ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a4

Al-Noor Journal for Information Technology and Cybersecurity

https://jncs.alnoor.edu.iq/

Performance Analysis of Hybrid Cryptography and Steganography for Sustainable Cybersecurity and Data Protection

[1] Mohammed Yaseen Alhayani, [2]Osama A. Qasim, [3]Omaima Muyassar, [4]Zainab Bashar

[1] Department of Software, Information Technology College, Ninevah University, Mosul, Iraq
[2] Computer Systems Technology, Technical Management Technology Institute Nineveh, Northern Technical University, Mosul, Iraq
[3,4] Department of Software, Information Technology College, Ninevah University, Mosul, Iraq

Article information

Article history:
Received: September, 02,2025
Revised: September, 20,2025
Accepted: November 21, 2025

Keywords:
Steganography
Cybersecurity
AES Encryption
PSNR
NPCR&UACI
Histogram

Correspondence:

Mohammed Yaseen Alhayani
mohammed.y.abdullah@uoninevah.edu.iq

Abstract

This study combines block and hybrid encryption techniques with steganography to defend textual content documents and conceal them in inner photos, supplying two-layer security in opposition to cyberattacks. The proposed method integrates Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Least Significant Bit (LSB) embedding to acquire robust cryptographic safety and imperceptible data hiding. Experimental outcomes reveal that the system achieves a 100% image matching charge with an encryption satisfaction of 99.6%, indicating high compatibility between encryption and steganography methods. Histogram analysis confirms uniform pixel intensity distribution without an observable distinction between natural and stego images. Peak Signal-to-Noise Ratio (PSNR) values reached up to 100.53 dB for medium-sized pics, displaying minimal distortion. NPCR consequences for encrypted snapshots were 99.60%, confirming sturdy sensitivity to pixel modifications, at the same time as NPCR for stego pix remained close to 0.003%, proving imperceptibility. UACI values for encrypted pix ranged between 34.20% and 46.89%, validating exceptional encryption, at the same time as UACI for stego snapshots remained negligible, confirming concealment performance. These results highlight the originality of the proposed hybrid version in combining AES, RSA, and LSB to concurrently attain high-speed encryption, stable key control, and undetectable information hiding.

DOI: https://doi.org/10.69513/jncs.v2.i2.a4 ©Authors, 2025, Alnoor University.

Study Overview

In today's virtual era, securing sensitive data against cyber threats has come to be a crucial assignment. Traditional cryptographic techniques, along with symmetric and uneven encryption, provide sturdy data protection, but the encrypted content itself regularly signals the presence of confidential conversation, which could draw the attention of attackers. Conversely, steganography conceals the very life of conversation with the aid of embedding mystery records within harmless-looking files consisting of photos, audio, or video. However, steganography alone lacks the cryptographic strength to protect information if the hidden content material is extracted [1]. To overcome those boundaries, researchers have explored hybrid techniques that integrate cryptography with steganography, aiming to achieve both fact confidentiality and concealment. Existing approaches often face trade-offs between pace, protection, and detectability, making them much less effective in environments where both efficiency and robustness are essential [2] This work

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a4

proposes a hybrid system that mixes Advanced Encryption Standard (AES) block cipher for instant and reliable data encryption, Rivest–Shamir–Adleman (RSA) for steady key trade, and Least Significant Bit (LSB) steganography for imperceptible facts hidden inside snapshots. Unlike conventional strategies, this technique eliminates the direct connection between plaintext files and intercepted communication, thereby strengthening resilience towards cyber-attacks [3]. The novelty of this study lies in the synergistic use of symmetric and uneven cryptography with steganography, imparting a multi-layered protection that ensures both cryptographic robustness and covert transmission. To validate the effectiveness of the proposed machine, overall performance is evaluated using more than one metric, including Peak Signal-to-Noise Ratio (PSNR), Entropy, Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI). These measures investigate both the excellence of encryption and the invisibility of hidden information, confirming the sustainability and practicality of the approach.

