Vokasi Unesa Bulletin of Engineering, Technology and Applied Science (VUBETA)
https://journal.unesa.ac.id/index.php/vubeta
Vol. 2, No. 3, 2025, pp. 619~631 DOI: 10.26740/vubeta.v2i3.40143
ISSN: 3064-0768

Adaptive Steganographic Technique for Digital Images Based on The Least Significant Bit Substitution

Ekhlas Ghaleb Abdulkadhim[1*], Zaman Mahdi Abbas[2], Muqdad Abdulraheem Hayder [3]
[1,2] Collage of Tourism Sciences, University of Kerbala, Kerbala, Iraq
[3]College of Education for Human Sciences, University of Kerbala, Kerbala Iraq

Article Info

Article history:

Received May 03, 2025
Revised June 09, 2025
Accepted August 10, 2025

Keywords:

Information Hiding
Image Steganography
LSB
Histogram Analysis
Image Quality Assessment Metrics

ABSTRACT

It has become natural to retain most of the information electronically, due thanks to developments and improvements in information and communication technology. Thus, information security has become a major significant problem. Aside from cryptography, this study employs two strategies could be utilized to share information securely to ensure secure information sharing. Cryptography and steganography are two of these mechanisms. Using an encryption key known to both the receiver and the sender, the message is encrypted. Without the encryption key, no one will be able to read the message. Thus, this study proposes an efficient method based on the Least Significant Bit (LSB). Employing the LSB substitution approach ensures reliability, since as it can decrease the embedding error rate. For image-based steganography, our algorithm is formed by exploiting LSB substitution combined with a Multi-Level Encryption Algorithm (MLEA) the algorithm combines LSB substitution with a Multi-Level Encryption Algorithm (MLEA), Secret Key (SK), transposition, and flipping. According to the experimental results, the proposed method is efficient and produces effectual effective outcomes. Several Quality Assessment Metrics (QAMs) evaluate 125 unique RGB images with varying degrees of hidden information, such as including PSNR, Contrast, and Image Histogram (IH). Besides security analysis, the results prove that the proposed approach withstands RS analysis with great strength. Furthermore, our experimental results demonstrate that this study thoroughly tests the proposed technique with several steganographic and statistical indicators. When it compared to those of other available approaches, the analysis confirms the practicality of our method, and which is easy to implement and superior.

1. INTRODUCTION

Information becomes more susceptible to attackers during transmission through various routes, particularly when it occurs over the internet [1][2]. Any compromise of sensitive data might cause long-lasting problems, making secure information sharing across communication channels critical. The necessity to safeguard data in transit has prompted the development of a number of several methods for doing so [3]. There isn't is no a silver bullet single solution for Internet security; every solution approach has its own set of pros and cons. Steganography is a well-liked technique that hides data inside within seemingly innocuous things items, such as photos, movies videos, music, and text [4]. The information concealed within these artifacts is difficult for the untrained sight eye to discern, since as steganography is a method that encrypts the cover medium, making its existence invisible to the human eye [5]. Images offer the best performance in concealing information among the cover items listed before, which is why they are the most popular choice for steganography.

Information hiding is a technique for concealing sensitive data within ordinary data [6]. This creates a covert communication channel between the sender and recipient, making the channel's existence invisible The

*CorrespondingAuthor
Email: ekhlas.g@uokerbala.edu.iq

use of audio steganography creates a covert communication channel between the sender and recipient, making the channel's existence invisible [7]. Information concealment is a new field of study that includes watermarking, steganography, fingerprinting, copyright protection and steganography and copyright protection. All of these information-hiding applications are fairly diverse [8]-[10]. Figure 1 illustrates the classification of information concealment. The classification of information concealment is shown in Figure 1.

Achieving a realistic information-hiding solution to hide conceal texts within images is the main primary objective of this study. It allows the user to give provide the system with both the text and the cover, and receive an image with the concealed content inside [11][12]. The transmission of an encrypted communication, on the other hand, may readily arouse the suspicions of an attacker. Thus, it is possible to decrypt the encrypted message, attack it, or intercept it the encrypted message [13][14]. So, to solve To address the problems and defects of encryption systems, Steganography approaches have been developed several steganography approaches have emerged through ongoing research. As a result, steganography conceals the existence so that no one can discover it [15][16].

So Therefore, we can define steganography as the best most effective technique for hiding information in digital media [17]. This is the opposite of the encryption system, as before the message is sent through the network The steganography process is the opposite of the encryption system. Before the system transmits the message across the network, it is embedded embeds in a digital host, which hides conceals the presence of the message [18][19]. This pattern may also include copyright protection for digital media, such as video, images and audio, in addition to while maintaining data privacy and confidentiality [20]. The expansion of modern communication capabilities requires necessities the use of specialized security methods and measures, especially particularly in the field of computer networks [21]. Providing network security is of paramount importance as the amount of data transmitted through the Internet increases. As a result, data confidentiality and integrity must be safeguarded versus against uncertified access and use [22][23]. The field of information concealment has exploded experienced a surge in popularity [24]. We can summarize the types of Steganography as shown below:

- Text Steganography: A term that includes hiding information within text files. This method buries confidential information behind every letter n of all the words in the text message.
- Image Steganography: It is the technique for hiding data through the use of a cover object, where the image becomes known as a steganography image. For the purpose of data hiding, pixel density is used to mask the images the system uses pixel density to mask the images.
- Audio Steganography: This way requires hiding data in audio files. Data in AU, MP3, and WAV audio files can be hidden using this approach The method embeds data in AU, MP3, and WAV audio files. Various methods hide audio, including phase coding, low-bit-rate coding, and spread spectrum.
- Video Steganography: An encryption method for any type of file or data into a digital video format. This method includes hiding data within the video (a mixture of photos) [25].
- Network or Protocol Steganography: This technology uses the network protocol as a cover object in order to hide data, such as IP, TCP, and UDP. Researchers use the OSI layer network model because it contains secret channels [26].

