Tikrit Journal of Pure Science Vol. 30 (4) 2025

DOI: https://doi.org/10.25130/tjps.v30i4.1945

IRAQI Academic Scientific Journals

Tikrit Journal of Pure Science

ISSN: 1813 – 1662 (Print) --- E-ISSN: 2415 – 1726 (Online)

Journal Homepage: https://tjpsj.org/

Tikrit Journal of Pure Science

A New Robust Data Hiding Method in Digital Image based on Pelican Optimization Algorithm

Ebtehal Talib

Ministry of Higher Education and Scientific Research, Baghdad, Iraq

Received: 17 Mar. 2025 **Received in revised forum:** 7 Jun. 2025 **Accepted:** 11 Jun. 2025

Final Proof Reading: 12 Aug. 2025 **Available oonline:** 25 Aug. 2025

ABSTRACT

Sharing and exchanging data over networks is often insecure, especially if the data is secret and important. Steganography is key research fields in information hiding, focusing on invisible communication and digital steganography, which offers private, secure communication through multimedia carriers. In this paper, propose a new steganography approach for hiding data in digital images using Pelican Optimization Algorithm (POA) and Least Significant Bit (LSB). The digital image was first divided into (4*4) blocks, then determined the best blocks for data hiding using POA, after that used LSB for data hiding. The results (MSE and PSNR are 0.7838 and 49.1743 respectively) are good when compared with related works and show good image quality.

Keywords: Steganography, Data Hiding, Digital Image, Pelican Optimization Algorithm (POA), Least Significant Bit (LSB).

Name: **Ebtehal Talib** **E-mail:** **talibebtehal@gmail.com**

Tikrit Journal of Pure Science Vol. 30 (4) 2025
DOI: https://doi.org/10.25130/tjps.v30i4.1945

طريقة قوية وجديدة لإخفاء البيانات بالاعتماد على خوارزمية تحسين البجع

ابتهال طالب

وزارة التعليم العالي والبحث العلمي، بغداد، العراق

الملخص

غالبًا ما يكون تبادل البيانات ومشاركتها عبر الشبكات غير آمن، خاصةً إذا كانت البيانات سرية ومهمة. يعد اخفاء المعلومات من المجالات البحثية الرئيسية، مع التركيز على الاتصالات غير المرئية والتخفي الرقمي، الذي يوفر اتصالات خاصة وآمنة من خلال حاملات الوسائط المتعددة. في هذه الورقة، نقترح نهجًا جديدًا لإخفاء البيانات في الصور الرقمية باستخدام خوارزمية تحسين البجع (POA) البت الاقل أهمية (LSB). تم تقسيم الصورة الرقمية أولاً إلى (4*4) كتل، ثم تحديد أفضل الكتل لإخفاء البيانات باستخدام خوارزمية البجع (POA)، وبعد ذلك تم استخدام أقل بت أهمية لإخفاء البيانات. النتائج (MSE و PSNR هي 0.7838 و 49.1743 على التوالي) جيدة عند مقارنتها بالأعمال السابقة وتظهر جودة صورة جيدة.

INTRODUCTION

In the contemporary world, communication is essential. Information is sent over many data channels during communication. There could be major security issues with this method. This has led to a greater focus on finding methods to safeguar1d sensitive data while it is being transmitted. A number of techniques have been put forth to encrypt and decrypt data, guaranteeing message secrecy [(1)]. Cryptography is a technique used to assure communication secrecy. But sometimes it is not enough to keep the contents of message secret, which is why cipher text is used. Although cipher text is easily detected, it alerts others when communication channels are being watched [(2)].

Thus, over the past 20 years, lot of research has been done on the delivery of secret messages through the exchange of plaintext. Message secrecy must be maintained, and steganography makes this possible [(3)]. Whereas cryptography is encrypting data with a key and transmitting it via a particular channel, steganography includes hiding data such that it doesn't appear to be hidden. A user or process is able to watch the communication process, but without the key, they are unable to take the pertinent data. When secret information is transmitted using steganography, neither the person nor the process is aware of it. Consequently, no effort is taken to obtain information [(4)].