Related Work

Varghese, F., & Sasikala, P. (2023) presented block size, key size, encryption speed, memory use, and security level as just a few of the variables to compare various encryption methods and steganography. In industries like information technology, banking, and healthcare, digital communication is essential. Steganography and cryptography techniques are employed to guarantee data security. They concluded that cryptography allows for the distortion of original signals by encrypting secret information in an unintelligible manner. Steganography conceals messages in secret data, including text, video, audio, and images. The basics of cryptography and steganography are examined in this review paper, which also evaluates encryption methods according to memory utilization, security level, block size, key size, and encryption speed. Unlike this study, our model develops a concrete hybrid AES–RSA–LSB framework with performance validation, moving from assessment to realistic implementation [4].

abd Qasim, O., & Golshannavaz, S. (2024) proposed a multi-layer encryption scheme and steganography to protect sensitive data in smart grids from cyber threats. The system uses the AES algorithm and a digital dictionary to encrypt data concealed within an image. The study evaluates performance parameters like PSNR, RMSE, UACI, and NPCR, proving that the proposed system is reliable and quick and strikes a balance between security and processing time. Based on recorded values for PSNR, RMSE, UACI, and NPCR, the study shows that the suggested multi-layer encryption system, which combines dictionary encryption and AES, is a reliable and quick way to protect sensitive data while striking a balance between security and processing time. This research can be used to develop a combined encryption and steganography system with broader capabilities to increase the security of text files[5]. We extend beyond their domain-unique method with the aid of integrating RSA for stable key trade with AES and LSB, improving both scalability and standard applicability for textual content-record protection.

This paper proposes a novel, multi-layered steganographic framework by Sanjalawe, Yousef, et al (2025). that enhances data integrity, authenticity, and confidentiality in the digital era. The framework combines to increase imperceptibility, robustness, and security, use Huffman coding, least significant bit embedding, and an encoder-decoder based on deep learning. The framework accomplishes strong data recovery, great visual quality, and improved defense against frequent attacks. This innovative approach advances secure communication and digital rights management. By balancing and optimizing[6] By combining deep learning, adaptive embedding, and compression in a novel way, this article tackles contemporary data-concealing issues while promoting imperceptibility and resilience in digital rights management and secure communication. Significant enhancements include strong data recovery, with text recovery accuracy frequently surpassing 100%, enhanced defense against common threats like noise and compression, and excellent visual fidelity, with Structural Similarity Index Metrics (SSIM) consistently above 99%. This study motivates our research approach by proposing a Least Significant Bit (LSB) technique for data hiding as well as using criteria to measure the similarity between plain images and encrypted images to know the quality of encryption and data hiding techniques[7]. While their attention is on AI-pushed embedding, our originality lies in uniting symmetric-asymmetric cryptography with LSB to provide twin-layer protection, ensuring both cryptographic security and covertness.

This study from Chang, C. C., & Echizen, I. (2025). explored a steganographic paradigm where hidden information is communicated through multiple agents interacting with an environment. Each agent learns a policy to disguise hidden messages within actions, while an observer associates behavioral patterns with their respective agents, revealing hidden messages. The interactions are governed by multi-agent reinforcement learning and shaped by feedback from the observer. The game of Labyrinth is used to exemplify action steganography, where subliminal communication is concealed within steering towards a destination. The stego-system[8] has been validated through experimental evaluations[9]. It has been concluded from this research the possibility of enhancing and adding encryption techniques with data hiding techniques for the purpose of enhancing data security, as well as using experimental evaluations and proposed standards for the purpose of analyzing performance and reaching the highest level of developing encryption and hiding techniques on data and text files. In assessment, our work does not rely on behavioral getting to know you but instead proposes a sustainable, photograph-primarily-based hybrid encryption–steganography system evaluated with extensively normal metrics (PSNR, Entropy, NPCR, UACI), making it extra practical for stable record transmission.

Methodology

The research-made text file, with a size of 31 bytes, contains normal text. Plain images and the encrypted file are displayed, along with a data-hiding (Least Significant Bit) technique that combines the encrypted text and plain image. The steganographic image is encrypted using a hybrid method for data security and contains symmetric and asymmetric techniques. The algorithms and hybrid techniques used are explained along with their working methods and formulas. The file is then decrypted and extracted as in Table 1. The AES algorithm's encryption process was successful, and the image-hiding technique maintained the same file size within the image. The quality of the steganographic technique is assessed for success in encryption and data-hiding processes.

