Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44)** : 1–8.
ISSN-0037-8712
doi:10.5269/bspm.79285

# A Comparative Analysis for Sustainable Cybersecurity Solutions on Improving Image Security via Hybrid, Symmetric and Asymmetric Encryption

Rana Raad Shaker Alnaily

ABSTRACT: The study suggests a new method for encrypting and securing images called the hybrid algorithm, which combines symmetric and asymmetric techniques, and compares it with AES, RSA, and other encryption algorithms. Five high-resolution grayscale photos of different sizes were used for encryption and decryption. The images were encrypted using AES, RSA, and hybrid algorithms. Performance analysis criteria like entropy, PSNR, correlation coefficient, and elapsed time were used to evaluate the algorithms' performance. Python was used for programming all simulation algorithms and criteria. Finding that hybrid encryption outperforms AES and RSA in terms of image size, strength, and encryption quality. It also outperforms RSA in PSNR and elapsed time for total encryption and decryption. The hybrid algorithm is 2% fast-er and has the lowest entropy value, making it resistant to statistical attacks. It has been discovered that the combination of symmetric and asymmetric encryption techniques creates a highly efficient algorithm for data security.

Keywords: Hybrid image encryption, data security, symmetric and asymmetric cryptography, AES, RSA, performance analysis.

## Contents



## 1. Introduction

These days, safeguarding and securing data is not just a necessity but also a competitive strategy that can lead to greater advantages across all industries. among the fundamental elements of every data security system. This is encryption, which transforms data (the plaintext) into a form that seems unintelligible (the ciphertext) using a mathematical method and certain secret information (the encryption key). The decryption process undoes this modification and reverses the results of the encryption algorithm using a mathematical technique and a secret value (the decryption key). An encryption technique with all of its possible keys, plaintext, and cipher-texts is called a cryptosystem, commonly known as a cryptographic system. The two most popular methods for encrypting data are. Depending on the kind of input, two different encryption methods are used: block ciphers and stream ciphers. From a fixed-size input, such as b bits, an encryption process called a block cipher generates a ciphertext made up of b bits. If the input is more than b bits, it can be further divided. Block ciphers can function in multiple ways, each appropriate for a certain use case [1]. This study uses block ciphers represented in symmetric and asymmetric encryption, represented by the AES and RSA algorithms [2,3]. The algorithms are analyzed based on specific criteria and previous studies; a hybrid algorithm was built that combines symmetric

2020 *Mathematics Subject Classification:* 94A60, 94A08.
Submitted September 30, 2025. Published March 22, 2026

and asymmetric encryption techniques. By adopting the three algorithms as an approach, we reach an advanced stage of encryption and data protection after making a comparison between the proposed algorithms and the hybrid algorithm through special quality analysis criteria. We aim to reach the highest levels of security that enable the user to obtain the advantage in any institutional field he chooses to implement a high data protection and security project.

Sood and Kaur in 2023, surveyed data encryption to guarantee the safety of this data and the potential for using encryption techniques to secure it. The researchers noted that information security refers to the procedures used to prevent sensitive data from being misused or disclosed due to the risks involved. Information security has become more crucial in data transmission and storage due to the quick development of digital data exchange. The art of encryption has grown more intricate as human intellect has advanced to increase the security of information. To increase the security of information, many encryption algorithms are used. An overview of the encryption techniques RSA, DES, and AES was given [3,4]. The AES algorithm was deter-mined to be the most effective in terms of speed, time, throughput, and collapse effect based on the literature review. As our study contributed, the security offered by the AES method can be further improved by applying multiple algorithms to the data and combining them with other encryption approaches [1].

Abd Qasim and Golshannavaz in 2024, suggested A multi-layer encryption system to safeguard private information in smart grids against online attacks. The AES algorithm and digital dictionary are used by the technology to encrypt data and hide it inside an image. The suggested system was examined using the fundamental performance evaluation metrics, including root mean square error (RMSE), maxi-mum signal-to-noise ratio (PSNR), and average processing times across ten runs. The study demonstrates that this methodology is dependable, quick, and strikes a balance between processing time and security, encouraging more research on a hybrid strategy to identify the best encryption technique. This study motivated us to move for-ward by proposing a new hybrid approach that is compared with the basic algorithms to find an optimal encryption method [5].