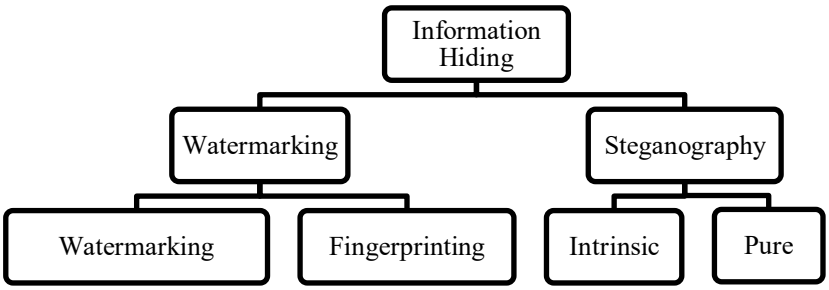


Figure 1. A classification of information hiding

In order To protect sensitive information from internet threats, steganography offers provides a variety range of techniques for hiding concealing data in within multimedia files [27]. The aforementioned strategy relies on the goal to obfuscate a message in images, which provides a secure and robust means of data transmission; LSB replacement is the most effective way to conceal information in multimedia.[28]. After that,

we convert the intensity of each color to its matching binary value. The secret message, denoted as 'B', is encoded using dual values after being transformed to ASCII values. Because of Due to its useful valuable qualities, the approach uses utilizes the RGB color model. Each pixel in this architecture makes use of utilizes 24 depths bits, and the 8-bit representations of colors vary range from 0 to 255 [29]. Because RGB can replicate more conceivable colors through the combination of its three hues, it is well-suited for encoding additional information. By taking RGB into account, we are dealing with a binary picture whose representation spans the integers 0-255, with the leftmost bit being the LSB and the rightmost bit the MSB. Also, think about consider the 0–255 range; changing the MSB from 0 has a huge significant impact, since as it alters the color intensity by 99%. There will be minimal change, say, of up to 2%, if we alter LSB from 1 to 1 or 0 to 1. Consequently, the suggested algorithm made use of utilizes LSB (Least Significant Bit) ideas to encrypt the secret data; the literature states that up to four LSB bits can be used to encrypt secret data the literature reports that up to four LSB bits can be encrypted, making it harder more difficult for a human to decipher. Modern, state-of-the-art approaches rely on just a few parameters, which makes them unreliable. The development of a new, trustworthy procedure primary objective of this endeavor is the primary objective of this endeavor to develop a new, trustworthy procedure. In order To ensure that the suggested method matched met fundamental requirements of image steganography, it was subjected to a careful thorough analysis from multiple angles and in various forms. Many ideas or elements for the balance tradeoff were utilized The researchers employed various techniques and elements to achieve the balance tradeoff, including the magic matrix, MLEA, Key, and LSB up to 4 bits, etc. among others, to meet all of the requirements for picture steganography [30]. Our proposed approach gives provides spatial and frequency domains, like such as ML and DL models, with all the necessary picture formats, dimensions, and colors they need in an efficient manner. What follows is a list of the main contributions.

Using the least significant bit replacement, we present and construct a digital image steganography technique.

- To achieve strong security, our suggested technique uses cover images that are selected appropriately and picture steganography parameters that are dependable.
- To achieve better results, our suggested method uses message bits embedded in randomly selected cover picture pixels.
- The proposed method is more efficient than state-of-the-art methods, according to the experimental data.

There are a total of This study consists of four parts to the rest of the document. Following an overview of relevant preparatory efforts in Section II, the following subsequent sections provide more detail on the suggested methodology and analyze and discuss the trial results in Section IV, and. Finally, the research is summarized in Section V section V summarizes the research.

Steganography plays an essential a crucial role in data encryption, especially particularly in the modern digital age. A plethora of steganographic techniques have evolved to meet the increasing demand for cyber-attack protection, including Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), LSB, and 2LSB. When deciding on a storage size and level of security, each approach has its own set of pros and cons.

Hakim et al.[31] rely Relies on the purpose to conceal a message in video pictures (AVI), which provides a secure and robust way of information transmission, and LSB replacement is the most efficient approach for hiding information in multimedia. Among the many benefits of their proposed video steganography system is the fact that it is both simple and effective in installing concealing the covert message, which increases its security and makes it very difficult to determine its exact location on the video due to the large file size (the number of frames). Researchers Hakim et al.[31]. In addition to LSB, several other steganographic techniques have been developed to conceal information within digital images, particularly in the frequency domain, such as 2LSB, DCT, and DWT. These techniques offer advantages in terms of resilience against image compression and modification, a known limitation of spatial domain-based methods, like such as 2LSB, as noted by Majeed et al.[32].

The 2LSB method advances the LSB steganography technique, a commonly used to conceal method for concealing information within digital images. The LSB method hides conceals data in the LSB of each pixel, producing resulting in minimal changes that remain undetectable to the human eye, as noted by Abduljaleel et al.[33]. Jabbar et al.[34], demonstrated that the 2LSB method offers significant advantages in hiding data without degrading image quality. Zhang et al.[35], The researchers used the DCT method because it operates in the frequency domain, this method provides providing superior resilience to lossy compression formats such as JPEG, which typically compromise hidden data in spatial-based methods like LSB and 2LSB. One of DCT's main advantages is its ability to retain hidden data even when the image undergoes compression or format modification (Modupe et al.) [36]. DWT is another technique frequently used in frequency-based image steganography. This method operates by decomposing an image into several frequency components, allowing data to be hidden in either the lower or higher frequencies according to the specific needs, as described by Jamele et al. [37]. One of DWT's advantages is its capability to handle high-resolution images, as well as its resilience to steganalysis attacks, which is more robust compared to spatial-based methods (Alexan et al.) [38].

2. METHOD

The LSB approach is used as a steganographic technique to conceal data within digital photographs in this study. The capacity ability to increase data storage capacity and decrease detection risk utilizing through the use of steganalysis techniques led to the selection of this strategy. Gathering relevant information is the initial stage of this work. Digital photos and the information to be incorporated make up the data. In order to make sure To ensure that changes are not clearly immediately noticeable, it is recommended that pictures chosen for message storage have good visual qualities this study recommends using images with high visual quality for message storage, such as high resolution and consistent colors. Gathering the data to be embedded, like text messages or binary files, follows the selection of the images. To further guarantee the security of the concealed information, the embedding algorithm is used to encrypt this data. The randomness of encryption output makes it harder to identify steganalysis techniques.

In our proposed procedure, defining the algorithm's notations is the initial stage. From Equations 1 to 8, we have used the symbol (FT) as a transposed image, (CI) as a cover image, (SM) as a stealthy message, and (FI) as a flipped image. Figure 2, Equations 1-8, and the suggested method all use S^{key} and S^{Im} as symbols to announce Skey and the stego-image, respectively. What follows is a more in-depth explanation of the algorithm. When we encode data into a picture an image, we have to must follow a certain specific process. We start by flipping the cover image upside down. We then used Equation 3 to separate the flipped image into its respective green, red, and blue channels.

