



# Embedding a Robust Secret Data Using Image Steganography with Segmentation and Zigzag

Zainab A. Yakoob

Department of Computer Sciences, University of Technology, Baghdad, Iraq  
[Zainab.a.yakoob@uotechnology.edu.iq](mailto:Zainab.a.yakoob@uotechnology.edu.iq)

DOI: <https://doi.org/10.33103/uot.ijccce.25.1.6>

## HIGHLIGHTS

- Highlights could be presented by 3-5 bullets.
- points capturing the novelty of
- methods and/or results of the work.

## ARTICLE HISTORY

**Received:** 16/February/2025

**Revised:** 09/March/2025

**Accepted:** 19/March/2025

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

## Keywords:

Segmentation, Steganography,  
Least Significant Bit (LSB),  
Zigzag pattern.

## ABSTRACT

*Data breaches, illegal access, and private property theft are becoming increasingly common in today's digital era, making security and information hiding essential sensitive information not protected by traditional security methods. An attractive option is region-based segmentation techniques, which split images into discrete areas for specific data embedding. By making the entire image less susceptible to attacks. Each segmented zone is given a zigzag pattern to further boost robustness. Because of the extra complexity this adds, it becomes harder for attackers to find the hidden data. Least Significant Bit (LSB) steganography is then used to reduce visual distortion by altering the least significant bits of pixels, which makes it challenging to detect. Nevertheless, it is vulnerable to attackers that examine the image's statistical characteristics. In this paper, a range of publicly accessible images from the internet were used with one screenshot from the user's personal computer to evaluate the effectiveness of the method suggested. Peak signal-to-noise ratio (PSNR) is used as a statistic to assess how effective the suggested approach is. In order to make sure that the embedding procedure does not substantially deteriorate the visual quality, PSNR compares the stego-image's quality to the original image. The highest error rate was obtained when using the Baboon and the screenshot images, where 88,599 and 91,175 were obtained, respectively, when hiding 5 bytes of data, while we obtained 61,946 and 64,034 when hiding 2,500 bytes. Effective data are hidden without sacrificing the integrity of the image, as indicated by a high PSNR score.*

## I. INTRODUCTION

The digitalization of multiple obligations has altered everyday routine activities in communities and given individual beings greater lifestyle flexibility in the last ten years. A crucial stage of digitization is image segmentation. In practically every aspect of image processing, segmentation is essential, and different strategies have been put forth to do this. Image segmentation is the first step in many image-processing applications, which is crucial. The division of a picture into uniform or homogeneous parts is known as image segmentation, and it is based on common characteristics such as pixel position, color characteristics, pattern recognition, and feature shapes [1]. Image segmentation is considered an important part, usually in the pre-processing stage of the image. Zigzag scans can be embedded on each block after segmentation, as in jpeg compression [2]. Advances in digital communication technologies have enabled the widespread use of digital media over networks. Among the many kinds of digital media are traditional audio, picture, and video formats. More recently, 360-degree films, virtual reality (VR), and augmented reality (AR) have been among the forms of networked immersive or three-dimensional (3D) media. Managing the confidentiality, integrity, and security of digital media shared by everyone, organizations, experts, and governments is essential as it occurs across wired and wireless networks. Depending on the size of the digital media files, these resources can also be used to hide a significant enough quantity of secret data in these files so that it is hidden during transmission. [3] [4].

As this indicates, information security is now a crucial component of digital media communication systems that offer user identification, data integrity, secrecy, and non-repudiation. Information security seeks to conceal the presence of secret information and to prevent adversaries from gaining access to it. Information hiding and cryptography can help achieve these goals [3] [5]. The study of cryptography and the information security methods are centered on utilizing encryption to safeguard sensitive data by converting plaintext into ciphertext [5]. Steganography is a technique for hiding data and information. It essentially takes use of people's perceptions to make it impossible for an individual to determine whether or not information is available. The information and facts that have been covered up are not immediately noticeable like patients' sensitive data. The primary use of steganography is to cover up files within other files [6] [7]. Therefore, while cryptography focuses on hiding the visible secret data by changing its format and structure, steganography focuses on not discovering secret data and adding an extra degree of security. Steganography can also be applied to watermarking to safeguard copyrighted product ownership. Any new steganography technique's main goal is to increase capacity or security. Improving the robustness or imperceptibility increases security. Imperceptibility relies on the generated stego-object's quality to be identical to the original by not appreciably altering the cover item. Creating an algorithm that can withstand steganalysis and attacks is what defines robustness [8] [9].

In this domain, numerous algorithms and methods have been created. Certain algorithms, such as those that blend in with images, audio, or other media, rely on the specifics of the carrier, while others may be applied to several carrier types. Any number of media, including text, images, audio, video, and even network protocols, can be the carrier of the hidden data. Steganography can therefore be divided into groups based on the cover media. There are numerous techniques for steganography, including phase coding, spread spectrum coding, echo hiding, and least significant bit (LSB). The most well-known and straightforward technique is LSB, in which the cover value's LSB is used in place of the hidden data bits [10] [11].

## II. RELATED WORK

The suggested solution in [12] uses a hybrid approach to data concealing, which combines identical matching with the optimal pixel adjustment procedure (OPAP) in a hybrid fashion. Additionally, data is split into segments and images into blocks to further make the method more unnoticeable. A data segment is then inserted into an image block where it has the least impact on image quality. The

experimental findings demonstrate that the suggested algorithm produces stego images of higher quality than the current standard techniques for data concealing.

In [13] uses a method to increase the security of information hiding; an improved LSB information hiding algorithm of color images using secret keys is proposed. This algorithm combines cryptography and information hiding, increasing the visual features visible to the human eye and utilizing digital signature and encryption technology for identity authentication. Eventually, the enhanced LSB image steganography algorithm employing encryption technology outperforms the standard LSB image steganographic method, raising the level of security and getting a higher PSNR. according to the experiment and comparison of PSNR and safety.