Ashok in 2024, discovered that secure end-to-end audio communication is essential has several problems. A review paper that covers security algorithms for voice communication and has evaluation criteria that are more expansive than those found in the literature would be beneficial to researchers in this subject. This study evaluates different approaches to secure speech transmissions via communication networks and gives a thorough review of end-to-end secure audio communication. The evaluation parameters include Recovered Speech Quality, Transmission Error Rate, System Security, and System throughput Capacity. The chaos of cryptography [6], on the other hand, offers appropriate cryptography for voice security. The researchers highlighted the shortcomings of the proposed fixes, such as evaluating and improving voice quality, and the requirements for further development of practical methods for using common security methods, which inspired us to develop our research by finding new evaluation methods and integrating different encryption techniques to achieve better security methods.

Modi et al., in 2025 [7]. Proposed hybrid encryption to protect sensitive data, including criminal information and prison records. The encryption process involves symmetric encryption and a symmetric key, with the symmetric key being decrypted by the recipient. The encrypted data is then sent to the receiver using the decrypted symmetric key. This approach addresses the issue of data being transferred between departments, where hackers can infiltrate and contaminate the information. The researchers conclude that hybrid encryption [8] is a secure solution for protecting sensitive data. At the end of the study, the researchers recommend hybrid encryption as a strategy to keep this data secure, which is what was highlighted in our study to create a hybrid encryption approach from two different algorithms and techniques.

This study examines various techniques for encrypting and decrypting images of various sizes (UltrSmall, Small, Medium, Huge), shapes, and dimensions by comparing the fundamental algorithms AES and RSA in greater detail and developing a hybrid encryption technique. Encryption employs a chaotic method to disperse the image's data using distinct procedures and encryption keys that are obtained by both the sender and the recipient. The encryption process is reversed using the encryption key in order to get the original data content for decryption. To determine the most effective method for encrypting and safeguarding image data, encryption algorithms are compared using specific criteria (correlation coefficient, PSNR, elapsed time, and entropy).

### 1.1. Advanced Encryption Standard (AES)

The symmetric algorithm known as Advanced Encryption Standard (AES) is used to safeguard data by converting it into a format that requires the correct key to view. It was established in 2001 by the National Institute of Standards and Technology (NIST). Despite being more difficult to install, it is nevertheless extensively used today since it is far more powerful than DES and triple DES. Multiple key lengths (128, 192, or 256 bits) are used by AES encryption to offer robust security against unwanted access. This effective and popular data security method can be used to encrypt files, safeguard private data, and secure internet connections. AES, a crucial part of modern encryption, is widely recognized for its ability to shield data from internet threats [9].

### 1.2. Rivest, Shamir, Adleman Algorithm (RSA)

Is an asymmetric or public-key cryptography technique. The Rivest-Shamir-Adleman (RSA) algorithm uses two distinct keys: the public key and the private key. While the private key is used for decoding and needs to be kept secret by the recipient, the public key is used for encryption and is known to everyone. The RSA algorithm bears the names of its 1977 founders, Ron Rivest, Adi Shamir, and Leonard Adleman [10].

### 1.3. Hybrid Algorithm

The hybrid algorithm works by the AES and RSA methods. The algorithm starts with generating an AES key and encrypting data with AES, after that encrypting the AES key with RSA algorithm. The decryption starts with decrypting the AES key with RSA and decrypting data with AES. Also, convert bytes to a hex string and save hex data to a file as Figure 1.

