 0

Then Red channel is selected.

b. If (Bs mod 3) = 1

Then Green channel is selected.

c. If (Bs mod 3) = 2

Then Blue channel is selected.

3. Apply the LSB algorithm to the selected channel and coding by storing the encrypted bit instead of the first bit of LSB bits.
4. Stego image is achieved.

An example is provided below to encrypt the word “help” as a secret message into the cover image. The steps of this example as follow:

1. Secret message = help.
2. Secret message in decimal = 104 101 108 112.
3. Huffman of the secret message = 135 0.
4. Huffman of the secret message in binary with 8 bits = 1 1 1 0 0 0 0 1 0 0 0 0 0 0 0 0.
5. Encryption key = 0 0 0 1 0 0 0 0.
6. First 4 bits of the Huffman’s secret message in binary = 1 1 1 0.
7. Second 4 bits of the Huffman’s secret message in binary = 0 0 0 1.
8. Third 4 bits of the Huffman’s secret message in binary = 0 0 0 0.
9. Fourth 4 bits of the Huffman’s secret message in binary = 0 0 0 0.
10. First 4 bits of the encryption key = 0 0 0 1.
11. Last 4 bits of the encryption key = 0 0 0 0.
12. The first 4 bits of the encrypted message = XNOR (Step 6, Step 10) = 0 0 0 0.
13. The second 4 bits of the encrypted message = XOR (Step 7, Step 11) = 0 0 0 1.
14. The third 4 bits of the encrypted message = XNOR (Step 8, Step 10) = 1 1 1 0.
15. The fourth 4 bits of the encrypted message = XOR (Step 9, Step 11) = 0 0 0 0.
16. The encrypted message bits = 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0.
17. Read the cover image. Table II shows the selection and encryption processes to create four pixels of the stego image.

TABLE II. THE SELECTION AND ENCRYPTION PROCESSES OF FOUR PIXELS IN THE STEGO IMAGE

Pixel	Channel	Value of the channels in binary (cover image)	Second LSB of the three channels	Selected channel	Message bit	Value of the channels in binary (stego image)
1st	R	01111011	$101_2 = 5_{10}$	2 B	0	01111011
	G	00100001				00100001
	B	10011110				10011110
2nd	R	01111011	$101_2 = 5_{10}$	2 B	0	01111011
	G	10100001				10100001
	B	10011111				10011110
3rd	R	01000111	$100_2 = 1_{10}$	1 G	0	01000111
	G	10010001				10010000
	B	10000001				10000001
4th	R	01111011	$110_2 = 3_{10}$	0 R	0	01111010
	G	00111110				00111110
	B	10001100				10001100

B. Decryption Algorithm

This section will present the processes for extracting the secret message from stego image. These processes are summarized below. In addition, Table III shows the determination of RGB channel based on second bit of LSB.

1. Get stego image.
2. Selection of one of three RGB channels based on second bit of LSB bits of three channels in decimal and return in Bs.
   a. If (B_s mod 3) = 0
   Then Red channel is selected.
   b. If (Bs mod 3) = 1
   Then Green channel is selected.
   c. If (Bs mod 3) = 2
   Then Blue channel is selected.
3. Apply the LSB algorithm on the selected channel to get the encrypted message bits (0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0).
4. Input the encryption key = (0 0 0 1 0 0 0 0) and apply the following steps:
   a. XNOR decoding on the first 4 bits of the encrypted message and the first 4 bits of the encryption key. Therefore, XNOR (0 0 0 0, 0 0 0 1) = 1 1 1 0.
   b. XOR decoding on the second 4 bits of the encrypted message and the last 4 bits of the encryption key. Therefore, XOR (0 0 0 1, 0 0 0 0) = 0 0 0 1.
   c. XNOR decoding on the third 4 bits of the encrypted message and the first 4 bits of the encryption key. Therefore, XNOR (1 1 1 0, 0 0 0 1) = 0 0 0 0.
   d. XOR decoding on the fourth 4 bits of the encrypted message and the last 4 bits of the encryption key. Therefore, XOR (0 0 0 0, 0 0 0 0) = 0 0 0 0.
5. The Huffman's secret message in binary is obtained = 1 1 1 0 0 0 0 1 0 0 0 0 0 0 0 0.
6. Convert each 8 bits of the Huffman's secret message to decimal = 135 0.
7. Apply the Huffman to normal which decodes the Huffman's secret message in decimal to get the normal secret message in decimal = 104   101   108   112.
8. Convert the secret message from decimal to character to get the secret message = help.