After dividing the blue channel into four equal halves, we use MGMx to shuffle them: BC1', BC2', BC3', and BC4'. The red channel values and differences in the standard model are then determined by CalDiff CalDiff then determines the red channel values and differences in the standard model. To decipher the message, we have used a secret key (Skey) and CalDiff in our suggested method, a Multi-Level Encryption Algorithm (MLEA). To encrypt the cover data in the blue cases and a randomly generated format, we can use the secret key, thanks to this functionality. We ultimately obtain the stego-image, SIm, by amalgamating the Skey with the red, green, and blue channels. Our exclusive message is securely embedded via MLEA in the four overlapping blocks of Blue channels, making decoding extremely complicated for highly complicated for adversaries. For more security in our proposed method, we used the magic matrix. A magic matrix is a matrix where the sum of every row and every column and the main secondary diagonal is similar, as shown in Figure 3. So, the blue channel's blocks are shuffled about at random by the magic matrix to improve the system

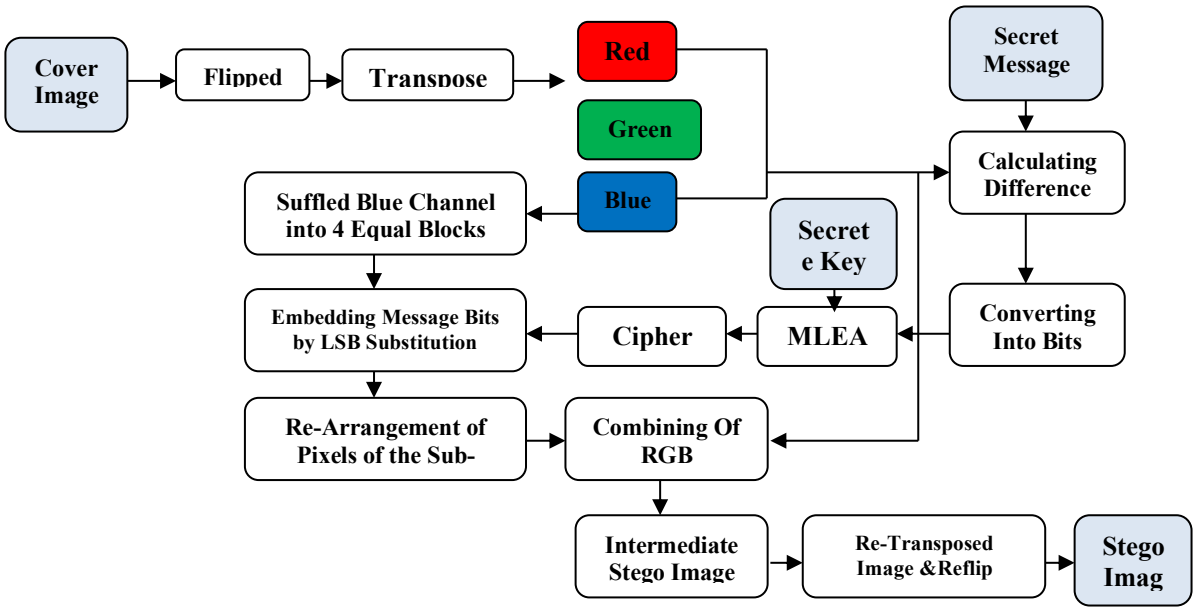


Figure 2. Proposed method

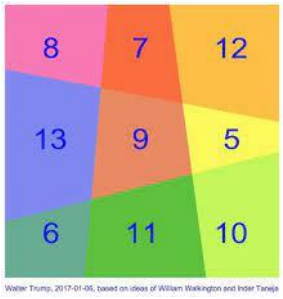


Figure 3. An example of the Magic Matrix

$$F^1 = flip\ (C^1) \quad (1)$$

$$F^T = transposed\ \ (F^1) \quad (2)$$

$$R^C\ , G^c, B^c = F^t \quad (3)$$

$$B^{c1}, B^{c2}\ , B^{c3}\ , B^{c4} = Sub\ Division\ of\ (B^c) \quad (4)$$

$$B^{c1\prime}, B^{c2\prime}\ , B^{c3\prime}\ , B^{c4\prime} = Shuffled\ using\ \ M^G\ M^X\ (B^{c1}, B^{c2}\ , B^{c3}\ , B^{c4}\ ) \quad (5)$$

$$C^{al}\ D^{iff}\ \ =\ \ Calculating\ Differencing(\ S^M, R^C) \quad (6)$$

$$C^{Text} = MLEA\ (\ C^{al}\ D^{iff}\ , S^{key}) \quad (7)$$

$$S^{IM} = Reconstruct\ Stego\ Image\ \left(\ S^{key}, B^{c1\prime}, B^{c2\prime}\ , B^{c3\prime}\ , B^{c4\prime}\ , R^C\ , G^c\right) \quad (8)$$

F^1=flipped Image,C^1=Cover Image,F^T=Transposed Image, C=Channels(R^C=Red ,G^C=Green, B^C=Blue) (B^{C1},B^{C2},B^{C3},B^{C4})=Sub Blocks of Blue Channel, M^G M^X=Magic Matrix, $C^{al}D^{iff}$= Calculating Differencing, S^{key}= Secret Key.

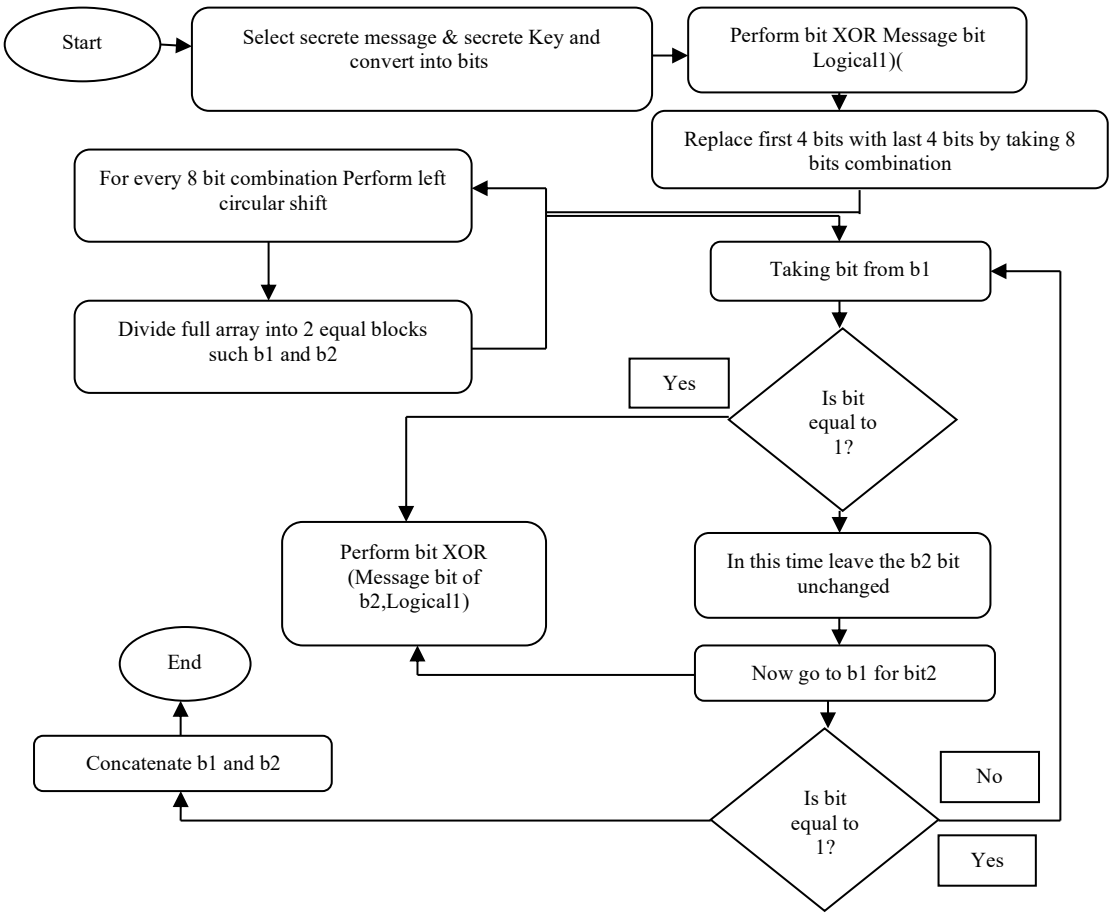


Figure 4. MLEA for Suggested Steganographic Method.