In [14], an enhanced Least Significant Bit (eLSB) embedding approach was proposed to conceal a text message within an image file. Secret messages are encrypted twice using the updated methodology. The header information can be discovered in the initial bytes of the headline image during the initial stage of metadata production. In the second stage, an improved approach is employed to conceal the secret bits in the cover image after processing by hashing the commonly used words. Although it reduces the amount of hidden data in the cover file, implementing it requires more computing power.

In [15], it was mentioned that it is probable that each color channel will have  $k$  least significant values picked for the secret data embedding, and moreover, the image quality is inversely proportional to the  $k$  value obtained.

In [16], it discusses steganography as a machine learning technique and offers an approach to data hiding through unsupervised machine learning (clustering k-mean algorithm). This three-step method, which employs hidden data inside the cover image, works as follows: first, it uses k-means cluster to divide the image into three clusters with greater contrast; next, it selects an image or text to use ASCII code to convert to binary; and finally, It hides a bits message under the covering image employing the ordered LSB technique.. The process is then put into place after that. By employing unsupervised machine learning, the proposed system achieves its goal of securely transmitting sensitive data without the concern of a man-in-the-middle attack.

In [17], it is proposed an algorithm that uses the LSB method to generate random places and randomly hide the secret text in the image. The following phase is the concealing stage, which involves putting the random places in the QR code contents file. The extraction procedure first scans the QR code content to find where the bits of data are hidden. Following that, the LSB technique is utilized to obtain the secret text. This study took significantly longer than the others with the same level of security. In [18], the purpose is to develop a comprehensive technique for safely transferring data by combining steganography and cryptography. Information can be sent covertly using two popular techniques: cryptography and steganography. In this article, RC4 is utilized to convert plaintext to cipher, and Least Significant Bit (LSB) is employed to integrate the cipher text into the image. The processing times mean square error (MSE) and (PSNR) are used to define the findings. The stego image's acceptable quality was demonstrated by the experimental findings, and the original steganography is made more secure by merging the two methods.

In [19], a unique approach to spatial image steganography is introduced. The innovative technique preserves the dimensions and clarity of the essential image while concealing and recovering long-lost hidden information within digital images. This image gradient has been employed to create an salient image that shows the power for every pixel in the image. Higher-energy pixels stand out more and are useful for hiding data because of their little visual degradation. Using the saliency image, a cumulative maximum energy matrix is created that produces horizontal seams that intersect the maximum energy path. A stego-image with a hidden message is produced by hiding the secret information along the seams. Make sure that the hidden data in the stego-image is invisible and that

there is minimal perceived image quality reduction. The stego-image's hidden message is reconstructed using the same procedures.

### III. IMAGE SEGMENTATION AND ZIGZAG PATTERN

The process of breaking an image up into its individual parts or sections is called segmentation. The problem being solved determines how much of this subdivision is done. Image processing techniques such as block-based segmentation are used to split a picture into smaller, non-overlapping rectangular sections known as blocks. The content and structure of the image are then examined by processing each segment alone or together. Image divisions, a crucial stage in block-based segmentation, involves dividing the image into blocks of the same size. Block Coordinating: To obtain the Feature Extraction, each block is examined separately: Each block has pertinent features retrieved from it, including pixel values, texture attributes, and color features. Block-Based Segmentation has numerous benefits, including scalability, parallel processing, and simplicity [20] [21].

A component of the JPEG compression process, the zigzag scan was used to convert the  $8 \times 8$  matrix of the measurement process result into a  $1 \times 64$  vector within the framework of transformation. Starting at the upper left, the sorting index followed the path of the arrow in *Fig. 1*. until it reached the bottom right matrix. The zigzag scan with mapping approach is effective because it can reduce the period of time needed to sort the data and group the components according to quantified coefficients. The bits data can be embedded in the defined order that has been decided for the identical duration of clock movements with the amount of entries (for  $8 \times 8$  segment size, 64 pixels). [22].

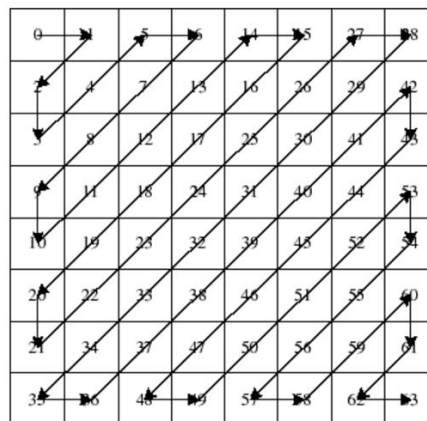


FIG. 1. ZIGZAG SCAN ON A 8X8 SEGMENT [22].

#### IV. STEGANOGRAPHY LEAST SIGNIFICANT BIT (LSB) METHOD

Steganography is becoming increasingly important as more people join the internet. Steganography is the art of concealing data using techniques that make it difficult to identify hidden characters in digital material. Steganography is a collection of secret communication techniques that prevents the letter from being seen or identified. The purpose of steganography is to remove any possibility of a hiding letter's existence [23]. The LSB method is one that is frequently applied to data embedding. It functions by substituting a different bit of secret data for the least significant bit in a byte. Each pixel in an image is made up of several tiny dots called pixels, and each pixel has three bytes, which represents RGB. These three bytes will determine the different colors of each pixel in the image, which will change the color of the entire image depending on how common each color is. For instance, the decimal RGB values for the color black are, respectively, (0, 0, 0). In contrast, the white color's decimal RGB values are (255, 255, 255). the color spectrum for a single byte will span from 0 to 255, or black to white. The least important bit-plane of a single byte cannot be changed without

noticeably altering the pixel's overall color. Thus, the least significant bit of the cover media will be replaced with the secret data bits during the embedding phase of the least significant bit approach. As can be seen, even if the LSB is altered, the pixel's overall color will stay unchanged. Thus, if the secret data is hidden in the least important area of the cover image, the eavesdroppers are unlikely to discover it [24] [25]. The final bit in the sequence of bits that has little effect on the value is known as the least-valued bit in the system of binary values. and this method uses it. The secret message bit is used to directly edit or replace the cover image's pixel values. Therefore, altering the value of this bit with the secret message bit will have minimal to no effect on the pixel value of the image. For instance, the decimal number 70 is equivalent to the binary value 1000110, has a final bit with a value of 0, which represents the LSB-bit. When this bit's value is set to 1 and an integer of 1000111 is created, the decimal value is 71. The observer notes that there is not much of an impact on value [17] [26].