Steganography LSB

is the process of hiding a file, message, picture, or video inside another image, video, or message. Steganós, which means "covered or concealed," and -graphia, which means "writing," are combined to form the Greek term steganography, which is where the name "steganography" originates. The acronym for Least Significant Bit is LSB. LSB embedding is based on the theory that a pixel's color won't change greatly if its final bit value is changed. 0 is black, for instance. Since the value is still black, albeit a lighter hue, changing it to 1 won't have much of an impact[10].

$S_i=C_i-(C_i \bmod 2) + M_i$ ……………………..(1)

Where:

- S_i = stego pixel value after embedding
- C_i = cover pixel value (original image pixel)
- M_i = message bit (0 or 1) to be embedded

Hybrid Algorithm

The symmetric and asymmetric block ciphers, AES and RSA, are the methods by which the hybrid algorithm operates. The process begins by creating an AES key and encrypting data using AES. Next, it generates public and private keys to encrypt the AES key using the RSA algorithm. First, the AES key is decrypted using RSA, and then the data is decrypted using AES. Additionally, as shown in figure 1, transform bytes to a hex string and save the hex data to a file.

$C=(E_{RSA}(K_{AES}),E_{AES}(M,K_{AES}))$……………………..(2)

Where:

- M = plaintext message
- K_{AES} = randomly generated AES session key
- $E_{AES}(M,K_{AES})$ = ciphertext of message using AES
- $E_{RSA}(K_{AES})$ = AES key encrypted using RSA public key
- C = final hybrid ciphertext (consisting of encrypted AES key + encrypted data)

Decryption process:

$M = D_{AES}\,(E_{AES}(M, K_{AES}), D_{RSA}(E_{RSA}(K_{AES}))$ ……………………..(3)

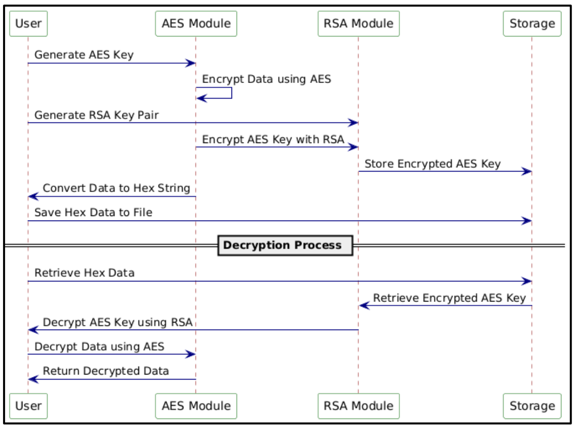
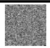


Fig. 1. Hybrid algorithm encryption and decryption.

Experimental Result

All encryption and masking operations inside images of encrypted files with their different bit sizes are displayed, in addition to displaying the results of the criteria and evaluation of the proposed algorithms and steganography technique to document and know the quality of the proposed data security. Table 1 shows three images with different dimensions and sizes. The first image represents the small image with fixed dimensions (750x750), the second image represents the medium size with different dimensions (1280x1221), and the third image is the large size with different dimensions (736x1308). The table shows the success of the file encryption process using the AES algorithm, as well as the success of the process of hiding the encrypted files inside the different images without changing the size of the image, which remained equal to the original image. The hybrid encryption algorithm succeeded in encrypting the hidden image and changing its size slightly. In the process of decrypting and extracting the files, the process was largely successful, as all files and images returned to their normal shape and size without change, which indicates a successful encryption and hiding process.

Table 1. Visual forms and sizes of original, encrypted file, and steganographic images.

Steganography& Encryption	Small Image (750x750)	231,604 bytes	48 bytes	231,604 bytes	214,986 bytes
	Medium Image (1280x1221)	1,144,732 bytes	48 bytes	1,144,732 bytes	1,181,729bytes
	Larg Image (736x1308)	1,458,341 bytes	48 bytes	1,458,341 bytes	 1,437,097bytes
Process	**Image**	**Hybrid Decryption**	**Steganographic Extraction**	**AES File Decryption**	**Original Image**
Decryption&Extraction	Small Image (750x750)	214,159 bytes	231,604 bytes	31 bytes	231,604 bytes
	Medium Image (1280x1221)	1,178,908 bytes	1,144,732 bytes	31 bytes	1,144,732 bytes
	Large Image (736x1308)	1,433,811 bytes	1,458,341 bytes	31 bytes	1,458,341 bytes