2.1. Embedding algorithm

Initially, we adopt an image as a cover image, next flip and transpose it. Upon the separation of separating the FT pictures into RGB channels, the blue channel is further partitioned into four equal segments for the purpose of message encryption the system further partitions the blue channel into four equal segments for message encryption. The blue channel is randomly combined utilizing a magic matrix to guarantee the protection of all individuals. The secret message bits and the red channel are used to calculate different values The system uses the secret message bits and the red channel to calculate different values. Along with appealing to MLEA, the secret key bits, we can produce a ciphertext Figure 4. Ultimately, employ the LSB to place the ciphertext into the sub-blocks of the four blue channels. One of the most important features of the MATLAB function, the magic matrix, is its ability to rotate and reflect, which means it does not introduce repeated values. The above means keeping the diagonals, columns, and rows of the matrix unchanged. In order To protect the system from tampering, the system must perform a simple process before encryption, which is involves covering the image using an MLEA and the secret key. Usually, MLEA performs image enhancements before encoding. MLEA swaps the start and end bits using XOR operations in order to ensure that all eight bits are used at once MLEA employs XOR operations to swap the start and end bits, ensuring the simultaneous use of all eight bits. Two identical block arrays are created by applying a left circular shift operation to each 8 bits. B1 and B2 are generated. The system generates B1 and B2. With B1 i== 1 and OR B2 by 1, etc.

2.2. Extraction Algorithm

We can produce the decoded message by using the stego image as input, flipping it, and then transposing it, which is the exact adverse inverse of the encoded message. To retrieve the matching red, green, and blue channels, activate flag 1. Check that the conditions for collecting the hidden message pixels from the four sub-blocks (BC1', BC2', BC3', and BC4') of the blue channel are consistent.

3. Evaluation And Experimental Results

We use utilize comparable studies to emphasize highlight the importance significance of this research. After rigorous examination, we used the proposed technique to analyze 12 LSB sub-based methods, including LSB-GLM, LSB-RGB, LSB Inverted, and Robust LSB. The Image Processing Place (IPP) and (USC-SIPI-2022) provided 125 pictures for the dataset used to evaluate the technique. The outcomes confirm that the suggested method can embed hidden messages without leading to causing any interference, deformation, or fishy suspicious behavior. Find more details below.

In addition Additionally, the suggested technique included histogram analysis on a few selected photos. To find out how compare the cover and stego photos compare to each other, we can use the histogram, which determines the exact frequencies of each pixel in the image. By dissecting the histograms of several images, such as Girl, Book, and Vegetables, we conduct a basic evaluation of the suggested method. The results show indicate that the plan can work is effective.

This study evaluates the proposed technique from many multiple angles and uses utilizes color graphics to explain illustrate it. Peak Signal-to-Noise Ratio is the key parameter for evaluating Stego and cover pictures. PSNR controls visual quality. PSNR over 30 dB indicates high-quality images. Equation (9) calculates 34 PSNR. Peak signal-to-noise ratio (PSNR) is computed using 10πlog10(Cmax² MSE) The system computes the peak signal-to-noise ratio (PSNR) using 10πlog10 (Cmax² / MSE).

The algorithm's analytical results are presented in Tables 1, 2, 3, and 4 sequentially. The proposed technique outperforms current solutions based on several views from multiple perspectives. The key to effective steganography is finding determining the right optimal bit rate for embedding messages in specific-sized images of a specific size. Calculate the message and image pixels before inserting the secret message into the image to determine the right proportions and image formats for each text size. This is why the proposed method should be examined from all angles The study should examine the proposed method from all angles. Choosing Selecting the right correct cover object for secret message encryption encrypting secret messages is essential crucial for secure web transmission. The proposed study shows demonstrates that the technique works is effective across various picture formats, including PNG, JPG, and BMP, picture formats, as well as different dimensions, and PSNR viewpoints. This section will examine the proposed work using various QAMs for security.

The suggested technique also carries out performs histogram analysis utilizing using a few small number of images. Usually Typically, a histogram is used to determine the specific frequencies of each pixel in an image a histogram determines the specific frequencies of each pixel in an image, a histogram is used, and to detect allowing for the detection of point-by-point contrast between cover and stego images. We primarily evaluate the suggested technique by segmenting the histograms of several images, including Girl, Book, and Vegetables (see Figures 5 and 6).

Table 1. Images(512x512) pixels with 15KB

Images	M-Size	PSNR Results
Girl		77.1
Book	15KB	81.4
Vegetable		85.7
Average of 125 images		81.4