## V. EVALUATION METHODS

The average MSE between the cover image's pixels and the steganography image's pixels is measured, and its value is determined using Equation (1) [19] [27].

$$MSE = \frac{1}{N} \sum_{i=1}^N (x_i - y_i)^2 \quad (1)$$

Where N refers to image size,  $x_i$  pixel from the original image and  $y_i$  corresponding pixel from the stego-image.

PSNR and MSE are two objective quality metrics, are used to assess the performance of the proposed schema. The steganography media's quality is determined using PSNR. One measure to assess the distortion (deformation) of steganography media is PSNR. The concealed information within the cover medium is undetectable to the human eye or ear if the PSNR value is higher than 30, and its value is determined using Equation (2) [28] [29]

$$PSNR = 10 \log_{10} \frac{x^2}{MSE} \quad (2)$$

Where  $x^2$  refers to the highest color level appeared in the image.

## VI. PROPOSED WORK

In order to enable secure data transfer over insecure channels, we presented a hybrid security system in this study that combines segmentation and steganography techniques. A more thorough introduction to the suggested technique will be provided in this section. The first step is to enter the secret text and compute the secret message length in bits in order to hide each bit in one color from each pixel. Then load the stego image to hide your message; then make the dimensions of the image equal to the nearest multiple of 8. The program will compare between the image size and the message size. If the message length is larger than the image size, you should select a bigger image. If the image size is larger than the message size, the program will convert the entire message to a binary vector and then segment the image into blocks. Each block has a size of 8\*8, which contains 64 pixels. Each pixel is represented by three bytes, each byte representing the intensity of the three primary colors, red, green, and blue (RGB), respectively. After that, each block converted it into a vector with a size 64 using a zigzag scan, as in *Fig. 1*. where each value represents a pixel. In this paper, we used only one color from these three, then converted it to binary and got the last bit, which represents the LSB. Take a bit at a time from the message binary vector and replace it with that LSB; that way, hiding 8 byte means 8 letters in each block, then drawing that block in the stego-image, etc. The length of the message in bytes must be known by the receiver in order to now end the extraction, so the secret message length will be hidden in a specific pixel that must be known by the receiver. Finally save the



stego-image and send it to the receiver. Fig. 2. shows a block diagram of the proposed system for hiding the secret message.

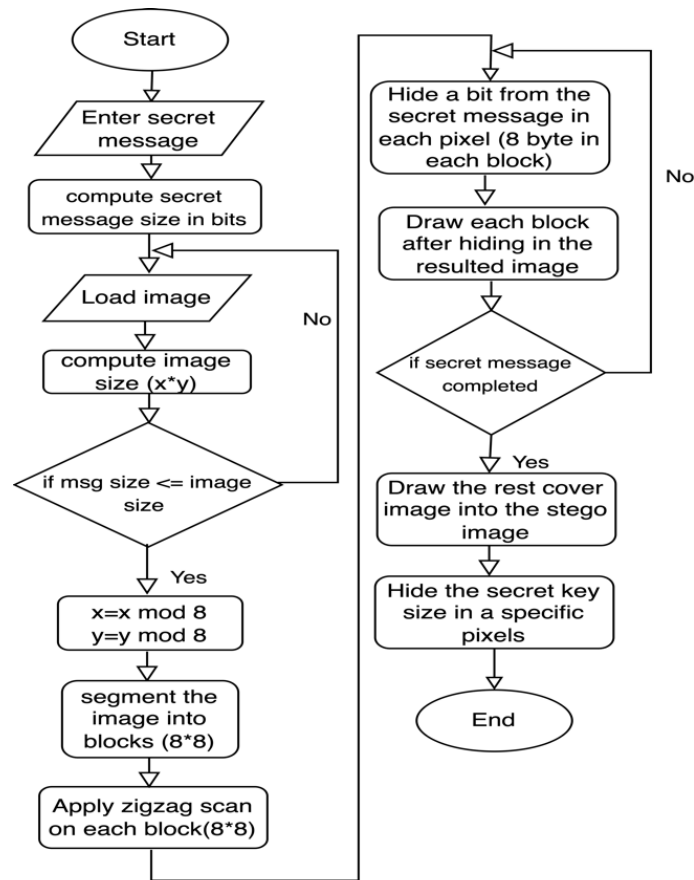


FIG. 2. A BLOCK DIAGRAM OF THE PROPOSED SYSTEM FOR HIDING.

On the other end, the receiver extracts the message by loading the stego-image and then obtains the secret message size from the location previously agreed upon with the sender. then adjust height and width to the closest multiple of 8. then segment the stego-image into 8\*8 blocks. the system converts each block into a vector by applying the zigzag scan. Each value represents a pixel with RGB values. The receiver agreed with the sender in which color hides the message, so get the color value, then convert it to the binary value and get the last bit from it. Repeat this process with each pixel, and after that combine each 8-bit together and convert each of them into its specific letter, finally display the secret message to the receiver. Fig. 3. displays the suggested system's block diagram for obtaining the secret message. When hiding in the image, one of the three colors is taken, or two or three colors are possible to hide inside it, but the type of image taken must be taken into account, as if the image is colored, there is no problem, but if the image is gray, then one color must be taken, as the values of the three colors are the same value, and any change, for example, in the red color will cause a difference in the other two colors, and it will become very clear that there is hiding inside the image. In one case, this problem can be solved, which is to hide the same bit in any color with a change in the other two colors so that it is not easily detected, and when extracting the message, it is easy to extract it from any of the colors.