TABLE III. THE DETERMINATION OF RGB CHANNEL BASED ON SECOND BIT OF LSB

Pixel	Channel	Value of the channels in binary (stego image)	Second LSB of the three channels	Selected channel	Message bit
1st	R	01111011	$101_2 = 5_{10}$	2 B	0
	G	00100001			
	B	10011110			
2nd	R	01111011	$101_2 = 5_{10}$	2 B	0
	G	10100001			
	B	10011110			
3rd	R	01000111	$100_2 = 1_{10}$	1 G	0
	G	10010000			
	B	10000001			
4th	R	01111010	$110_2 = 3_{10}$	0 R	0
	G	00111110			
	B	10001100			

IV. EXPERIMENTAL RESULTS AND DISCUSSION

In this study, the Lena color image (RGB) with (512 × 512 × 3) dimensionality was used in order to conduct six different experiments. The six different experiments were implemented based on various lengths of the secret message in bits (i.e., 3640, 6872, 26224, 33128, 40032, and 66288 bits). In this proposed method, we have used Huffman method in order to reduce the dimensionality of the data (i.e., secret message). Furthermore, there are two logic gates which are XNOR and XOR have been used for the purpose of encrypting the Huffman of the secret message with the encryption key. It is worth mention that all experiments have been implemented in MATLAB R2019a programming language over a PC Core i7 of 3.20 GHz with 16 GB RAM and SSD 1 TB (Windows 10). The proposed method has been evaluated in terms of the most common performance measurements used in the steganography techniques which are Mean Square Error (MSE), Structural Similarity Index Measure (SSIM), and Peak Signal-to-Noise Ratio (PSNR). Besides, the proposed method has been evaluated in terms of the execution time. The MSE, PSNR and the execution time can be calculated as the following equations:

$$MSE = \sum_{m=0}^{M-1} \sum_{f=0}^{F-1} \|A(m,f) - T(m,f)\|^2 \quad (1)$$

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

$$Execution\ Time\ (T) = T_{End} - T_{Start} \quad (3)$$

where, $A(m, f)$ refers to the pixel value of the cover image, $T(m, f)$ refers to the pixel value of the stego image, and M and F refer to the height and width of the images, respectively. In the six different experiments, the minimum and maximum numbers of the secret message bits are 3640 and 66288, respectively. Based on the experiments results, when the minimum number of the secret message bits is used, the proposed method is achieved 0.0013 MSE, 77.1531 PSNR, and it has taken 0.9543 sec for the execution time. Meanwhile, the proposed method has been obtained 0.0140 MSE, 64.4589 PSNR, and 8.2383 sec by using the maximum number of the secret message bits.

Furthermore, Table IV illustrates the full results of the six different experiments in terms of MSE, PSNR, SSIM, and encryption time in seconds. Fig. 3 shows the histograms of the three colors (red, green, and blue) separately for the original image (cover image) and the stgo images with different lengths of secret messages in bits. Moreover, Fig. 4 demonstrates all the color histograms (red, green, and blue) for the original image (cover image) and the stgo images with different lengths of secret messages in bits. Based on Fig. 3 and Fig. 4, the proposed method has not been influenced the three channels of the original image colors (red, green, and blue). In other words, the proposed method has the ability to encrypt high numbers of secret message bits without affecting the quality of the image.