This paper uses a new method based on Pelican Optimization Algorithm (POA) and Least Significant Bit (LSB) to hide data in host images. this scheme has optimized the result to get a tradeoff between robustness and imperceptibility. The organization of this paper is as follows: the paper explains the Pelican Optimization Algorithm in section 2 and the Least Significant Bit in section 3. The related work is explained in section 4. The proposed data hiding method is explained in section 5. Performance evaluation metrics used to evaluate the proposed method explained in section 6, then the results and discussion are explained in Section 7. Finally, the conclusion is shown in section 8.

PELICAN OPTIMIZATION ALGORITHM (POA)

The Pelican Optimization Algorithm (POA) is a nature-inspired Swarm intelligence technique as

show in figure (1), the pelican, a large bird with a strong mouth and wide neck pouch, prefers social interaction and group living. They hunt by diving from 10-20 meters, reaching shallow waters, and extending their wings to remove excess water. They swallow the fish to remove excess water[5].

The pelican optimization mathematical model based on two parts: the first part is initialization of the population: in every pelican in the population represents a potential fix for the optimization issue [6]. They start out in the search space at random locations within predetermined ranges. The second part is the objective function: each candidate solution's values for the objective function are assessed to see how well it addresses the given problem. In POA, the hunting process is divided into two primary stages: exploration and exploitation[7, 8].

- **Exploration Stage**: Pelicans move toward randomly selected prey spots in order to explore the search space. The algorithm's capacity to search the space for viable solutions is improved during this phase[8].
- **Exploitation Stage**: Pelicans hone their search by concentrating on nearby neighborhoods close to where they are now, hoping to get better answers by taking use of the surrounding areas[9]. Up until it finds the optimal solution, the algorithm switches back and forth between these stages, adjusting the population and objective values[9].

LEAST SIGNIFICANT BIT (LSB)

In steganography, the Least Significant Bit (LSB) approach is a popular way to conceal data inside an image. This method has three key points (Minimal Visual Distortion, Capacity and security). Modifying a pixel's least important bit won't drastically alter the image's appearance overall, which makes it perfect for covertly storing data [10]. The size and resolution of the image determine how much data may be buried. More info can be hidden in larger, more pixelated images. Because the hidden data is directly embedded in the pixel values of the image, the LSB approach, while easy to use and efficient for concealing small quantities of data, may be susceptible to discovery and extraction by image analysis or compression [11].

Basic steganography uses this technique frequently, especially when the intention is to covertly conceal data in digital material [12].

A set of binary integers (such as RGB values for color images, where each color component is typically 8 bits) corresponds to each pixel in digital images. The lowest bit in the binary encoding of a pixel value are the least significant bits, and changing it little affects how the image looks [11].

- **Binary Pixel Representation for Data and Image:** An image's pixels are usually represented by 8 bits each (for example, 255 in decimal is 11111111 in binary). The three color channels (Red, Green, and Blue) in image are each represented by eight bits. As an illustration:

Colors: Red: 11001011, Green: 10111010, Blue: 11101101(10).

- **Data Embedding**: the least significant bit of a pixel's color value is replaced with a bit of the secret data (0 or 1) using the LSB technique to conceal data. For instance, you can take the bits of the binary value 01000001 (the ASCII value 65) and embed them in the LSBs of the image's pixels if you wish to conceal the letter "A" from view [12].

$$\begin{bmatrix} \text{Red} & 203 & 11001011 \\ \text{Green} & 186 & 10111010 \\ \text{Blue} & 237 & 11101101 \end{bmatrix}$$

Following the insertion of a single bit of secret data (such as a 1 for "A"):

$$\begin{bmatrix} \text{Red} & \text{stays the same} & 11001011 \\ \text{Green} & \text{bit set to 1} & 10111011 \\ \text{Blue} & \text{bit set to 0 instead of 1} & 11101100 \end{bmatrix}$$

DOI: https://doi.org/10.25130/tjps.v30i4.1945

The LSB adds very little to the color value, therefore even when certain bits are altered, the total visual difference in the image is undetectable. For example, the human eye does not detect a pixel change from 237 to 236 [12].

- **Extraction Process:** The LSBs of the pixels are recovered in the same order as they were inserted in order to recover the concealed data. The concealed data is then pieced back together using these retrieved parts.