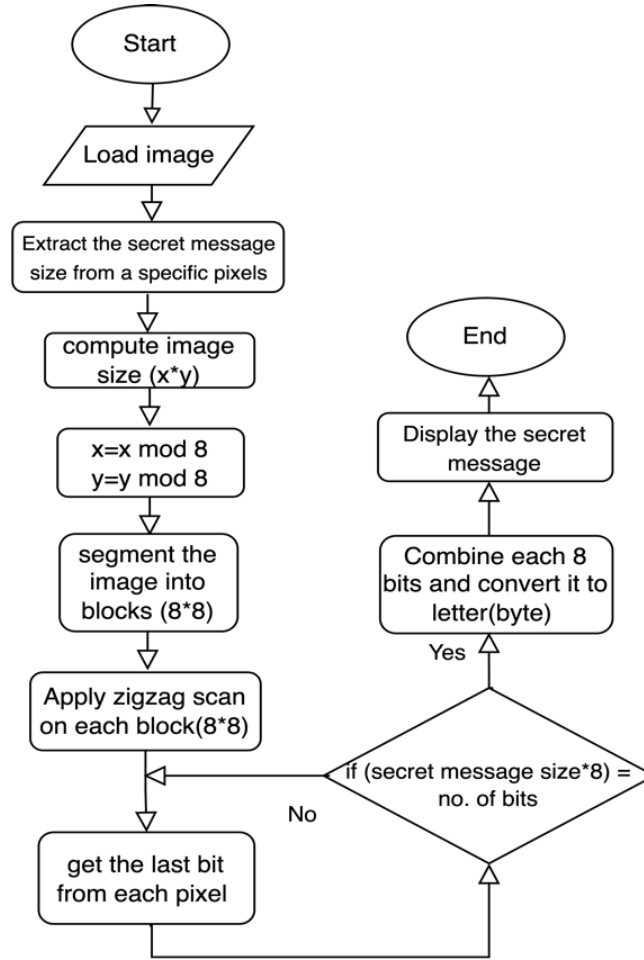


FIG. 3. A BLOCK DIAGRAM OF THE PROPOSED SYSTEM FOR EXTRACTING.

## VII. EXPERIMENTAL RESULTS AND DISCUSSION

The system was tested on various images, some of which are well-known on the Internet, such as Lina's image, which is useful in comparing the results with other research and other images with different sizes and colors as shown in Table I. The system applied to images with varying secret message sizes, hiding in each pixel a single bit. Additionally, we segmented the image using region-based into  $8 \times 8$ , applied the zigzag scan, selected one of the three colors, hid a bit with it, and compared the differences in MSE and PSNR between the two ways. It was noted that the MSE and PSNR vary by very small percentages and the time taken for hiding by only one bit is less than using the segmentation and applying the zigzag scan, but as for security, the zigzag method is definitely more difficult to retrieve the original secret message, especially since the length of the text is hidden in a distributed manner over more than one pixel according to a previous agreement between the sender and the receiver. The stego-images with their size shown in Table I have a result of hiding 5, 300, and 2500-byte message lengths using LSB only. Table II shows the result of hiding different secret message lengths using segmentation and zigzag scanning using the same original image.

TABLE I. TEST IMAGES WITH ITS SIZE AND RESULTS OF HIDING BY LSB





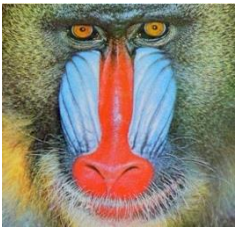
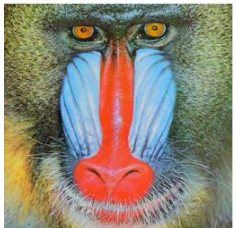











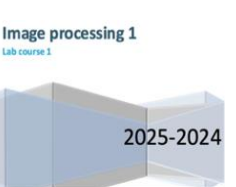

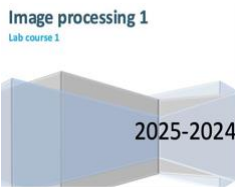




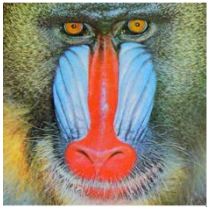
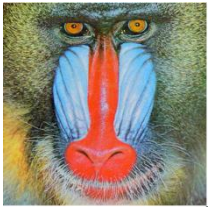
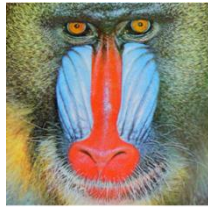
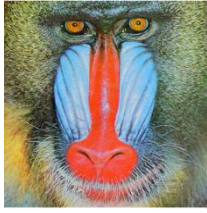








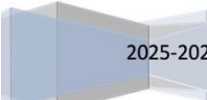
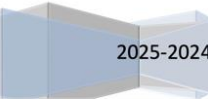
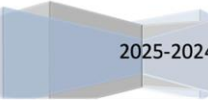
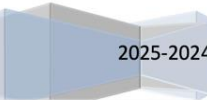
Image Number And Size	Original Image	Hide 5 Byte	Hide 300 Byte	Hide 2500 Byte
(1) Lena 225*224				
(2) Baboon 499*499				
(3) light house 6554×8192				
(4) seven color 178×177				
(5) screen shot 769×531				



TABLE II. HIDING RESULTS USING SEGMENTATION AND ZIGZAG SCANNING

Hide 5 byte	Hide 300 byte	Hide 1500 byte	Hide 2500 byte
			
			
			