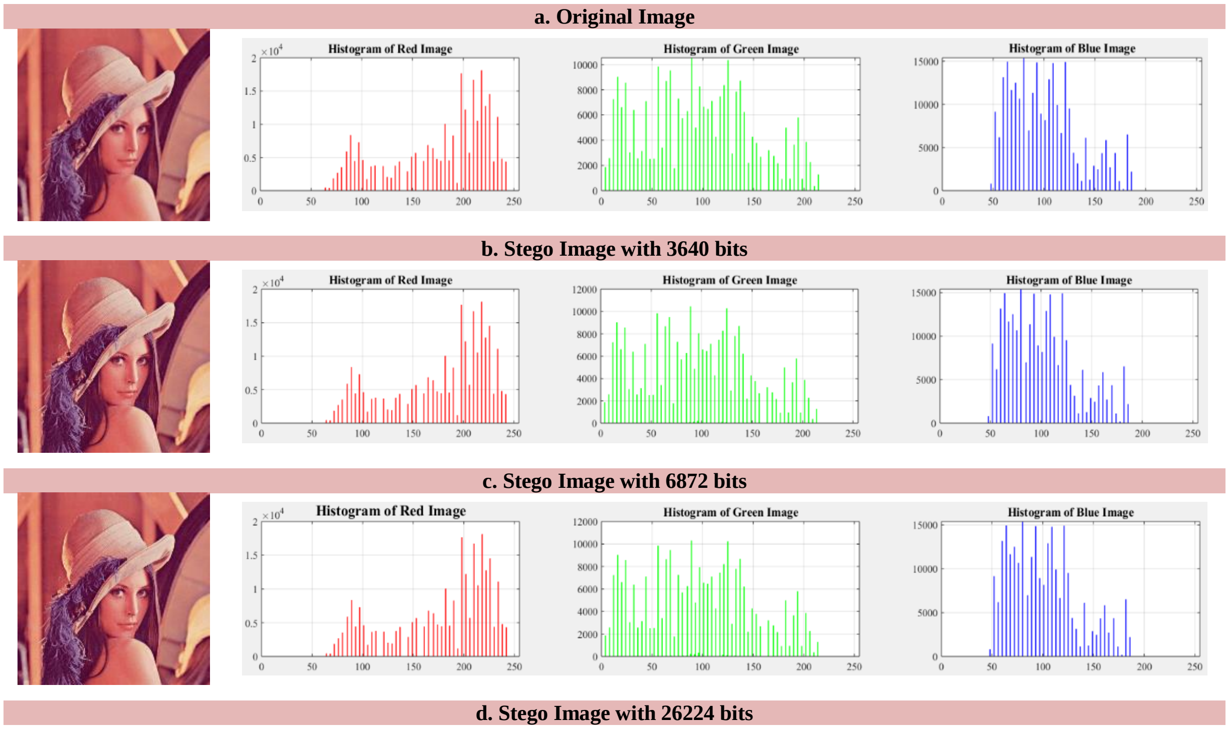
Moreover, the proposed method has been compared with other methods using Lena image [30, 33-37] as shown in Table V. The experimental results showed that the proposed method has been outperformed the other methods in terms of number of bits, MSE, SSIM and PSNR. Although the proposed method has been shown the high ability to encrypt a high number of bits in RGB image, there are some limitations in the proposed method which can be summarized as follow:

- All experiments of the proposed method have been conducted using one image only. In other words, the proposed method is evaluated using the Lena image only.

- The proposed method has been evaluated based on the standard image size (512 × 512 × 3). Whilst other evaluations based on varying the image sizes may lead to obtaining different results.