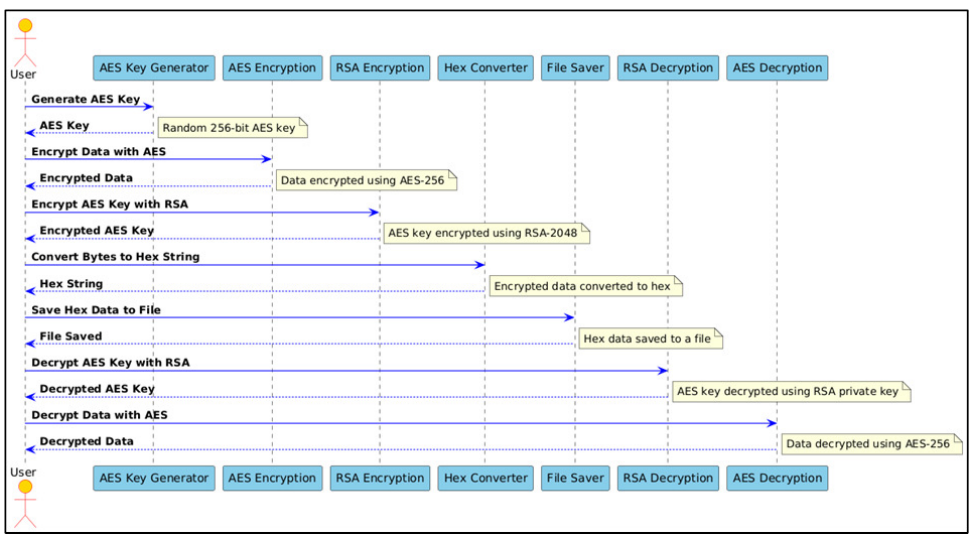


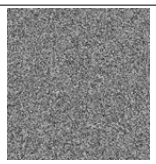
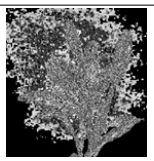
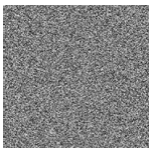
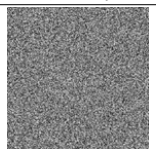
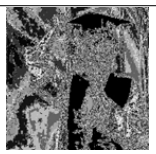
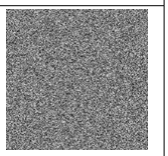
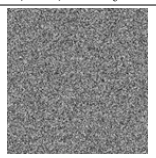
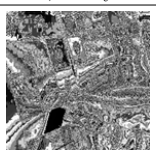
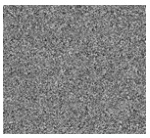
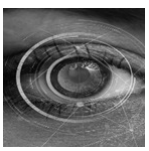
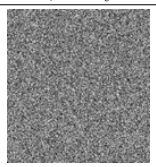
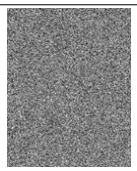
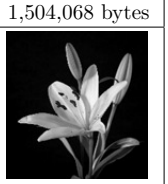
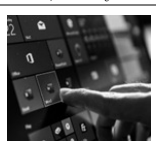
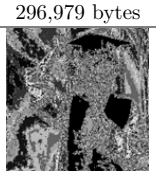
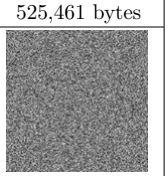
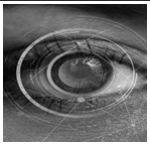
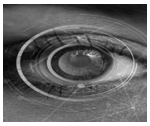
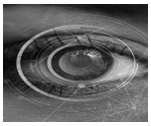

Figure 1: Hybrid encryption and decryption.

## 2. Experiment Result

Five high-resolution grayscale photos of various sizes from the actual world were used. In terms of size, the first image is variable and measures 910×963 (as an UltrSmall image), the second is fixed at 1080x1080 (as a Small image), the third is variable at 1078×779 (as a Medium image), and the final one is huge at 1078×1392 [11] as in Table 1. The AES, RSA, and hybrid algorithms were used to encrypt the pictures. The suggested criteria in the performance analysis procedure were used to evaluate the picture encryption and decryption algorithms' performance. Python is the programming language used to write all simulation algorithms.