Histogram Analysis

A histogram of the pixel intensity values is typically referred to as the image's histogram in image processing contexts[11]. The number of pixels in an image at each of the several intensity levels included in the image is shown by this histogram, which is a graph. An 8-bit grayscale image can have 256 different intensities; hence, the histogram will graphically show 256 numbers that indicate the distribution of pixels among those grayscale values. Another way to histogram color photos is to produce separate histograms for the red, blue, and green channels or a 3-D histogram where the brightness at each point indicates the number of pixels[12]. The evaluating for the pixel intensity distribution of an image is included by equation below:

$$H(I)= \frac{1}{N} \sum_{i=0}^{L-1} Count(I=i) \quad (1)$$

Table 2 shows histograms of original, hidden, and extracted images for AES-encrypted algorithms[13]. AES algorithm and least significant bit steganography successfully encrypt files and uniformly distribute pixel intensity values, ensuring constant pixel distribution and no difference between natural and hidden images.

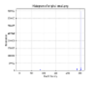
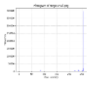
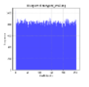
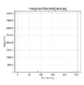
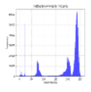
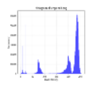
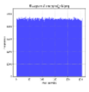
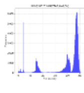
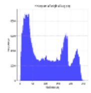
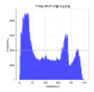
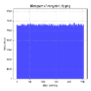
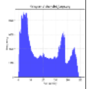
Process	**Image**	**Original Image**	**Stego Img&file**	**Hybrid Encrypted Img**	**Hybrid Decrypted Img**
Steganography & Extraction	Small Image (750x750)				
	Medium Image (1280x1221)				
	Large Image (1280x1221)				

Table 2. Histogram graphics of original, hidden file image, extracted image.

Peak Signal-to-Noise Ratio (PSNR)

PSNR refers to the ratio of a signal's maximal power to the power of corrupting noise that reduces the representation's fidelity in engineering. PSNR[14] is typically expressed using the decibel scale as a logarithmic quantity since many signals have a very large dynamic range. PSNR is frequently used to measure the reconstruction quality of images and videos that have undergone encryption, lossy compression, and encryption quality[15]. The formula below can be used to determine the PSNR value, where R is the image's maximum pixel value (255 for 8-bit images, for example):

$$\textbf{PSNR = 10.}\ \text{Log}_{10}\left(\frac{R^2}{MSE}\right) \quad (2)$$

Table 3. PSNR values for original image with stego Img&file, encrypted, decrypted and extracted image.

Image	**Stego Img&file**	**Encrypted Image**	**Decrypted Image**	**Extracted Image**
Small	91.01 dB	5.19 dB	100 dB	91.01 dB
Mid	100.53 dB	6.47 dB	100 dB	100.53 dB
Large	97.55 dB	7.55 dB	100 dB	97.55 dB

Table 3 shows minimal difference between original and hidden images, with a full PSNR value indicating effective encryption. The hybrid algorithm outperforms, indicating higher quality. Hidden files do not alter original image properties, indicating the efficiency of the techniques used.

Number of Pixels Change Rate (NPCR)

NPCR is a crucial metric for evaluating the effectiveness of image encryption algorithms, indicating the sensitivity of the scheme to small changes. Low values indicate minimal alterations, while higher values suggest more visible alterations, potentially indicating less secure or noticeable embedding techniques[16]. More obvious changes are indicated by higher NPCR scores, which could point to less secure or more obvious embedding methods as equation below[17, 18]:

$$\text{NPCR} = \frac{\sum i,jD(i,j)}{W\times H} \times 100\% \quad (3)$$

Unified Average Changing Intensity (UACI)

Image encryption methods are assessed by UACI, which measures the change in an encrypted image due to minor modifications. Low UACI values indicate minimal pixel intensity differences, ideal for steganography to prevent detection. Significant intensity variations are suggested by higher UACI values, which may increase the steganographic image's detectability[17, 19].

$$\text{UACI}=\left(\frac{1}{W\times H}\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{C_1(i,j)-C_2(i,j)}{255}\right)\ 100\% \quad (4)$$

Table 4. NPCR&UACI value for original with encrypted, decrypted and stego Img&file.