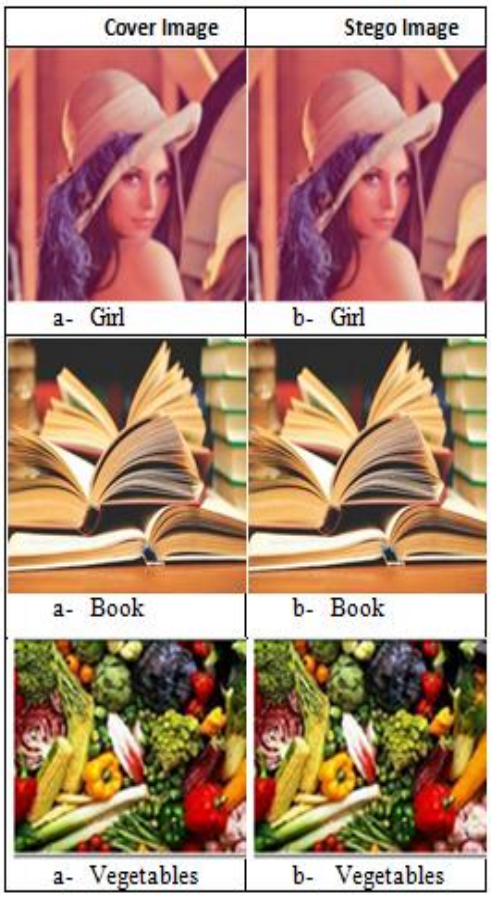


Figure 5. Comparisons of the cover image and the stego image

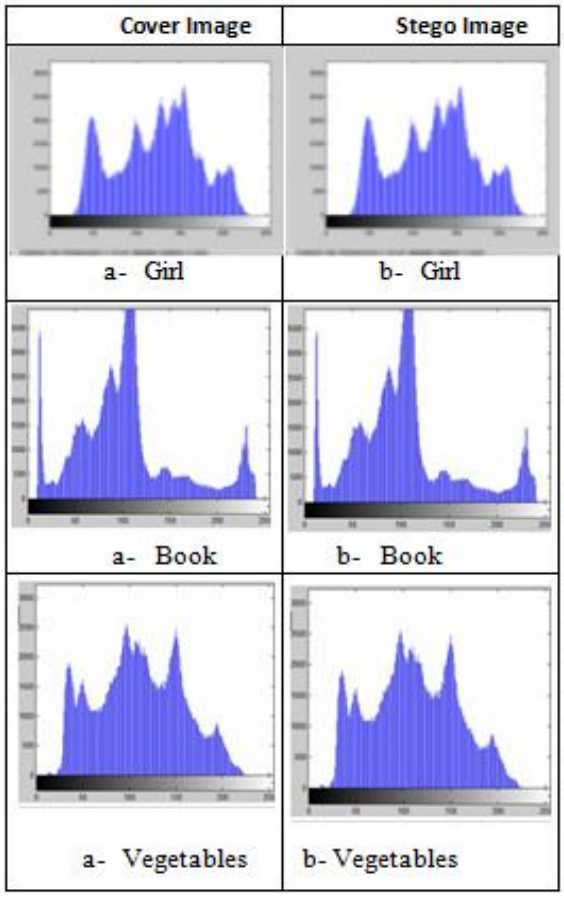


Figure 6. Comparisons of histograms within cover and stego images

Table 2. PSNR Results of different images by applying P2

Images	Girl		Book		Vegetables	
	128x	72.4	128x	71.2	128x	71.0
Dimensions and PSNR Results	256x	77.7	256x	74.6	256x	72.3
	512x	80.5	512x	75.9	512x	73.6
	1024x	76.86	1024x	73.9	1024x	72.3
Average of 125 images	Average of PSNR Results of different Dimensions(D)	D-128=70.5	D-256=75.13	D-512=77.12	D-1024=84.3	

3.1. Performance Analysis

This study uses peak signal-to-noise ratio predictions to assess the method. Stego picture quality is usually measured by PSNR typically measures the quality of steganographic images. Table 3 shows PSNR values for three stego images. PSNR directly affects stego image quality. When the cover picture C is M × M and the stego image S is N × N, the pixel values (x, y) for the cover image range from 0 to M-1, while those for the

stego image, they range from 0 to N-1. The PSNR can be calculated as follows The system calculates the PSNR as follows:

$$PSNR = 10.Log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (9)$$

Image pixel values max out reach they're at MAX the maximum value. If pixels were 8-bit per sample, the maximum value is 255. A greater PSNR suggests better stego image quality. The system calculates the PSNR using Eq. (9). Table 5 for PSNR values shows presents the PSNR values-based values for state-of-the-art methods with and the proposed method.

Table 3. PSNR Results of Images (512x512) embedded in (9,10,11, and 14KB) Text Sized

Images	Girl		Book		Vegetables	
	9KB	71.2	9KB	69.1	9KB	88.3
Dimensions and PSNR	10KB	73.3	10KB	71.3	10KB	82.1
	11KB	75.4	11KB	72.6	11KB	84.5
	14KB	80.1	14KB	76.3	14KB	81.6
Average of 125 images	Average PSNR Results on Multiple Text Size	9KB=76.2	10KB=75.56	11KB= 77.5	14KB= 79.33	

Table 4. PSNR Results of image types (JPG, PNG, BMP) with Dimension (512x512) 15KB Message Size

Images	The Size of Message	JPG.	PNG.	BMP.
Girl		83.36	86.75	69.77
Book	15KB	81.42	82.92	74.57
Vegetable		85.17	85.61	82.86
Average of 125 images		83.31	85.09	75.73

Table 5. Advanced methods based on PSNR values, with the suggested method.

Comparison Between Multiple Steganography Methods			
Images	Girl	Book	Vegetable
GLM[39]	78.34	79.86	77.33
Secure RGB[40]	77.99	81.31	82.10
Inverted LSB[41]	70.91	79.99	80.00
LSB IMST[42]	73.04	82.98	84.32
IMST[43]	76.99	80.09	82.98
Robust ST[44]	77.32	76.66	79.97
Proposed Method	79.35	84.02	88.15

In comparison to the images in Figures 5 and 6, the cover and stego shots exhibit minimal distortion. Consequently, the suggested steganography method is a potent and resilient strategy for generating stego pictures images that remain indecipherable to external observers. The suggested technique focuses on utilizing the Bitmap (BMP) picture image file format. The BMP file format is utilized for handling graphic files in Windows The system utilizes the BMP file format to handle graphic files in Windows. Another advantage of utilizing BMP files in Windows applications is its their simplicity and widespread use. The pixel size correlates with is directly related to the image dimensions in a BMP file. Consequently, it offers increased capacity for encoding binary codes. The greatest most significant quantity of concealed characters can be augmented while simultaneously reducing the total file size through the application of the zip technique. We evaluate BMP images with the proposed approach across different dimensions to examine the diverse data sizes included within them. The outcomes of the diverse assessments are presented in The study presents the outcomes of the diverse assessments in Table 6. Which is compares the dimensions of various BMP images utilizing the suggested steganography algorithm The study compares the dimensions of various BMP images using the proposed steganography algorithm.

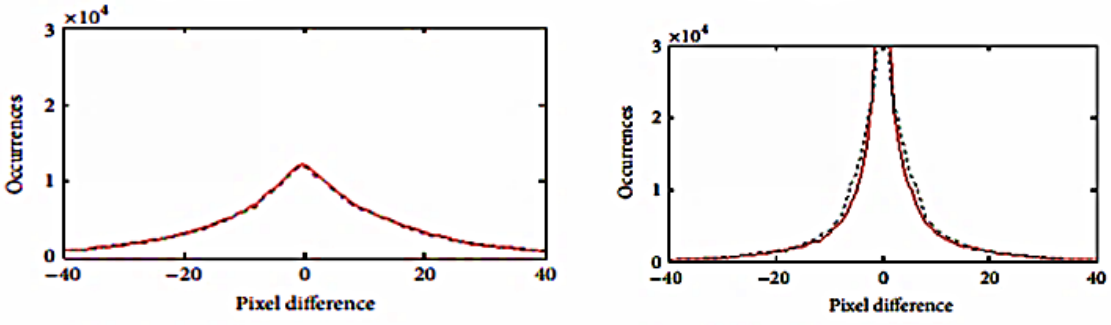
Table 6. Comparison of different sizes in Bitmap images