The AES algorithm outperforms the RSA algorithm in terms of encryption efficiency and strength, with a 2.150% increase in the size of encrypted images compared to a 648.2% increase for the RSA algorithm.

Table 1: Forms, original img size, encrypted & decrypted images by algorithms

| Process | Image | Original Image | AES | RSA | Hybrid |
|---|---|---|---|---|---|
| Encryption | UltrSmall Image (910x963) |  39,058 bytes |  878,522 bytes |  292,195 bytes |  878,522bytes |
| | Small Image (1080x1080) |  85,163 bytes |  1,169,124 bytes |  488,553 bytes |  1,169,116 bytes |
| | Medium Image (1078x779) |  313,301 bytes |  861,193 bytes |  392,014 bytes |  861,193 bytes |
| | Huge Image (1078x1392) |  974,284 bytes |  1,504,073 bytes |  1,173,825 bytes |  1,504,068 bytes |
| Decryption | UltrSmall Image (910x963) |  39,058 bytes |  176,792 bytes |  176,792 bytes |  289,745 bytes |
| | Small Image (1080x1080) |  85,163 bytes |  296,979 bytes |  296,979 bytes |  525,461 bytes |
| | Medium Image (1078x779) |  313,301 bytes |  204,402 bytes |  204,402 bytes |  313,780 bytes |
| | Huge Image (1078x1392) |  974,284 bytes |  622,703 bytes |  622,703 bytes |  973,196 bytes |

This is due to AES's superior speed and efficiency in handling large amounts of data, particularly for images. RSA, on the other hand, is designed for securing small data portions, resulting in a lower expansion rate. Hybrid encryption outperforms AES and RSA in terms of size and appearance, with a 2.300% increase in original image size [12].

### 2.1. Correlation Coefficient

Correlation coefficient contains horizontal, vertical, and diagonal analysis for images [13] to use the optimal way for optimizing the methods [14]. Below is the equation of correlation coefficient ($r$) between two adjacent pixel.

$$r = \frac{\sum (x_{i-ux})(y_{i-uy})}{\sqrt{\sum (x_{i-ux})^2 \sum (y_{i-uy})^2}} \tag{2.1}$$

In Table 2, the five original images are measured for each of the diagonal, vertical, and horizontal correlations. Because the neighboring pixels are similar, the original images have a high correlation in all three directions.

Table 2: Correlation coefficients of original image

| Image | Horizontal | Vertical | Diagonal |
|---|---|---|---|
| UltrSmall | 0.9939 | 0.9961 | 0.9914 |
| Small | 0.9916 | 0.9950 | 0.9881 |
| Medium | 0.9971 | 0.9959 | 0.9936 |
| Huge | 0.9903 | 0.9900 | 0.9803 |

According to Table 3 in all Correlation coefficients types, the Hybrid values have correlation close to zero, indicating randomness and strong encryption unlike AES and RSA values [15].

Table 3: Correlation coefficients of encrypted image

| Image | Horizontal | | | Vertical | | | Diagonal | | |
|---|---|---|---|---|---|---|---|---|---|
| | AES | RSA | Hybrid | AES | RSA | Hybrid | AES | RSA | Hybrid |
| UltrSmall | 0.0028 | 0.7234 | -0.0004 | -0.0002 | 0.7364 | 0.0007 | -0.0005 | 0.6615 | 0.0014 |
| Small | -0.0023 | 0.5938 | -0.0002 | 0.0002 | 0.6350 | -0.0010 | -0.0005 | 0.5357 | -0.0010 |
| Medium | 0.0007 | 0.5969 | 0.0019 | 0.0018 | 0.5789 | -0.0009 | -0.0007 | 0.4942 | 0.0015 |
| Huge | -0.0015 | -0.0442 | 0.0010 | -0.0008 | 0.2655 | 0.0008 | 0.2163 | 0.1764 | -0.0003 |

### 2.2. Peak Signal-to-Noise Ratio (PSNR)

Encryption analysis ranges from below 10 dB for highly secure encryption, 10-20 dB for moderate distortion, and above 20 dB for weak encryption [16,17]. PSNR value can be calculated by equation below [18]:

$$PSNR = 10.\log_{10}\left(\frac{R^2}{MSE}\right) \tag{2.2}$$

$R$ is representing maximum possible pixel value of the image (255 for 8-bit images).