Image	NPCR Stego	NPCR Encrypted	NPCR Decrypted	UACI Encrypted	UACI Decrypted	UACI Stego
Small	0.0030%	99.6078%	0.0000%	46.8995%	0.0000%	0.0000%
Mid	0.0005%	99.6141%	0.0000%	39.3076%	0.0000%	0.0000%
Large	0.0007%	99.6069%	0.0000%	34.2089%	0.0000%	0.0000%

Table 4 measures the number of pixels changed between original and steganographic images, with low NPCR values indicating minimal changes. Larger images have lower NPCR due to more evenly distributed hidden data. UACI (Unified Average Changing Intensity) shows minimal impact on intensity levels. LSB steganography is nearly imperceptible in all image sizes, with larger images distributing embedded data more evenly[19, 20].

Discussion

Based on the above criteria (Tables 1-5), the results can be discussed that the method of encrypting a file using the AES block cipher algorithm and hiding it inside an image using LSB is almost undetectable across all image sizes, and it is impossible to predict whether the file will appear inside an image, and the reasons are as follows:

1- Changes are less noticeable in larger images because the embedded data is evenly distributed.

2- To fully protect the data from unauthorized individuals and enhance the security and reliability of data protection, it is recommended to use the hiding technique in conjunction with data encryption.

3- The process of encrypting and hiding the file inside an image was not distinguished from the original image, in addition to the success of encrypting the image and returning it and successfully extracting the file from it without obstacles.

4- Flexibility and compatibility of encryption methods with high-quality hiding methods and following the image quality and encryption standards, we find that the image matching rate was 100% and the encryption quality reached 99.6%.

Table 5 lines up our results against previous works on the same metrics (PSNR, NPCR, UACI, Encryption Quality, Image Matching Rate) which suggests better effectiveness of the results and values of our study in light of the criteria of encryption efficiency and data hiding.

Table 5. Comparative analysis of proposed model vs. previous Works.

Study / Method	PSNR (dB)	NPCR (%)	UACI (%)	Encryption Quality (%)	Image Matching Rate (%)	Remarks
Varghese & Sasikala (2023)	—	—	—	Compared algorithms qualitatively	—	Focused on reviewing algorithms, no experimental benchmark.
Qasim & Golshannavaz (2024)	e.g., ~40–50 dB	~99%	~33–35%	—	—	Multi-layer AES + dictionary encryption with steganography.
Sanjalawe et al. (2025)	SSIM > 99%	—	—	—	—	Deep learning + LSB + Huffman coding; focused on robustness and imperceptibility.
Chang & Echizen (2025)	—	—	—	—	—	Reinforcement learning steganography; evaluated by experimental scenarios, not PSNR/NPCR.
Proposed AES + RSA + LSB (This work)	**91.01–100.53 dB**	**99.60%+**	**34.20–46.89%**	**99.6%**	**100%**	Dual-layer hybrid encryption + imperceptible LSB embedding with high efficiency.

Despite those promising results, several limitations should be acknowledged. First, the LSB technique, even as effective as it is in hiding data, is known to be at risk of statistical and steganalysis attacks, which could compromise security if attackers employ superior detection techniques. Second, the approach depends heavily on the dimensions and quality of the quilt photo; small or low-resolution photographs restrict embedding potential, and boom, there's the hazard of distortion. Third, the machine introduces computational overhead due to the dual use of AES and RSA encryption, which might also restrict scalability in real-time or aid-limited environments. Finally, this looks at targeting more often than not at photo carriers; extending the technique to different

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a4

multimedia codecs (audio, video) remains unexplored.

Conclusion

The study reveals that the method of encrypting the file using the AES block cipher algorithm and hiding it inside an image using LSB is almost undetectable across all image sizes, and increasing the complexity of the protection using the hybrid encryption algorithm that encrypted the hidden image did its job successfully. This is due to the even distribution of the embedded data in the larger images, the recommendation to use the stash technique in conjunction with data encryption, the indistinguishability of the process from the original image, and the compatibility of the encryption methods with high-quality stash methods. The flexibility and compatibility of the encryption methods with high-quality stash methods were concluded, and by following the image quality and encryption standards, we found that the image matching rate was 100% and the encryption quality reached 99.6%. The study demonstrates the effectiveness of combining AES, RSA, and LSB steganography for stable information hiding. Future studies need to raise awareness on enhanced steganographic strategies, expand the technique to multimedia providers, optimize for resource-restricted systems, compare the gadget on large datasets, and integrate the hybrid version into stable communication protocols or cloud-based frameworks. This will help increase a more steady, bendy, and extensive relevant solution for sustainable cybersecurity.