			
Image processing 1 <small>Lab course 1</small> 	Image processing 1 <small>Lab course 1</small> 	Image processing 1 <small>Lab course 1</small> 	Image processing 1 <small>Lab course 1</small> 

The system computes the time consumed during converting the secret messages in different lengths (5, 16, 200, 300, 1500, and 2500). These messages were written using different letters, numbers, and special characters, and it was noted that there is no difference, as each letter, number, or special characters was represented by one byte, as shown in *Fig. 4*. The time for the hiding process and extracting process with different message lengths using only LSB and segmentation with a zigzag scan are applying to different images. The time taken to hide and recover the hide varies according to some factors, for example, the size of the text to be hidden, and of course the larger the text, the longer the time taken to hide. Also, the type of image and its resolution affect the time taken, especially if the

message is large and the image resolution is high; it will take more time than other images; an example of this is the image of the lighthouse. The results are registered and are shown in Fig. (5, 6, 7, 8 and 9).

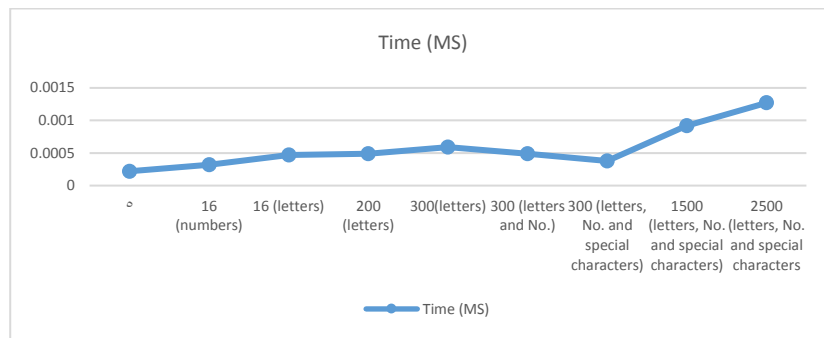
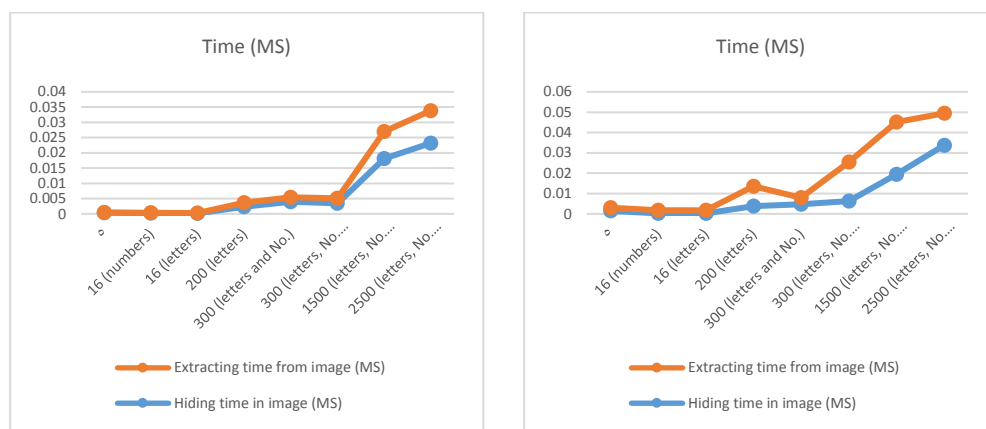


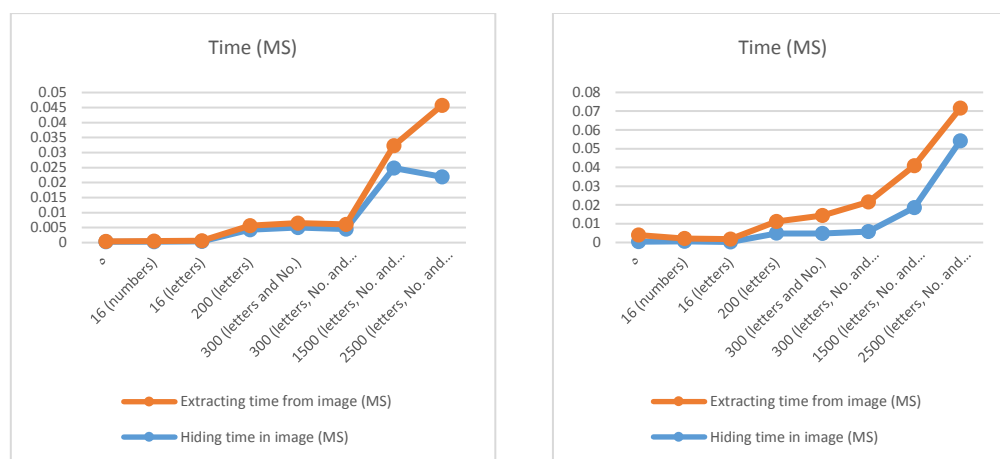
FIG. 4. TIME EXECUTION FOR CONVERTING MESSAGE TO BINARY IN DIFFERENT LENGTHS.



using LSB

using zigzag

FIG. 5. TIME EXECUTION FOR HIDING AND EXTRACTING THE SECRET MESSAGE FROM LENA IMAGE IN DIFFERENT LENGTHS.



using LSB

using zigzag

FIG. 6. TIME EXECUTION FOR HIDING AND EXTRACTING THE SECRET MESSAGE FROM BABOON IMAGE IN DIFFERENT LENGTHS.