RELATED WORK

In this paper [13] suggested a unique chaos-theoretic approach for image steganography. Three chaotic sequences are produced using the suggested approach using unique 3D chaotic map (LCA map) with maximum Lyapunov exponent of 20.58. In this paper [14] presents a method of LSB-based image steganography with a secret map focus. This technique encrypts concealed data with sequentially or randomly inserted secret keys. Before being hidden in a cover image, the hidden data is dispersed at random, and the pixels of the cover of the cover image are chosen at random using the secret map as a guide. This improves the LSB-based image steganography's concealed information security. In particular, by altering RGB images' least significant bit, this paper[15] aims ti improve image data augmentation by producing new versions of preexisting images through cropping and flipping methods that retain the original image's information while producing variations for improved machine learning models. The data hiding technique for DICOM medical images presented in this paper [16] uses adversarial neural cryptography with SHA-256 for anonymity and secrecy. Using variety of medical datasets, a secure hash algorithm with 256 bits (SHA-256) is utilized to verify the legitimacy and integrity of the images.

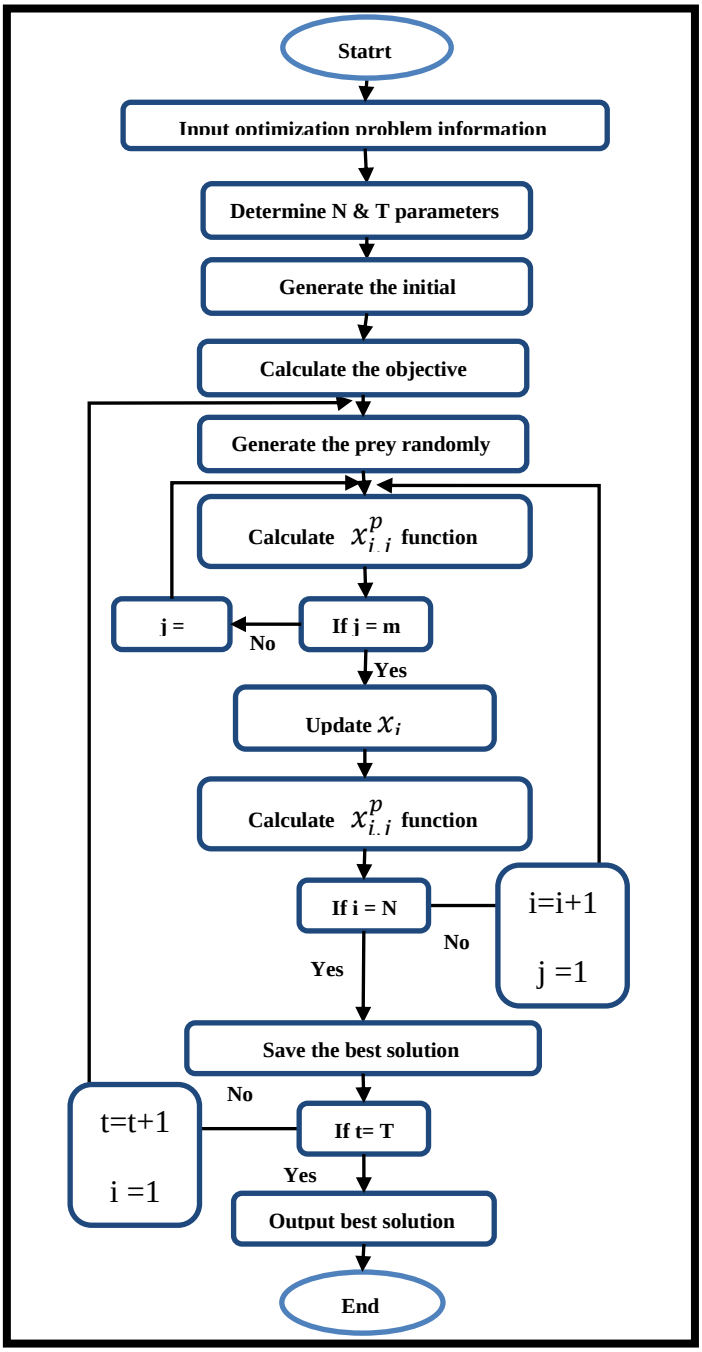

Fig. 1: Flowchart of the Pelican Optimization Diagram

THE PROPOSED METHOD

The "Hiding Process" method makes it easier to integrate the data into a host image. Finding the ideal positions to hide the data into the host image is done using the Pelican Optimization Algorithm (POA). The POA Algorithm was developed by analyzing pelican behavior and hunting strategy, drawing inspiration from the cognitive process of these birds. The proposed image at each recognized point is calculated by combining the host image and the data using Least Significant Bit (LSB) at last bit. The final image is produced by using this hiding technique iteratively to each of the chosen positions. A modified image with the hided data is explained in figure (2).