TABLE IV. THE RESULTS OF THE SIX DIFFERENT EXPERIMENTS

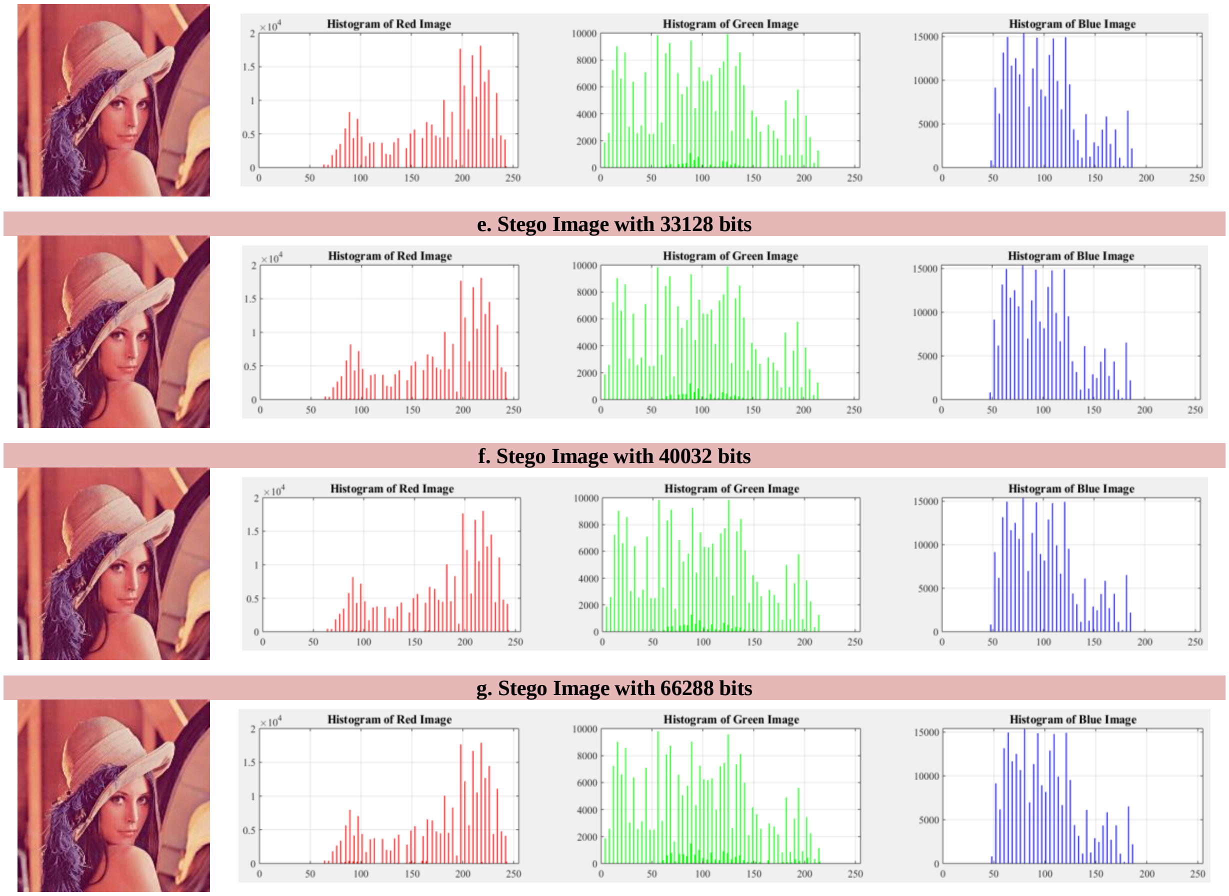
Image	Number of bits	MSE	PSNR	SSIM	Encryption Time (s)
Lena (512 × 512 × 3)	3640	0.0013	77.1531	0.9999998	0.9543
	6872	0.0023	74.4227	0.9999996	1.0754
	26224	0.0091	68.5274	0.9999983	3.2982
	33128	0.0116	67.480	0.9999976	4.4995
	40032	0.0140	66.6573	0.9999969	4.8424
	66288	0.0233	64.4589	0.9999934	8.2383