File Size				
Cover Image	Text File	Stego Image	Hide Message	Retrieve
513 KB	3.81KB	564 KB	✓	✓
472 KB	20.1KB	Failed	-	-
1.1 MB	11.1 KB	1.44 MB	✓	✓
1.0 MB	10.2 KB	Failed	-	-
2.84 MB	12.1 KB	4.29 MB	✓	✓
4.14 MB	17.0 KB	4.19 MB	✓	✓
2.34 MB	54.1 KB	Failed	-	-
7.14 MB	55.1 KB	8.99 MB	✓	✓
8.7MB	384 KB	13.2 MB	✓	✓
8.9MB	415 KB	Failed	-	-

3.2. Security analysis

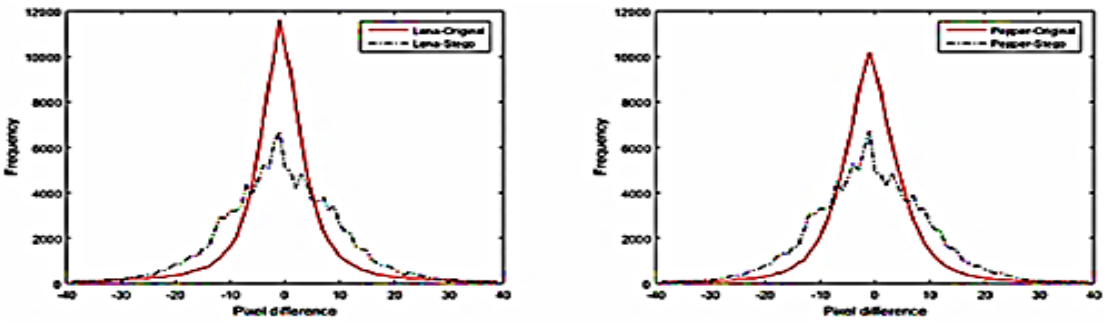
The section detailing the method's security has been covered covers the with to about Pixel Difference Histogram (PDH) and RS steganalysis. The most conventional and effective quantitative steganalysis for LSB-based methods is the PDH and RS analysis [45], which can reveal whether there is a lack of data in the stego-picture. The negative consequences of the RS investigation hit significantly impacted the LSB replacement methods hard, while the negative consequences of the PDH investigation hit had a profound effect on the PVD methods hard. Since the suggested approach makes use of utilizes concepts like such as adjusted LSB replacement and value differencing, it should be examined by both RS inquiry and PDH. To dissect the efficacy of the expanded procedure the analysis should apply both RS inquiry and PDH [46], RS steganalysis is employed here. So, to examine or hack the secret-covered picture, the RS plot applied over 500 inserted photographs.Therefore, the structure described in [47][48] guides both RS and PDH considerations. Examining two reference pictures with RS, in Figure 7a and b display the Girl and the book.

On the x-axis, we can see the ratio of hiding abilities, and on the y-axis, we can see the ratio of unique and regular groupings. In order to draw a quadrilateral, four variables are required, as stated in references [46]-[50]: S-m, Sm, R-m, and Rm. In order for the RS analysis to reveal the presence of implanted bits, Rm-Sm must be smaller than R-2m-S. When running RS analysis on datasets with Sm ≈ S-m and Rm ≈ R-m, the steganographic-based method cannot be detected. The condition Sm*S-m* < *Rm*R-m applies because the curves of R-m and Rm lie above the curves of S-m and Sm, and because the curves of S-m and Sm are of identical length. Both of these facts appear in Figure 8a and 8b. Not only that, but Rm and R-m have identical lengths. Therefore, the intended strategy is quite resistant, as shown by RS research. To verify the strategy's efficacy of the strategy we must incorporate LSB and value differencing concepts into PDH and RS evaluations. To show the disparity between the two dimensions—pixel difference and frequency—we use a PDH graph. Two typical images, "Girl and the book", were analyzed using PDH. The study presents the results in Figures 8a and 8b. The dotted line shows the cover image, while the solid line shows the PDH analysis of the stego image. It is clear that The step impact and crisscross presence are negligible. The curves and arcs, on the other hand, demonstrate how smooth the smoothness of the stego image is. Therefore, it is reasonable to assume that the suggested approach is pitifully resistant to PDH verification.



a) Girl b) Book

Figure7. RS Plot of Girl and Book standard images.



a) Girl b) Book

Figure 8. PDH Plot of Girl and Book standard images.

4. CONCLUSION

In this study, we suggested a secret key-based LSB substitution image steganography technique. The suggested method uses employs a random concept approach to adopt select cover image pixels to and insert message bits, to achieve thereby achieving better improved performance. The evaluation of steganographic techniques involves the comparison between comparing the steganographic capacity and with the quality of the digital image. The proposed method in this study can effectively improve enhance the steganographic capacity and the quality of the digital images. Experimental outcomes demonstrate that this study critically evaluates the proposed technique using several steganography methods and various statistical criteria. The obtained outcomes display demonstrate that our suggested proposed method works efficiently with various QAM models, such as including PSNR.

Furthermore, researchers emphasize that the experimental outcomes demonstrate a high level of durability, acceptable payload limits, insensitivity, and resistance to scaling, slicing, modification, and other types of attacks. The drawbacks of this work are include the use of the RGB color model, a restricted limited payload, and high time complication complexity. What is more Moreover, the provided approach holds up performs poorly under PDH analysis but remarkably well under RS analysis.

In the future, combining image hiding with encryption may be explored to achieve a better data hiding system. It should also prioritize compression methods like the Huffman code, the HSI model, and the acronoment method. Additionally, to acquire achieve effective steganography for secure transmitter-receiver communication, it may be necessary to employ specific machine learning approaches, like such as unsupervised learning or different various deep learning architectures.

REFERENCES

[1] A. OluwakemiC., A. Kayo S., and O. Ayotunde J., "Efficient Data Hiding System using Cryptography and Steganography," *International Journal of Applied Information Systems*, vol. 4, no. 11, pp. 6–11, 2012. https://doi.org/10.5120/ijais12-450763

[2] J. Kaur and S. Sharma, "Enhanced Image Steganography Technique Using Cryptography for Data Hiding," *New Approaches for Multidimensional Signal Processing*, pp. 175–185, 2021.https://doi.org/10.1007/978-981-33-4676-5_13

[3] E. Ghaleb Abdulkadhim, S. Hammad Dhahi, and M. Salman Al-Shemarry, "Review on Various Image Protection Methods," *Journal of Al-Qadisiyah for Computer Science and Mathematics*, vol. 15, no. 4, pp. 41–47, 2023. https://doi.org/10.29304/jqcsm.2023.15.41364

[4] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin, and M. Z. I. Shamsuddin, "Information Hiding using Steganography," *National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings,* pp. 21–25, 2003. https://doi.org/10.1109/NCTT.2003.1188294

[5] R. Ibrahim and T. S. Kuan, "Steganography Algorithm to Hide Secret Message inside an Image," vol. 2, pp. 102–108, 2011.