DOI: https://doi.org/10.25130/tjps.v30i4.1945

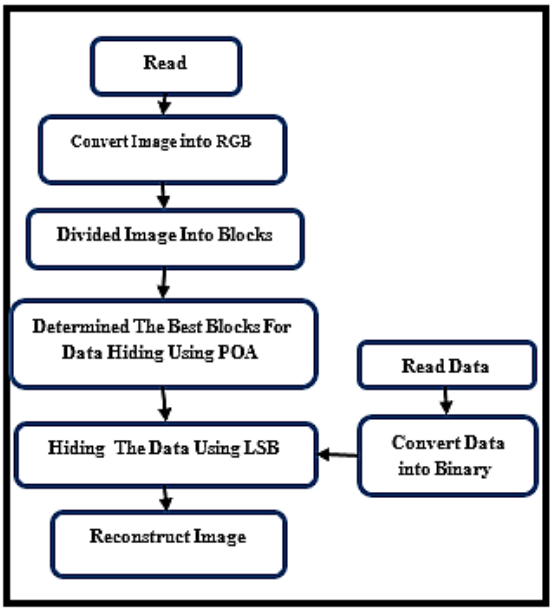

Fig. 2: Flowchart of the Proposed Data Hiding Method.

For the hidden data into the image was using Algorithm (1).

Algorithm (1): The Proposed Hiding Data Algorithm

Input: Image, Data

Output: Image with Hiding Data

Start

Step1: Read image (256×256) and convert it to RGB

Step2: Read data and convert it into binary form

Step3: Divided image into (4*4) blocks

Step4: Determine the POA population size (N) and the number of iterations (T).

Step5: Initialization of the position of pelicans and calculate the objective function using Eq.1

$$X_{i,j} = l_j + rand\,(u_j - l_j), i = 1,2,\ldots.N, j = 1,2,\ldots..M \quad \ldots\ldots (\text{Eq. } 1)$$

#Where:

#$X_{i,j}$ is the value of the variable(j[th]) specified by the candidate solution (i[th])

#N: number of population and M: problem variables

#Rand: random number in interval [0, 1],

#l_j and u_j : are lower and upper bound of problem variables.

Step6: For t = 1:T

Step7: Generate the position of the prey at random.

Step8: For I = 1:N

Step9: Stage 1: Exploration

For j = 1:m

Step10: Calculate new status of the jth dimension using Eq.2

$$X_{i,j}^{p1} = \begin{cases} X_{i,j} + rand\,(p_j - I.X_{i,j}), & F_p < F_i \\ X_{i,j} + rand\,(X_{i,j} - p_j), & else \end{cases} \quad \ldots\ldots (2)$$

End.

#Where:

$X_{i,j}^{p1}$: new status of the pelican (i[th]) in the j[th] dimension based on stage1,

I : random number (one or two),

p_j: is prey location, and F_p: value of objective function

Step11: Update the i[th] population member using Eq.3

$$X_i = \begin{cases} X_i^{p1}, & F_i^{p1} < F_i \\ X_i, & else \end{cases} \quad \ldots\ldots (3)$$

Step12: Stage 2: Exploitation

For j = 1:m.

Step13: Calculate new status of the jth dimension using Eq.4

$$X_{i,j}^{p2} = X_{i,j} + R\left(1 - \frac{t}{T}\right).(2.rand - 1).X_{i,j} \quad \ldots..(4)$$

End.