a. Original Image

b. Stego Image with 3640 bits

c. Stego Image with 6872 bits

d. Stego Image with 26224 bits

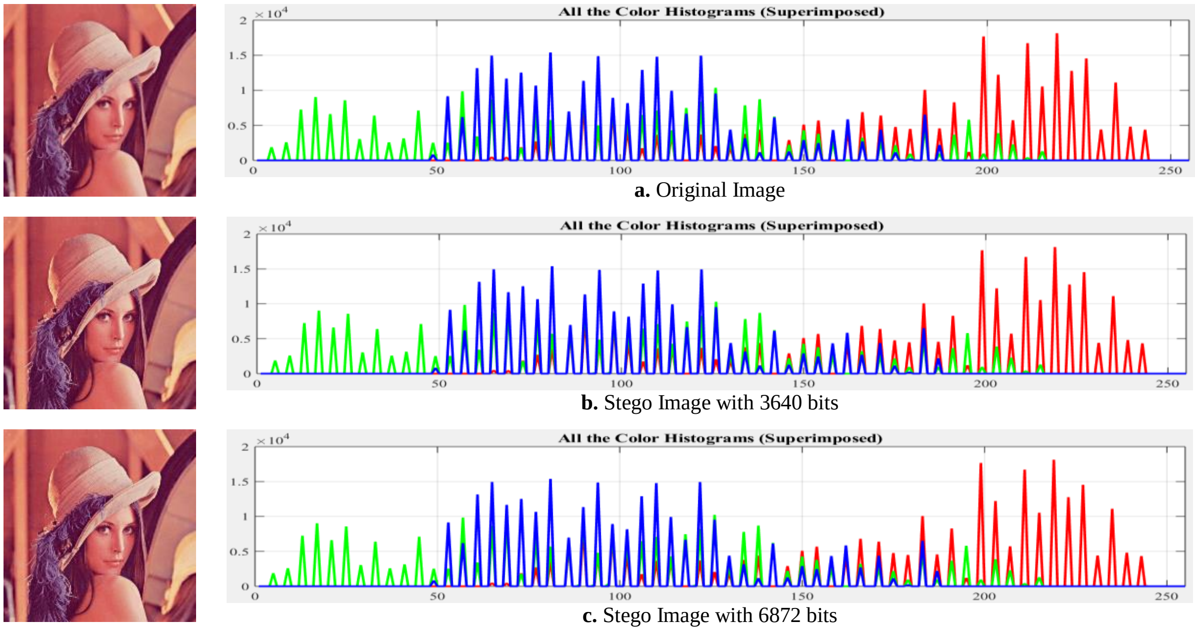


e. Stego Image with 33128 bits

f. Stego Image with 40032 bits

g. Stego Image with 66288 bits

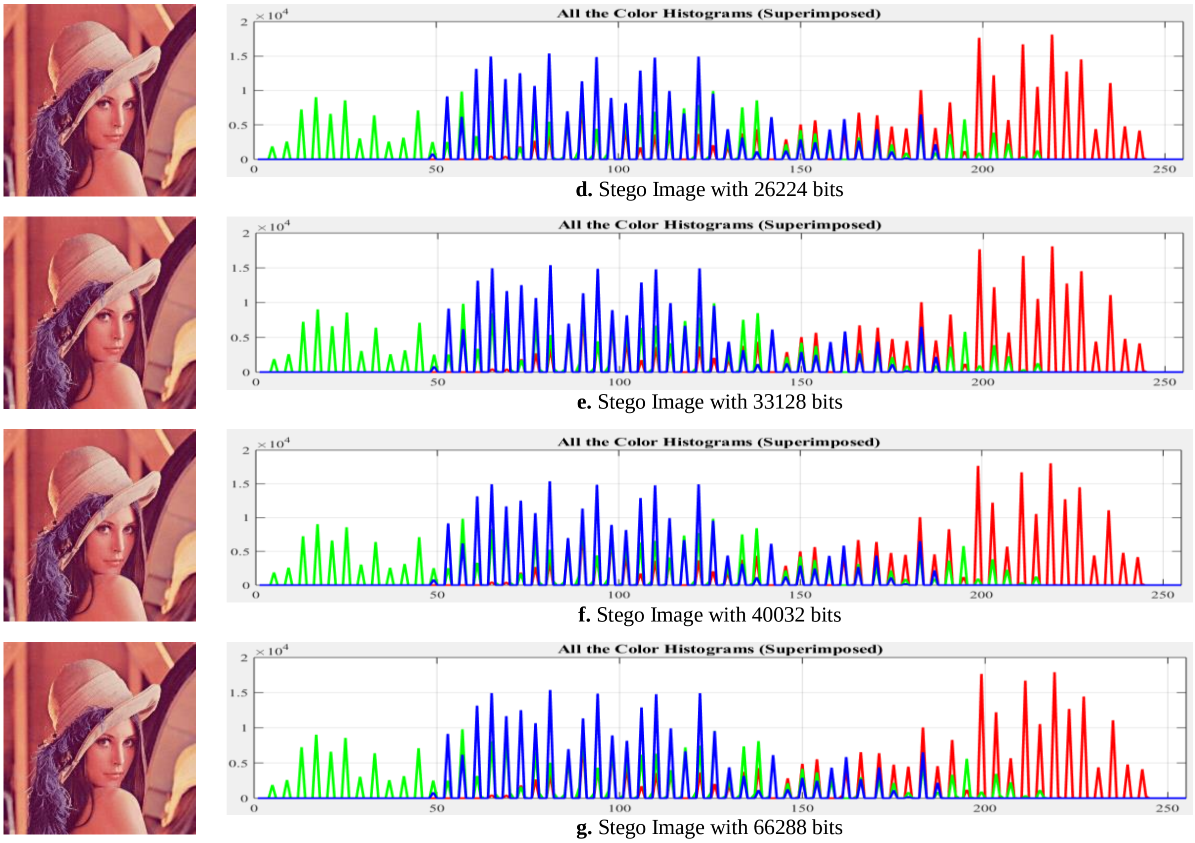
Fig. 3. The separated histograms of three colors for the original image and stego images with different lengths of secret messages bits.



a. Original Image

b. Stego Image with 3640 bits

c. Stego Image with 6872 bits



d. Stego Image with 26224 bits

e. Stego Image with 33128 bits

f. Stego Image with 40032 bits

g. Stego Image with 66288 bits

Fig. 4. All the color histograms for the original image and stego images with different lengths of secret messages bits.

TABLE V. COMPARISON RESULTS BETWEEN METHODS USING LENA IMAGE

Method	Number of bits	MSE	SSIM	PSNR
[33]	24500	-	0.997242	52.9817
[34]	960	5.73706	0.99374	40.54391
[35]	22248	0.042486	0.999919	57.079979
[36]	1200	0.0038	-	72.242
[37]	14357	-	-	41.72
[30]	32000	0.1290	-	57.0260
Proposed Method	**3640**	**0.0013**	**0.9999998**	**77.1531**
	66288	**0.0233**	**0.9999934**	**64.4589**

V. CONCLUSION

In this paper, we have presented a new method in the encryption of secret messages in the RGB image. The proposed method is used the Huffman technique in order to reduce the secret message dimensionality. In addition, there are two logic gates (i.e., XNOR and XOR) have been used in order to encrypt the Huffman of the secret message with the encryption key. The proposed method has been implemented based on six different experiments with respect to various lengths of the secret messages in bits (i.e., 3640, 6872, 26224, 33128, 40032, and 66288 bits). All experiments have been performed using the RGB Lena image with the size of (512 × 512 × 3). The experimental results are showed that the proposed method has been achieved 0.0013 MSE, 0.9999998 SSIM, 77.1531 PSNR, and it has taken 0.9543 sec when the number of the secret message was 3640 bits. Meanwhile, the proposed method achieved 0.0233 MSE, 0.9999934 SSIM, 64.4589 PSNR, and 8.2383 sec when the number of the secret message was 66288 bits. Based on the results, the proposed method is able to encrypt the secret message with a high number of bits efficiently. Future work can include using different RGB images such as Airplane, Peppers, and Baboon with varying sizes and other measurements such as Bits Per Pixel (BPP).