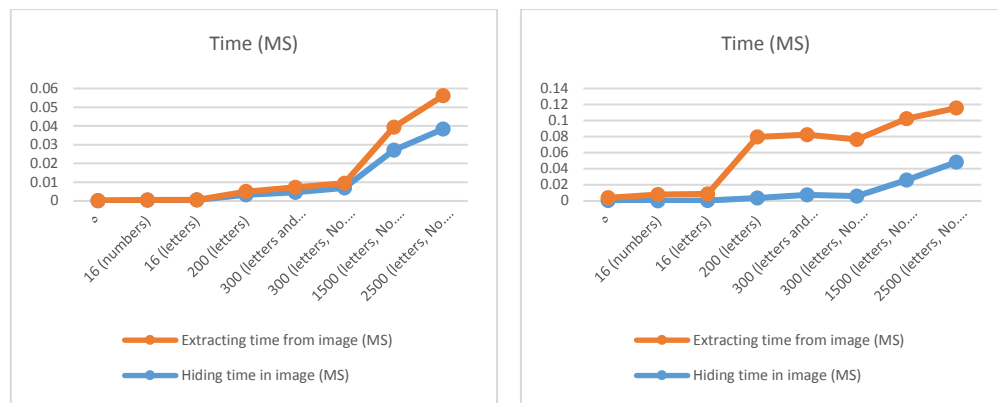


FIG. 7. TIME EXECUTION FOR HIDING AND EXTRACTING THE SECRET MESSAGE FROM LIGHT HOUSE IMAGE IN DIFFERENT LENGTHS.

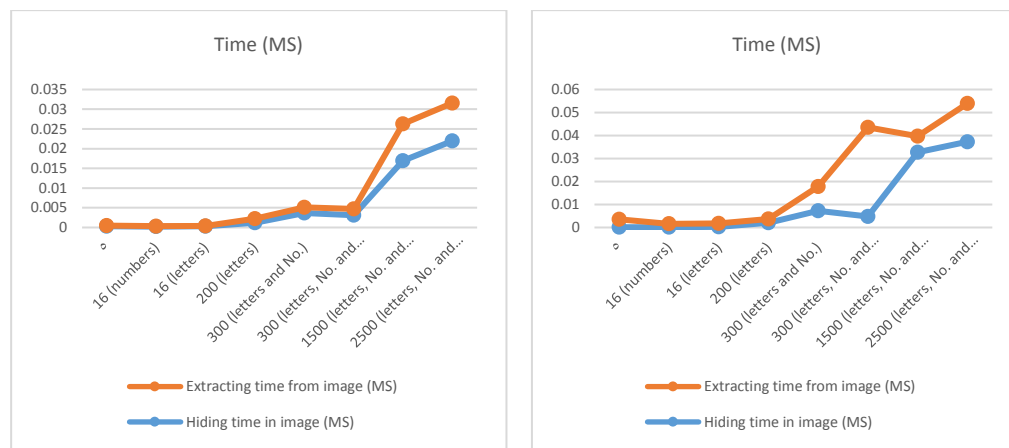


FIG. 8. TIME EXECUTION FOR HIDING AND EXTRACTING THE SECRET MESSAGE FROM SEVEN COLOR IMAGE IN DIFFERENT LENGTHS.

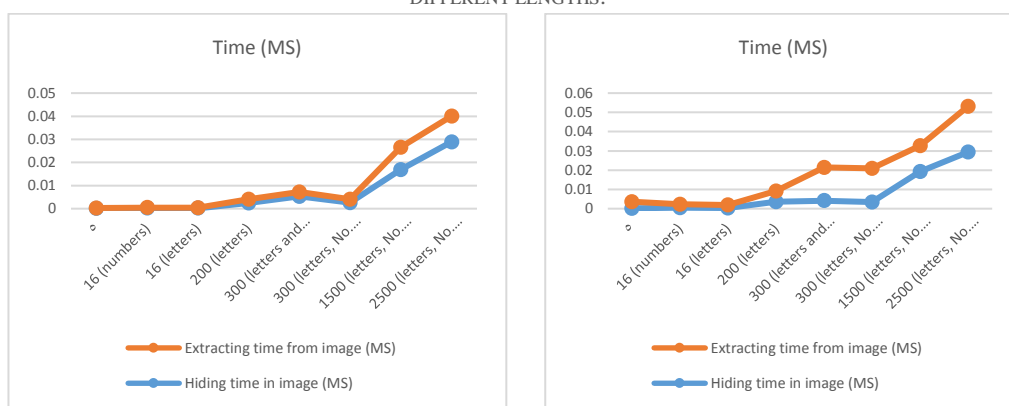


FIG. 9. TIME EXECUTION FOR HIDING AND EXTRACTING THE SECRET MESSAGE FROM SCREEN SHOT IMAGE IN DIFFERENT LENGTHS.

The system was evaluated using MSE, and PSNR was calculated in several cases in terms of the difference in the length of the hidden secret messages and the used hiding method and it's compared

with the results of related work as in Table III. Five different images were used, and the results are fixed in Tables IV and V. It was noted that the MSE and PSNR are sometimes near to equal, especially if the length of the secret message to be hidden is short, because in the case of hiding by the LSB or by the segmentation with zigzag method, the hiding locations will be so close. This is normal because the hiding locations differ when using segmentation from what we use when using LSB only, where the image is divided into several blocks, and here the locations of the original image will differ from the LSB once to what it was in the segmentation again. When comparing the original image with the stego image, each pixel with the corresponding hiding one was different in each hidden method in the proposed work, so MSE found it different each time from each method even if the same message was hidden. The lower the MSE, the higher the PSNR, and therefore the relationship between them is inverse. The suggested technology has real-world applications such as encrypted interaction, electronic watermarking, and medical imaging secrecy. Limitations may include sensitivity for sophisticated steganalysis strategies, computational complexity in huge images size, and deformations that influence extraction accuracy.