Step14: Update the i[th] population member using Eq.5

$$X_i = \begin{cases} X_i^{p2}, & F_i^{p2} < F_i \\ X_i, & else \end{cases} \quad \ldots\ldots (5)$$

End.

Step15: Update best candidate solution.

End.

Step16: Output best blocks for data hiding

Step17: For each block:

Step18: Hiding the data using LSB in tow last bits of the RGB values of the pixle.
Step19: Reconstruct Image
End
For the hidden data extraction from the image was using Algorithm (2).

Algorithm (2): The Proposed Data Extraction Algorithm
Input: Image that has the hidden data
Output: The hidden data
Start
Step 1: Read the Image (256×256) with hiding Data and convert it to RGB.
Step 2: Split the image into blocks (4×4).
Step 3: Define the population size (N) and the number of iterations (T) of POA.
Step 4: Initialize positions of the pelican and calculate the objective function using Eq.1.
Step 5: For t = 1:T
Step 6: Generate at random the prey position.
Step 7: For i = 1:N
Step 8: Stage 1: Exploration
For j = 1:M,
calculate the new status of the j^{th} dimension using Eq.2.
Update the ith population member using Eq.3.
Step 9: Stage 2: Exploitation
For j = 1:M,
calculate the new status of the j^{th} dimension using Eq.4.
Update the i^{th} population member using Eq.5.
Step 10: Update the best candidate solution.
Step 11: Detect the blocks that has the hiding data.
Step 12: For each block:
Extract the LSBs from the two least significant bits of the RGB values of each pixel.
Convert extracted bits into binary form.
Step 13: Rebuild the hidden data from binary form.
Step 14: The extracted data is the output
End

The hidden data should be strong against attacks and undetectable to preserve the image's visual quality. Lastly, the performance of the proposed method was evaluated using PSNR and MSE.

PERFORMANCE EVALUATION METRICS

The computation of the various metrics are used to assess the effectiveness of the suggested data hiding method [17, 18]. Those metrics are the Mean Square Error (MSE) and the Peak-Signal-to-Noise Ratio (PSNR) are used to calculate the similarity between the modified image with hiding data and original image in order to illustrate the visual quality of the modified image[19, 20].

Mean Square Error (MSE)

The host and the image with hiding data are denoted by (a, b) and $G'(a, b)$ respectively ,and the size of the image is represented as $(k1 \times k2)$ in Equation 6. Small MSE values means acceptable degradation [18, 21].

$$MSE = \sum\sum ((a, b) - G'(a, b))\ k2\ b{=}1\ k1\ a{=}1\ 2\ k1 \times k2 \ldots\ldots (6)$$

Peak-Signal-to-Noise Ratio (PSNR)

When it comes to data hiding, the image's quality needs to be quite good. The hiding data in the host should be perceptually invisible. In a reconstructed image, a PSNR (7) of at least 30 dB is generally regarded as adequate. Acceptable values, however, vary depending on the needs of the application [19, 22].

$$PSNR = 10 \log10\ 2552\ MSE \ldots\ldots (7)$$

RESULTS AND DISCUSSION

Several images (Lena, Peppers, and Baboon) are employed, that are popular in the image processing. these are all 256×256 in size. Additionally, comparisons with similar

algorithms from the literature are made. The first column (A,B,C) in Figure (3) displays the original image of Lena, peppers, and the baboon respectively, the second column (A,B,C) represents the image with hiding data.