REFERENCES

[1] T. Limbasiya and D. Das, "Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication," IEEE Systems Journal, vol. 14, no. 1, pp. 520-529, 2019.

[2] M. Elhoseny et al., "Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions," Sustainability, vol. 13, no. 21, p. 11645, 2021.

[3] T. Naqash, A. Iqbal, and S. H. Shah, "Review on Safe Reversible Image Data Hiding," in 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019: IEEE, pp. 0929-0932.

[4] B. Swathi, K. Shalini, and K. N. Prasanthi, "A review on steganography using images," Asian Journal of Computer Science and Information Technology, vol. 2, no. 8, 2012.

[5] M. K. I. Rahmani, K. Arora, and N. Pal, "A crypto-steganography: A survey," International Journal of Advanced computer science and applications, vol. 5, no. 7, 2014.

[6] M. Mittal, S. Gupta, P. K. Keserwani, and M. C. Govil, "Security Enhancement using Vectoring, Cryptography and Steganography," in 2023 International Conference on Intelligent Systems, Advanced Computing and Communication (ISACC), 2023: IEEE, pp. 1-8.

[7] J. Kour and D. Verma, "Steganography techniques–A review paper," International Journal of Emerging Research in Management & Technology, vol. 3, no. 5, pp. 132-135, 2014.

[8] F. Sharmin and M. I. Khan, "Image steganography using combined nearest and farthest neighbors methods," International Journal of Advanced Computer Science and Applications, vol. 10, no. 11, 2019.

[9] N. Singh, "Survey paper on steganography," International Refereed Journal of Engineering and Science (IRJES), vol. 6, no. 1, pp. 68-71, 2017.

[10] M. K. Abed, M. M. Kareem, R. K. Ibrahim, M. M. Hashim, S. Kurnaz, and A. H. Ali, "Secure medical image steganography method based on pixels variance value and eight neighbors," in 2021 International Conference on Advanced Computer Applications (ACA), 2021: IEEE, pp. 199-205.

[11] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," IEEE transactions on image processing, vol. 10, no. 10, pp. 1593-1601, 2001.

[12] F. Q. A. Alyousuf, R. Din, and A. J. Qasim, "Analysis review on spatial and transform domain technique in digital steganography," Bulletin of Electrical Engineering and Informatics, vol. 9, no. 2, pp. 573-581, 2020.

[13] A. O. Modupe, A. E. Adedoyin, and A. O. Titilayo, "A Comparative Analysis of LSB, MSB and PVD Based Image Steganography," Int. J. Res. Rev, vol. 8, no. 9, pp. 373-377, 2021.

[14] S. Rustad, P. N. Andono, and G. F. Shidik, "Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)," Signal Processing, p. 108908, 2022.

[15] S. Rahman et al., "A Comprehensive Study of Digital Image Steganographic Techniques," IEEE Access, vol. 11, pp. 6770-6791, 2023.

[16] R. A. Watheq, F. Almasalha, and M. H. Qutqut, "A new steganography technique using JPEG images," International Journal of Advanced Computer Science and Applications, vol. 9, no. 11, 2018.

[17] V. Lakshminarayanan and I. Bhattacharya, "Advances in Optical Science and Engineering," Springer Proceedings in Physics, vol. 166, pp. 533-539, 2014.

[18] G. Paul, I. Davidson, I. Mukherjee, and S. Ravi, "Keyless dynamic optimal multi-bit image steganography using energetic pixels," Multimedia tools and applications, vol. 76, no. 5, pp. 7445-7471, 2017.

[19] O. I. I. Al-Farraji, "New technique of steganography based on locations of LSB," International Journal of Information Research and Review, vol. 4, no. 01, pp. 3549-3553, 2017.