[6] M. A. Hayder and E. G. Abdulkadhim, "Enhance a Cloud-Based Distance Learning Computing Management System (LCMS)," *Intelligent Systems and Networks*, pp. 686–693, 2021. https://doi.org/10.1007/978-981-16-2094-2_78

[7] S. R. Kim, J. N. Kim, S. T. Kim, S. Shin, and J. H. Yi, "Anti-reversible Dynamic Tamper Detection Scheme Using Distributed Image Steganography for IoT Applications," *The Journal of Supercomputing*, vol. 74, pp. 4261–4280, 2018. https://doi.org/10.1007/s11227-016-1848-y

[8] O. Evsutin, A. Melman, and A. A. Abd El-Latif, "Overview of Information Hiding Algorithms for Ensuring Security in IoT based Cyber-Physical Systems," *Security and Privacy Preserving for IoT and 5G Networks*, pp. 81–115, 2022. https://doi.org/10.1007/978-3-030-85428-7_5

[9] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "An Overview of Steganography Techniques Applied to the

Protection Of Biometric Data," *Multimedia Tools and Applications*, vol. 77, no. 13, pp. 17333–17373, 2018. https://doi.org/10.1007/s11042-017-5308-3
[10] I. Banerjee, "Text Steganography using Article Mapping Technique (AMT) and SSCE," *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 2, no. 4, 2011. https://doi.org/10.5815/ijcnis.2012.12.08
[11] V. Lakshmi and B. V. Raju, "FPGA Implementation of Lifting DWT Based LSB Steganography Using Micro Blaze Processor," *Int. J. Comput. trends Technol.*, vol. 6, no. 1, 2013.
[12] A. Kamilaris and A. Pitsillides, "Mobile Phone Computing and the Internet of Things: A Survey," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 885–898, 2016. https://doi.org/10.1109/JIOT.2016.2600569
[13] T. Qiu, R. Qiao, and D. O. Wu, "EABS: An Event-Aware Backpressure Scheduling Scheme for Emergency Internet of Things," *IEEE Transactions on Mobile Computing*, vol. 17, no. 1, pp. 72–84, 2017. https://doi.org/10.1109/JIOT.2016.2600569
[14] E. Ghaleb, "Design and Optimization of Tourism Information Management System Based on Artificial Intelligence," *Wasit Journal for Pure Sciences*, vol. 3, no. 3, pp. 101–111, 2024. https://doi.org/10.31185/wjps.508
[15] E. G. Abdulkadhim, M. S. Al-Shemarry, and E. M. T. A. Alsaadi, "An Efficient Algorithm for Covert Contacting in IoT," *AIP Conference Proceedings*, vol. 3097, no. 1, 2024. https://doi.org/10.1063/5.0209934
[16] S. Pramanik, "A New Method for Locating Data Hiding in Image Steganography," *Multimedia Tools and Applications*, vol. 83, no. 12, pp. 34323–34349, 2024. https://doi.org/10.1007/s11042-023-16762-3
[17] Y. Yao, J. Wang, Q. Chang, Y. Ren, and W. Meng, "High Invisibility Image Steganography with Wavelet Transform and Generative Adversarial Network," *Expert Systems with Applications*, vol. 249, p. 123540, 2024. https://doi.org/10.1016/j.eswa.2024.123540
[18] H. H. Nguyen, S. Marcel, J. Yamagishi, and I. Echizen, "Master Face Attacks on Face Recognition Systems," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 4, no. 3, pp. 398–411, 2022. https://doi.org/10.1109/TBIOM.2022.3166206
[19] L. Ambardi, S. Hong, and I. K. Park, "Segtex: A Large Scale Synthetic Face Dataset for Face Recognition," *IEEE Access*, vol. 11, pp. 131939–131949, 2023. https://doi.org/10.1109/ACCESS.2023.3336405
[20] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image Steganography using LSB and Hybrid Encryption Algorithms," *Applied Sciences*, vol. 13, no. 21, p. 11771, 2023. https://doi.org/10.3390/app132111771
[21] C. A. Sari, "Secure Image Steganography Algorithm Based on Dct with OTP Encryption," *Journal of Applied Intelligent System*, vol. 2, no. 1, pp. 1–11, 2017. https://doi.org/10.33633/jais.v2i1.1330
[22] M. M. Mohamed, S. Ghoniemy, and N. I. Ghali, "A Survey on Image Data Hiding Techniques," *International Journal of Intelligent Computing and Information Sciences*, vol. 22, no. 3, pp. 14–38, 2022.
[23] Y. Bhavani, P. Kamakshi, E. Kavya Sri, and Y. Sindhu Sai, "A Survey on Image Steganography Techniques Using Least Significant Bit," *Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2021*, Springer, pp. 281–290, 2022. https://doi.org/10.1007/978-981-16-7610-9_20
[24] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021. https://doi.org/10.1109/ACCESS.2021.3053998
[25] B. Lakshmi Sirisha and B. Chandra Mohan, "Review on Spatial Domain Image Steganography Techniques," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 6, pp. 1873–1883, 2021. https://doi.org/10.1080/09720529.2021.1962025
[26] S. Kaur, S. Singh, M. Kaur, and H.-N. Lee, "A Systematic Review of Computational Image Steganography Approaches," *Archives of Computational Methods in Engineering*, vol. 29, no. 7, pp. 4775–4797, 2022. https://doi.org/10.1007/s11831-022-09749-0
[27] A. M. Adeshina, S. F. A. Razak, S. Yogarayan, and M. S. Sayeed, "Hardware-Accelerated Least Significant Bit Framework: A Low Cost Approach to Securing Clinical Data," *Informatica*, vol. 48, no. 22, 2024. https://doi.org/10.31449/inf.v48i22.5583
[28] A. Hutabarat and R. Sawitri, "Text Data Embedding into Images Using Chaotic Least Significant Bit Encod-ing Steganography," *Jurnal Pepadun*, vol. 5, no. 3, pp. 286–298, 2024. https://doi.org/10.23960/pepadun.v5i3.246
[29] A. Hildayanti and M. S. Machrizzandi, "Image Optimization Technique using Local Binary Pattern and Multilayer Perceptron Classification to Identify Potassium Deficiency in Cacao Plants Through Leaf Images," *Vokasi Unesa Bulletin Of Engineering, Technology and Applied Science*, vol. 2, no. 1, pp. 77–87, 2025. https://doi.org/10.26740/vubeta.v2i1.34587
[30] S. Arivazhagan, W. S. L. Jebarani, S. T. Veena, and E. Amrutha, "Extraction of Secrets from LSB Stego Images Using Various Denoising Methods," *International Journal of Information Technology*, vol. 15, no. 4, pp. 2107–2121, 2023. https://doi.org/10.1007/s41870-023-01265-z
[31] F. N. Hakim and M. Sholikhan, "Enhancing Data Security through Digital Image Steganography: An Implementation of the Two Least Significant Bits (2LSB) Method," *International Journal of Graphic Design*, vol. 2, no. 2, pp. 222–235, 2024. https://doi.org/10.51903/ijgd.v2i2.2124
[32] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, "A Review on Text Steganography Techniques," *Mathematics*, vol. 9, no. 21, p. 2829, 2021. https://doi.org/10.3390/math9212829
[33] I. Q. Abduljaleel, Z. A. Abduljabbar, M. A. Al Sibahee, M. J. J. Ghrabat, J. Ma, and V. O. Nyangaresi, "A Lightweight Hybrid Scheme For Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques," *Journal of Sensor and Actuator Networks*, vol. 11, no. 4, p. 66, 2022. https://doi.org/10.3390/jsan11040066
[34] K. K. Jabbar, B. T. Munthir, and S. A. Thajeel, "Digital Watermarking by Utilizing the Properties of Self-Organization Map Based on Least Significant Bit and Most Significant Bit," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 6, pp. 6545–6558, 2022. https://doi.org/10.11591/ijece.v12i6.pp6545-6558
[35] Q. Zhang, Z. Xu, Z. Yang, Z. Ren, S. Yuan, and J. Cheng, "Enhancing Visual Place Recognition using Discrete