TABLE III. COMPARISON WITH PREVIOUS WORKS

Ref.	eMSE	ePSNR
[12] use Lena (color)	4 blocks=0.0134 8 blocks=0.0119 16 blocks=0.0071	4 blocks=66.8678 8 blocks=67.3747 16 blocks=69.6335
[13] use Lena (gray)	-	56.513
[14] use Lena (color)	0.00245	12.6619
[15] use Lena (color)	-	32.490
[16] hide SecretMessage 170 bytes	0.0636	29.3015
[17] use Lena (color)	-	48.7
[18] use Lena (color)	0.00011	87.716
[19] use Lena (gray)	0.0060	70.3505
Proposed work	Table V, VI	Table V, VI

TABLE IV. PROPOSED WORK RESULTS WITH 5 AND 300 MSG LENGTH USING LSB AND LSB WITH ZIGZAG

Picture	LSB (msg length=5)		LSB with zigzag (msg length=5)		LSB (msg length=300)		LSB with zigzag (msg length=300)	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
lena	0.001	81.989	0.001	81.989	0.022	64.16	0.024	64.086
Baboon	0.005	88.599	0.004	88.406	0.005	71.199	0.005	71.149
Light house	0.001	78.7	0.001	79.095	0.005	61.602	0.044	61.657
Seven color	0.001	87.897	0.002	87.897	0.039	68.487	0.037	68.706
Screen shot	0.001	91.175	0.001	91.175	0.002	0.003	73.036	0.003

TABLE V. PROPOSED WORK RESULTS WITH 1500 AND 2500 MSG LENGTH USING LSB AND LSB WITH ZIGZAG

Picture	LSB (msg length=1500)		LSB with zigzag (msg length=1500)		LSB (msg length=2500)		LSB with zigzag (msg length=2500)	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
lena	0.124	57.188	0.121	57.299	0.204	55.036	0.202	55.067
Baboon	0.024	64.254	0.024	64.239	0.041	62.031	0.042	61.946
Light house	0.226	54.586	0.228	54.555	0.377	52.366	0.374	52.406
Seven color	0.204	60.534	0.196	60.719	0.325	58.319	0.327	58.29
Screen shot	0.016	66.101	0.015	66.253	0.026	63.971	0.026	64.034

## VIII. CONCLUSION

This paper has different points to conclude because it uses various message lengths, different images, and different methods. Furthermore, when images with hidden messages were shared online using applications like Viber or WhatsApp, the compression methods used by those applications may have damaged the hidden data. In order to address this problem, WinRAR was used to compress the image sending. During transmission, this method guaranteed the integrity of the hidden data. Power of Message Length As may be assumed; a longer message usually results in a lower PSNR. This is because the image pixels must go through more substantial alterations as a result of the necessity to include more bits. Complexity of Images The zigzag pattern's effect appears to change according on how complicated the image is. The PSNR improvement brought about by the zigzag pattern is more noticeable for photos with complicated patterns (such as "Baboon," "Lighthouse"). The Impact of the Zigzag Pattern For all image sizes and message lengths, the zigzag pattern continuously raises the PSNR values when compared to the conventional LSB approach. This suggests that localized distortion is decreased by the zigzag pattern's efficient distribution of the hidden data throughout the image. The results of the research show how successful the suggested steganographic method, which pairs LSB steganography, zigzag pattern embedding, and image segmentation, is. By more equally dispersing the hidden data throughout the image, the zigzag pattern greatly increases the method's robustness while improving visual quality and lowering detectability. The results of comparing the suggested technique's image quality to those of other comparable LSB algorithms demonstrate how much better our method is than the others in terms of PSNR and embedding capacity.

## REFERENCES

- [1] G. Raghuwanshi, Y. Gupta, D. Sinwar, D. Singh, U. Tariq, M. Attique, K. Pin and Y. Nam, "Image Segmentation Based on Block Level and Hybrid Directional Local Extrema," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 3939-3954, 2022. DOI: 10.32604/Cmc.2022.018423.
- [2] W. Xiao, N. Wan, A. Hong a. X. Chen, "A Fast JPEG Image Compression Algorithm Based on DCT," in *IEEE International Conference on Smart Cloud (SmartCloud)*, Sweden, 2020. DOI: 10.1109/Smartcloud49737.2020.00028.
- [3] D. N. Tran, H.-J. Zepernick a. T. M. C. Chu, "Review of LSB Data Hiding in Digital Media : A Survey," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 22, no. 30, pp. 1-50, 2022. <https://doi.org/10.4108/Eai.5-4-2022.173783>.
- [4] A. K. Sahu, G. Swain, "High fidelity based reversible data hiding using modified LSB matching and pixel difference," *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 4, pp. 1395-1409, 2022. <https://doi.org/10.1016/j.jksuci.2019.07.004>.
- [5] M. Tarawneh, *Cryptography:Recent Advancesand Research Perspectives*, USA: (IntechOpen), 2023. DOI:10.5772/intechopen.111847.
- [6] S., R. Sindhu a. Pragati, "Information Hiding using Steganography," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 4, pp. 1549-1554, 2020. DOI: 10.35940/ijeat.D8760.049420.
- [7] Y. A. Khaleel, "High Security and Capacity of Image Steganography for Hiding Human Speech Based on Spatial and Cepstral Domains," *ARO-The Scientific Journal of Koya University*, vol. 8, no. 1, pp. 95-106, 2020. <https://doi.org/10.14500/aro.10670>.
- [8] T. Barhoom, W. Saqer a. Tawfiq, "Steganography and Hiding Data with Indicators-based LSB Using a Secret Key," *Engineering, Technology & Applied Science Research*, vol. 6, no. 3, pp. 1013-1017, 2016. <https://doi.org/10.48084/Etasr.649>.
- [9] Mula, M. Sasmal a. Debasmita, "An Enhanced Method for Information Hiding Using LSB Steganography," in *Journal of Physics, India*, 2021. DOI:10.1088/1742-6596/1797/1/012015.
- [10] E. W. Abood, A. M. Abdullah, M. A. Al Sibahee, Z. A. Abduljabbar, V. O. Nyangaresi, S. A. A. Kalafy a. M. J. J. Ghrabta, "Audio steganography with enhanced LSB method for securing encrypted text with bit cycling," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, pp. 185-194, 2022. DOI: <https://doi.org/10.11591/Eei.V11i1.3279>.