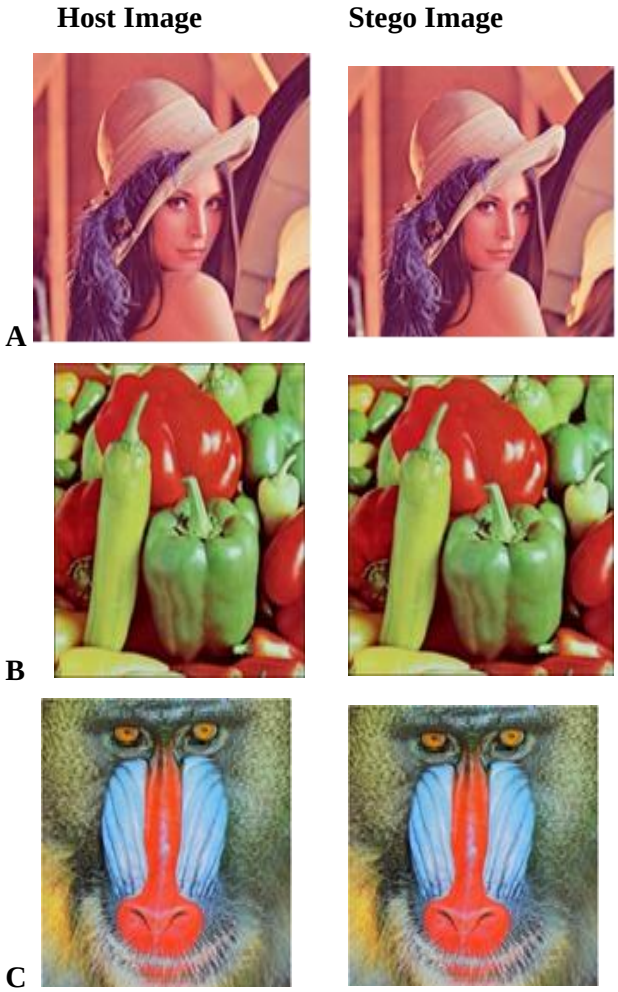

Fig. 3: The Host Images and Stego Images.

Table (1) shows the performance evaluation values when applied the proposed algorithm on some test images, while Table (2) shows the comparison with other methods.

Table 1. Performance Evaluation of Proposed Method

Image	MSE	PSNR
Lena	0.7838	49.1743
peppers	0.8038	49.0592
baboon	0.7931	49.1302

Table 2. Performance Evaluation comparison with other methods.

References	Image Size	MSE	PSNR
Proposed algorithm	256 × 256	0.7838	49.1743
[14]	256 × 256	8.6632	38.7540
[15]	256 × 256	1.6845	45.8661

The MSE is used to assess how resilient image is to various attacks. MSE contrasts between the original image and the stego image. low MSE values means that the suggested approach was resistant to attacks. The quality of the stego image after reconstructed it was compared with host image using the PSNR. The recommended method is effective when its value is high. In this section discussed the results of the proposed method with other related works as show in Table (2). The proposed method is a reliable for protecting image because it exhibits great capabilities.

CONCLUSION

Proposes an image steganography method in this paper by combining both Pelican Optimization Algorithm (POA) and Least Significant Bit (LSB). Peak-Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) were used to evaluate the performance of the suggested method. The suggested approach showed good results when compared with related works. Apply the proposed method to video and audio, and use different swarm algorithm as future work.

Conflict of interests: The author declared no conflicting interests.

Sources of funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author contribution: Author contributed in the study.

REFERENCES

1. Gary Ka C, H. An Overview on Steganography. Advanced in Computers. 2011;83:51-107. https://doi.org/10.1016/B978-0-12-385510-7.00002-3

2. Douglas M, Bailey, K., Leeney, . An overview of steganography techniques applied to the protection of biometric data. Multimed Tools Appl 2018;77:17333–73. https://doi.org/10.1007/s11042-017-5308-3

3. Mansi SaV, M. current Statues and Key Issues in Image Steganography:A Survey. Computer Science Review. 2014;13:95-113. https://doi.org/10.1016/j.cosrev.2014.09.001

4. Patel SaC, S., . Steganography Using Hybrid Crypto Encryption Technique. IOT Based Control Networks and Intelligent Systems: Proceedings of 3rd ICICNIS. 2022:453-66. . https://doi.org/10.1007/978-981-19-5845-8_32

5. Trojovský P, Dehghani M. Pelican optimization algorithm: A novel nature-inspired algorithm for engineering applications. Sensors. 2022;22(3):855. https://doi.org/10.3390/s22030855

6. Abualigah L, Yousri D, Abd Elaziz M, Ewees AA, Al-Qaness MA, Gandomi AH. Aquila optimizer: a novel meta-heuristic optimization algorithm. Computers & Industrial Engineering. 2021;157:107250. https://doi.org/10.1016/j.cie.2021.107250