Table 4: PSNR values for original and decrypt image

| Image | AES | RSA | Hybrid |
|---|---|---|---|
| UltrSmall | 100 dB | 100 dB | 52.08 dB |
| Small | 100 dB | 100 dB | 49.29 dB |
| Medium | 100 dB | 100 dB | 100 dB |
| Huge | 100 dB | 100 dB | 100 dB |

From Table 4 PSNR value is full, that meaning there is no difference at all between the two images for all algorithms.

Table 5 shown multiple comparisons between encrypted photos, the Hybrid and AES algorithms surpassed the RSA method, demonstrating that its encryption quality is superior. The PSNR value between the original and encrypted images is desirable, suggesting effective encryption (high distortion) for hybrid algorithm.

Table 5: PSNR values for original and encrypt image

| Image | AES | RSA | Hybrid |
|---|---|---|---|
| UltrSmall | 8.15 dB | 8.97 dB | 5.69 dB |
| Small | 5.68 dB | 7.65 dB | 8.16 dB |
| Medium | 7.01 dB | 6.91 dB | 7.03 dB |
| Huge | 8.88 dB | 9.25 dB | 8.89 dB |

### 2.3. Elapsed Time

The elapsed time used to measure running and processing time for the algorithms to conclude which algorithm is better and faster. According to Table 6, the Hybrid is faster than others for total encryption and decryption.

Table 6: Total elapsed time per second of encrypt and decrypt image

| Image | AES | RSA | Hybrid |
|---|---|---|---|
| UltrSmall | 1.27 sec | 1.18 | 0.48 sec |
| Small | 1.29 sec. | 1.65 | 0.66 sec |
| Medium | 1.38 sec | 1.24 | 0.63 sec |
| Huge | 1.52 sec | 2.31 | 1.22 sec |

### 2.4. Entropy Analysis

More randomness is indicated by an entropy value near 8, which strengthens the image's resistance to cryptanalysis [19]. Entropy (Hx) value can be calculated by equation below [20]:

$$H(x) = -\sum_{i=0}^{255} p_{(xi)} \log_2 p_{(xi)} \tag{2.3}$$

Table 7: Entropy values for encrypted decrypted image

| Image | Originlal | AES encrypted | AES decrypted | RSA encrypted | RSA decrypted | Hybrid encrypted | Hybrid decrypted |
|---|---|---|---|---|---|---|---|
| UltrSmall | 6.2412 | 7.99981 | 5.3035 | 5.0067 | 5.3035 | 7.9962 | 5.2960 |
| Small | 5.3035 | 7.99983 | 6.2412 | 5.8710 | 6.2412 | 7.9981 | 6.2878 |
| Medium | 7.0631 | 7.999812 | 7.0631 | 6.4936 | 7.0631 | 7.9993 | 7.0631 |
| Huge | 7.3095 | 7.99988 | 7.3095 | 6.8063 | 7.3095 | 7.9997 | 7.3095 |

According to Table 7 above it can be concluded that; AES and hybrid encryption achieve high entropy (∼8) across all image sizes, making them highly resistant to statistical attacks. RSA encryption shows lower entropy, suggesting it does not randomize pixel intensities as effectively. Decrypted images for both AES and RSA return nearly to their original entropy values, while RSA-decrypted images retain slightly altered entropy values. AES with RSA is more effective for image encryption when security and randomness are primary concerns, as it achieves near-perfect entropy.