References

1. Abdullah, M.Y., et al. *Implementing Blockchain Technology in Robotic Decision Making*. in *2024 36th Conference of Open Innovations Association (FRUCT)*. 2024. IEEE.
2. Ortakci, Y. and M.Y. Abdullah. *Performance analyses of aes and 3des algorithms for encryption of satellite images*. in *Innovations in Smart Cities Applications Volume 4: The Proceedings of the 5th International Conference on Smart City Applications*. 2021. Springer.
3. Alhayani, M. and M. Al-Khiza'ay. *Analyze symmetric and asymmetric encryption techniques by securing facial recognition system*. in *International Conference on Networking, Intelligent Systems and Security*. 2022. Springer.
4. Varghese, F. and P. Sasikala, *A detailed review based on secure data transmission using cryptography and steganography.* Wireless Personal Communications, 2023. **129**(4): p. 2291-2318.
5. abd Qasim, O. and S. Golshannavaz, *Data protection enhancement in smart grid communication: An efficient multi-layer encrypting approach based on chaotic techniques and steganography.* e-Prime-Advances in Electrical Engineering, Electronics and Energy, 2024. **10**: p. 100834.
6. Alhayani, M., N. Alallaq, and M. Al-Khiza'ay. *Optimize one max problem by PSO and CSA*. in *International Congress on Information and Communication Technology*. 2023. Springer.
7. Sanjalawe, Y., et al., *A deep learning-driven multi-layered steganographic approach for enhanced data security.* Scientific Reports, 2025. **15**(1): p. 4761.
8. Sabharwal, A., P. Yadav, and K. Kumar, *Graph Crypto-Stego System for Securing Graph Data Using Association Schemes.* Journal of Applied Mathematics, 2024. **2024**(1): p. 2084342.
9. Chang, C.-C. and I. Echizen, *Steganography in Game Actions.* IEEE Access, 2025.
10. Aslam, M.A., et al. *Image steganography using least significant bit (lsb)-a systematic literature review*. in *2022 2nd International Conference on Computing and Information Technology (ICCIT)*. 2022. IEEE.
11. Hashim, A.T., A.K. Jabbar, and Q.F. Hassan. *Medical image encryption based on hybrid AES with chaotic map*. in *Journal of Physics: Conference Series*. 2021. IOP Publishing.
12. Peeples, J., W. Xu, and A. Zare, *Histogram layers for texture analysis.* IEEE Transactions on Artificial Intelligence, 2021. **3**(4): p. 541-552.
13. Mohd, N.A.A. and A.Y.A. Ashawesh. *Enhanced AES algorithm based on 14 rounds in securing data and minimizing processing time*. in *Journal of Physics: Conference Series*. 2021. IOP Publishing.
14. Ibrahim, A.G.A., M. Saleh, and A.A. Elmahallawy, *De-Noising of Secured Stego-Images using AES for Various Noise Types.* Przeglad Elektrotechniczny, 2023. **99**(2).
15. Suriyan, K., et al., *Performance analysis of peak signal-to-noise ratio and multipath source routing using different denoising method.* Bulletin of Electrical Engineering and Informatics, 2022. **11**(1): p. 286-292.
16. Ignacio-Cerrato, S., et al., *Optimized data management with color multiplexing in QR codes.* Physica Scripta, 2024. **99**(10): p. 105036.
17. Rahman, S., et al., *A Huffman code LSB based image steganography technique using multi-level encryption and achromatic component of an image.* Scientific Reports, 2023. **13**(1): p. 14183.
18. Hatem, F., et al. *A Method of Removing Rain or Snow from A Color Image using MATLAB*. in *2024 35th Conference of Open Innovations Association (FRUCT)*. 2024. IEEE.
19. Yildirim, M., *Steganography-based voice hiding in medical images of COVID-19 patients.* Nonlinear Dynamics, 2021. **105**(3): p. 2677-2692.
20. Salih, M.M., et al. *Capacity, spectral and energy efficiency of oma and noma systems*. in *2024 35th Conference of Open Innovations Association (FRUCT)*. 2024. IEEE.