Cosine Transform and Difference-Based Descriptors," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 71, no. 7, pp. 3368–3372, 2024. https://doi.org/10.1109/TCSII.2024.3358982
[36] A. O. Modupe, A. E. Adedoyin, A. O. Titilayo, and F. O. Deborah, "A Comparative Analysis of LSB, MSB and PVD Based Image Steganography," *International Journal of Research and Review*, vol. 8, no. 9, pp. 373–377, 2021. https://doi.org/10.52403/ijrr.20210948
[37] E. M. Jamel, "Image Steganography Based on Wavelet Transform and Histogram Modification," *Ibn AL-Haitham Journal for Pure and Applied Sciences*, vol. 33, no. 1, pp. 173–186, 2020. https://doi.org/10.30526/33.1.2365
[38] W. Alexan, M. El Beheiry, and O. Gamal–Eldin, "A Comparative Study Among Different Mathematical Sequences In 3d Image Steganography," *International Journal of Computing and Digital Systems*, vol. 9, no. 4, pp. 545–552, 2020. https://doi.org/10.12785/ijcds/090403
[39] R. Huang, C. Lian, Z. Dai, Z. Li, and Z. Ma, "A Novel Hybrid Image Synthesis-Mapping Framework for Steganography without Embedding," *IEEE Access*, vol. 11, pp. 113176–113188, 2023. https://doi.org/10.12785/ijcds/090403
[40] S. Dhar and A. K. Sahu, "Digital to Quantum Watermarking: A Journey from Past to Present and Into the Future," *Computer Science Review*, vol. 54, p. 100679, 2024. https://doi.org/10.1016/j.cosrev.2024.100679
[41] P. K. Dhar, A. Kaium, and T. Shimamura, "Image steganography based on Modified Lsb Substitution Method and Data Mapping," *International Journal of Computer Science and Network Security*, vol. 18, no. 3, pp. 155–160, 2018.
[42] A. A.-A. Gutub, "Pixel Indicator Technique for RGB Image Steganography," *Journal of Emerging Technologies in Web Intelligence*, vol. 2, no. 1, pp. 56–64, 2010. https://doi.org/10.4304/jetwi.2.1.56-64
[43] D. Sharma and C. Prabha, "Hybrid security of EMI using edge-based steganography and three-layered cryptography," *Applied Data Science and Smart Systems*, CRC Press, pp. 278–290, 2024. https://doi.org/10.1201/9781003471059-37
[44] G. P. C. Venkata Krishna and D. Vivekananda Reddy, "RETRACTED: Machine Learning-Enhanced Hybrid Cryptography and Image Steganography Algorithm for Securing Cloud Data," *Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology*, vol. 46, no. 2, pp. 4657–4667, 2024. https://doi.org/10.3233/JIFS-236229
[45] Z. Wang, M. Zhou, B. Liu, and T. Li, "Deep Image Steganography Using Transformer and Recursive Permutation," *Entropy*, vol. 24, no. 7, p. 878, 2022. https://doi.org/10.3390/e24070878
[46] A. Sharif, M. Mollaeefar, and M. Nazari, "A novel Method For Digital Image Steganography Based on a New Three-Dimensional Chaotic Map," *Multimedia Tools and Applications*, vol. 76, pp. 7849–7867, 2017. https://doi.org/10.1007/s11042-016-3398-y
[47] W. Zhang, D. Li, C. Ma, G. Zhai, X. Yang, and K. Ma, "Continual Learning For Blind Image Quality Assessment," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 3, pp. 2864–2878, 2022. https://doi.org/10.1109/TPAMI.2022.3178874
[48] G. Swain, "Two New Steganography Techniques Based on Quotient Value Differencing with Addition-Subtraction Logic and PVD with Modulus Function," *Optik (Stuttg).*, vol. 180, pp. 807–823, 2019. https://doi.org/10.1016/j.ijleo.2018.11.015
[49] A. Pradhan, A. K. Sahu, G. Swain, and K. R. Sekhar, "Performance Evaluation Parameters of Image Steganography Techniques," *International Conference on Research Advances in Integrated Navigation Systems (RAINS)*, pp. 1–8, 2016. https://doi.org/10.1109/RAINS.2016.7764399
[50] M. Sahu, N. Padhy, S. S. Gantayat, and A. K. Sahu, "Performance Analysis of various image Steganography Techniques," *Second International Conference on Computer Science, Engineering and Applications (ICCSEA)*, pp. 1–6, 2022. https://doi.org/10.1109/ICCSEA54677.2022.9936446

BIOGRAPHIES OF AUTHORS

Ekhlas Ghaleb Abdulkadhim is a lecturer at the College of Tourism Sciences, University of Kerbala, Kerbala, IRAQ. She received a BSc degree in Computer Sciences and Information Systems from the University of Technology in Iraq in 2006. She is received the M.S.C. from Ferdowsi University of Computer Engineering in 2018. She primarily researches in the computer systems and Software engineering. Readers may contact her at email: ekhlas.g@uokerbala.edu.iq.

Zaman Mahdi is a lecturer in Tourism Sciences at the University of Kerbala, Kerbala, Iraq. She received a BSc degree from AlMustensiriyah Engineering College (MIC) in Computer and Software Engineering, Iraq, in 2010. She is received the her M.Eng from Altinbas University (AU) in Electrical and Computer Engineering in Turkey in 2019. She is mainly researching in the computer systems and Image processing. Readers may contact her at email: zaman.m@uokerbala.edu.iq.

Muqdad Abdulraheem Hayder is a lecturer in the College of Education for Human Sciences, University of Kerbala, Kerbala, Iraq He is received the a BSc degree from the University of Technology's Department of Computer Sciences and Information System in Iraq in 2000. He is received the M.S.C. from Ferdowsy University of Computer Engineering in 2019. He is mainly researching in the computer systems and Software engineering. Readers may contact her at email: muqdad.a@uokerbala.edu.iq