- [11] H. S. El-sayed, S. F. El-Zoghdy and O. S. Faragallah, "Adaptive Difference Expansion-Based Reversible Data Hiding Scheme for Digital Images," *Arabian Journal for Science and Engineering*, vol. 41, no. 3, p. 1091–1107, 2016. DOI: 10.1007/S13369-015-1956-7.
- [12] Kaur, G. Navdeep a. Swarnjeet, "Segmentation and Block Based Image Steganography using Optimal Pixel Adjustment Process and Identical Approach," in *RAECS VIET Panjab University Chandigarh, Afghanistan*, 2015. DOI: 10.1109/RAECS.2015.7453372.
- [13] X. Zhou, W. Gong, W. Fu and L. J. Jin, "An improved method for LSB based color image steganography combined with cryptography," in *IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*, Okayama, Japan, 2016. DOI: 10.1109/ICIS.2016.7550955.
- [14] J. Raj Jayapandiyan, C. Kavitha A. K. Sakthivel, "Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization," *IEEE access*, vol. 8, pp. 136537-136545, 2020. DOI: 10.1109/ACCESS.2020.3009234.
- [15] O. Elharrouss, N. Almaadeed, a. S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," in *IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIOT)*, Doha, Qatar, 2020. DOI: 10.1109/Iciot48696.2020.9089566.
- [16] H. H. Hassan, M. A. A. Khodher, "Data Hiding by Unsupervised Machine Learning Using Clustering K-mean Technique," *Iraqi Journal of Computers, Communications, Control & Systems Engineering (IJCCCE)*, vol. 11, no. 4, pp. 37-49, 2021. <https://doi.org/10.33103/Uot.Ijccce.21.4.4>.
- [17] H. S. Wdhayeh, R. A. Azeez, A. J. Mohammed, "A Proposed Algorithm for Hiding a Text in an Image Using QR Code," *Iraqi Journal of Computers, Communications, Control & Systems Engineering (IJCCCE)*, vol. 23, no. 1, pp. 1 - 9, 2023. <https://doi.org/10.33103/Uot.Ijccce.23.1.1>.
- [18] M. M. A. Zaid, A. A. T. Al-Khazaali a. A. A. Mohammed, "LSB Steganography using Dual Layer for Text Cryptostego," in *BIO Web of Conferences*, Iraq, 2024. <https://doi.org/10.1051/Bioconf/20249700069>.
- [19] R. Shmueli, D. Mishra, T. Shmueli a. O. Hadar, "A novel technique for image steganography based on maximum energy seam," *Multimedia Tools and Applications*, vol. 83, p. 70907–70920, 2024. <https://doi.org/10.1007/S11042-024-18476-6>.
- [20] J. Aqel, N. M. Zaitouna a. Musbah, "Survey on Image Segmentation Techniques," in *International Conference on Communication, Management and Information Technology*, Jordan, 2015. <https://doi.org/10.1016/J.Procs.2015.09.027>.
- [21] M. Hassan, S. Sharmeen, A. Rahman, M. A. Ali, H. Kabir, "Block Based Image Segmentation.," in *Advances in Communication, Network, and Computing*, Berlin, Heidelberg, 2012. [https://doi.org/10.1007/978-3-642-35615-5\\_3](https://doi.org/10.1007/978-3-642-35615-5_3).
- [22] R. Candra, S. Madenda, S. A. Sudiro a. M. Subali, "The implementation of an efficient Zigzag scan," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 9, no. 2, pp. 95-98, 2017. <https://doi.org/10.1016/J.Jksuci.2018.01.011>.
- [23] A. K. Hammoud, H. N. Mohaisen. M. Q. Mohammed., "Secret information hiding in image randomly method using steganography and cryptography," *Int. J. Nonlinear Anal. Appl.*, vol. 12, no. Special Issue, pp. 1283-1291, 2021. 10.22075/IJNAA.2021.5644.
- [24] M. A. Pirdawood, S. R. Kareem a. O. Al-Rassam, "Encryption of Color Images with a New Framework: Implementation Using Elzaki Transformation," *ARO-The Scientific Journal of Koya University*, vol. 7, no. 1, pp. 170-180, 2024. <https://doi.org/10.14500/aro.11618>.
- [25] Obaid, A. S. Taleb, "Embedding Secret Data in Color Image Using LSB," *Journal of Education for Pure Science-University of Thi-Qar*, vol. 12, no. 2, pp. 196-206, 2022. <https://doi.org/10.32792/jeps.v12i2.191>.
- [26] D. Darwis, A. Junaidi, D. A. Shofiana a. Wamiliana, "A New Digital Image Steganography Based on Center Embedded Pixel Positioning," *CYBERNETICS AND INFORMATION TECHNOLOGIES*, vol. 21, no. 2, pp. 89-104, 2024. DOI:10.2478/cait-2021-0021.
- [27] P. Maniriho, T. Ahmad, "Information hiding scheme for digital images using difference expansion and modulus function," *Journal of King Saud University – Computer and Information Sciences*, vol. 31, pp. 335-347, 2019. <https://doi.org/10.1016/J.Jksuci.2018.01.011>.
- [28] H. M. Vijayalaxmi, A. S. Rao, A. M. Khan, D. Kotyan, D. Disha, R. Pratheeksha a. C. Rao, "A study on secured encryption of medical images using significant visual cryptography," *Engineering Research Express*, vol. 6, no. 2, 2024. DOI 10.1088/2631-8695/Ad3dad.

- [29] Z. N. Sultani a. B. N. Dhannoon, "Image and audio steganography based on indirect LSB," Kuwait J.Sci., vol. 48, no. 4, pp. 1-12, 2021. DOI:10.48129/kjs.v48i4.8992.