7. Geetha K, Anitha V, Elhoseny M, Kathiresan S, Shamsolmoali P, Selim MM. An evolutionary lion optimization algorithm-based image compression technique for biomedical applications. Expert Systems. 2021;38(1):e12508. https://doi.org/10.1111/exsy.12508

8. Alamir N, Kamel S, Megahed TF, Hori M, Abdelkader SM. Developing hybrid demand response technique for energy management in microgrid based on pelican optimization algorithm. Electric Power Systems Research. 2023;214:108905. https://doi.org/10.1016/j.epsr.2022.108905

9. SeyedGarmroudi S, Kayakutlu G, Kayalica MO, Çolak Ü. Improved Pelican optimization algorithm for solving load dispatch problems. Energy. 2024;289:129811. https://doi.org/10.1016/j.energy.2023.129811

10. Dabeer O, Sullivan K, Madhow U, Chandrasekaran S, Manjunath B. Detection of hiding in the least significant bit. IEEE Transactions on Signal Processing. 2004;52(10):3046-58. . https://doi.org/10.1109/TSP.2004.833869

11. Qasim AJ, Din R, Alyousuf FQA. Extended Method of Least Significant Bits on Colour Images in Steganography. QALAAI ZANIST SCIENTIFIC JOURNAL. 2024;9(3):1146-58. https://doi.org/10.25212/lfu.qzj.9.3.45

12. Darwis D, Pamungkas N, editors. Comparison of least significant bit, pixel value

differencing, and modulus function on steganography to measure image quality, storage capacity, and robustness. Journal of Physics: Conference Series; 2021: IOP Publishing. https://doi.org/10.1088/1742-6596/1751/1/012039

13. Sharif A, Mollaeefar M, Nazari M. A novel method for digital image steganography based on a new three-dimensional chaotic map. Multimedia Tools and Applications. 2017;76:7849-67. https://doi.org/10.1007/s11042-016-3398-y

14. ALabaichi A, Al-Dabbas MaAAK, Salih A. Image steganography using least significant bit and secret map techniques. International journal of electrical & computer engineering (2088-8708). 2020;10(1). https://doi.org/10.11591/ijece.v10i1.pp935-946

15. Ghnemat R, Al-mashaqbeh S, editors. Novel Image Data Augmentation Technique for Deep Learning Using Least Significant Bit Encryption. Proceedings of the 2024 9th International Conference on Machine Learning Technologies; 2024. . https://doi.org/10.1145/3674029.3674053

16. Hameed MA, Hassaballah M, Abdelazim R, Sahu AK. A novel medical steganography technique based on adversarial neural cryptography and digital signature using least significant bit replacement. International Journal of Cognitive Computing in Engineering. 2024;5:379-97. https://doi.org/10.1016/j.ijcce.2024.08.002

17. Talib E, Hassan NF, Jamil AS. The Defensive Methods Against Deepfake. Iraqi Journal of Science. 2023:5345-57. https://doi.org/10.24996/ijs.2023.64.10.39

18. Mellimi S, Rajput V, Ansari IA, Ahn CW. A fast and efficient image watermarking scheme based on deep neural network. Pattern Recognition Letters. 2021;151:222-8. https://doi.org/10.1016/j.patrec.2021.08.015

19. Jamil AS, Hassan NF. Proposed Color Image Lightweight Encryption using SALSA20 with Key Derivation Function. Baghdad Science Journal. 2025;22(1). https://doi.org/10.21123/bsj.2024.9280

20. Habib HB, Hussein WA, Abdul-Rahman AK. A hybrid cryptosystem based on latin square and the modified BB84 quantum key distribution. Tikrit Journal of Pure Science. 2022;27(4):100-3. https://doi.org/10.25130/tjps.v27i4.42

21. AL-Khafaji GK, Hussain AA. A Pixel Based Method for Image Compression. Tikrit Journal of Pure Science. 2021;26(1). https://doi.org/10.25130/tjps.v26i1.108

22. Hussein QM, Abdullah AS, Mohammed NQ. The efficiency of Color Models layers at Color Images as Cover in text hiding. Tikrit Journal of Pure Science. 2016;21(1):130-9. https://tjps.tu.edu.iq/index.php/tjps/article/download/963/624