[20] M. M. Hashim, M. S. M. Rahim, F. A. Johi, M. S. Taha, and H. S. Hamad, "Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats," International Journal of Engineering & Technology, vol. 7, no. 4, pp. 3505-3514, 2018.

[21] H. L. Hussein, A. Abbass, S. Naji, S. Alaugby, and J. Lafta, "Hiding text in gray image using mapping technique," in Journal of Physics: Conference Series, 2018, vol. 1003, p. 012032.

[22] Y. P. Astuti, E. H. Rachmawanto, and C. A. Sari, "Simple and secure image steganography using LSB and triple XOR operation on MSB," in 2018 International Conference on Information and Communications Technology (ICOIACT), 2018: IEEE, pp. 191-195.

[23] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Graded fuzzy edge detection for imperceptibility optimization of image steganography," The Imaging Science Journal, pp. 1-13, 2023.

[24] H. Hiary, K. E. Sabri, M. S. Mohammed, and A. Al-Dhamari, "A hybrid steganography system based on LSB matching and replacement," International Journal of Advanced Computer Science and Applications, vol. 7, no. 9, 2016.

[25] C. A. Sari, G. Ardiansyah, and E. H. Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 17, no. 5, pp. 2400-2409, 2019.

[26] S. Ghoul, R. Sulaiman, and Z. Shukur, "A Review on Security Techniques in Image Steganography," International Journal of Advanced Computer Science and Applications, vol. 14, no. 6, 2023.

[27] R. M. Neamah, J. A. Abed, and E. A. Abbood, "Hide text depending on the three channels of pixels in color images using the modified LSB algorithm," International Journal of Electrical and Computer Engineering, vol. 10, no. 1, p. 809, 2020.

[28] H. R. Kareem, H. H. Madhi, and K. A.-A. Mutlaq, "Hiding encrypted text in image steganography," Periodicals of Engineering and Natural Sciences, vol. 8, no. 2, pp. 703-707, 2020.

[29] D. Ratnasari and A. S. Aji, "Text to Color Image Steganography Using LSB Technique and XOR Operations," International Journal of Applied Business and Information Systems, vol. 3, no. 2, pp. 59-65, 2019.

[30] A. Setyono, "Securing and hiding secret message in image using xor transposition encryption and LSB method," in Journal of Physics: Conference Series, 2019, vol. 1196, no. 1: IOP Publishing, p. 012039.

[31] M. Ulker and B. Arslan, "A novel secure model: Image steganography with logistic map and secret key," in 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 2018: IEEE, pp. 1-5.

[32] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed, and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," Journal of Systems Engineering and Electronics, vol. 29, no. 3, pp. 639-649, 2018.

[33] E. A. Abbood, R. M. Neamah, and S. Abdulkadhm, "Text in Image Hiding using Developed LSB and Random Method," International Journal of Electrical & Computer Engineering (2088-8708), vol. 8, no. 4, 2018.

[34] S. N. Abd-Alwahab, M. K. WAli, and M. F. Bonneya, "Text Hiding in Coded Image Based on Quantization Level Modification and Chaotic Function," International Journal of Integrated Engineering, vol. 13, no. 1, pp. 148-158, 2021.

[35] Ö. Çataltaş and K. Tütüncü, "Comparison of LSB image steganography technique in different color spaces," in 2017 international artificial intelligence and data processing symposium (IDAP), 2017: IEEE, pp. 1-6.

[36] S. A. Mahdi and A. K. Maisa’a, "An Improved Method for Combine (LSB and MSB) Based on Color Image RGB," Engineering and Technology Journal, vol. 39, no. 1B, pp. 231-242, 2021.

[37] S. N. Mali, P. M. Patil, and R. M. Jalnekar, "Robust and secured image-adaptive data hiding," Digital Signal Processing, vol. 22, no. 2, pp. 314-323, 2012.