## 3. Discussion

When reviewing the benchmark results for the AES, RSA and hybrid encryption algorithms, the results can be discussed as follows:

1. About the image size, hybrid encryption outperforms AES and RSA with a 2.300% increase in original image size.
2. Hybrid values have a close-to-zero correlation, indicating strong encryption unlike AES and RSA.
3. Hybrid and AES algorithms outperform RSA in encryption quality for PSNR.
4. Elapsed time, Hybrid is faster than others for total encryption and decryption.
5. According the Entropy, AES and hybrid encryption have high entropy, making them resistant to statistical attacks unlike RSA encryption which has lower entropy.

## 4. Conclusion

Based on the results of the speed, strength, encryption accuracy, homogeneity and entropy criteria, we find that the proposed hybrid encryption algorithm is 2% faster than the rest, in addition to the efficiency, quality and effectiveness of encryption, which reaches the lowest value for the number 8, which means high encryption quality. As for the homogeneity of pixels in images and entropy values, the hybrid algorithm was the best than the rest, which outperformed the others in terms of entropy values and image pixel homogeneity, making it immune to statistical attacks. Summary of the study: It can be concluded that the combination of symmetric and asymmetric encryption techniques produces a highly efficient algorithm and develops encryption capabilities to reach an optimal way to secure and encrypt data.

## References


1. R. Sood and H. Kaur. A literature review on rsa, des and aes encryption algorithms. In *Emerging Trends in Engineering and Management*, pages 57–63, New Delhi, India, 2023. SCRS.
2. M. Alhayani and M. Al-Khiza'ay. Analyze symmetric and asymmetric encryption techniques by securing facial recognition system. In M. Ben Ahmed, B. A. Abdelhakim, B. K. Ane, and D. Rosiyadi, editors, *Emerging Trends in Intelligent Systems & Network Security*, volume 147 of *Lecture Notes on Data Engineering and Communications Technologies*. Springer, Cham, 2023.
3. M. M. Salih, B. M. Khaleel, N. H. Qasim, W. S. Ahmed, S. Kondakova, and M. Y. Abdullah. Capacity, spectral and energy efficiency of oma and noma systems. In *2024 35th Conference of Open Innovations Association (FRUCT)*, pages 652–658, Tampere, Finland, April 2024. IEEE.
4. S. M. Radhi and R. Ogla. In-depth assessment of cryptographic algorithms namely des, 3des, aes, rsa, and blowfish. *Iraqi Journal of Computers, Communications, Control and Systems Engineering*, 23(3):125–138, 2023.
5. O. Abd Qasim 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*, 10:100834, 2024.
6. G. Ashok. Modified image encryption algorithm based on chaotic cryptography. In *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pages 1506–1512, Coimbatore, India, November 2023. IEEE.
7. R. Modi, A. S. Jammoria, A. Pattiwar, A. Agrawal, and S. P. Raja. Secure system to secure crime data using hybrid: Rsa-aes and hybrid: Blowfish-triple des. *International Journal of Electronic Security and Digital Forensics*, 17(1-2):194–232, 2025.
8. S. Das and S. Namasudra. A novel hybrid encryption method to secure healthcare data in iot-enabled healthcare infrastructure. *Computers and Electrical Engineering*, 101:107991, 2022.
9. Y. Ortakci and M. Y. Abdullah. Performance analyses of aes and 3des algorithms for encryption of satellite images. In M. Ben Ahmed, İ. Rakıp Karaş, D. Santos, O. Sergeyeva, and A. A. Boudhir, editors, *Innovations in Smart Cities Applications Volume 4*, volume 183 of *Lecture Notes in Networks and Systems*. Springer, Cham, 2021.
10. H. T. Sihotang, S. Efendi, E. M. Zamzami, and H. Mawengkang. Design and implementation of rivest shamir adleman's (rsa) cryptography algorithm in text file data security. *Journal of Physics: Conference Series*, 1641(1):012042, 2020.
11. F. Hatem, S. R. Alatba, M. Y. Abdullah, T. Nimchenko, and A. Myronchenko. A method of removing rain or snow from a color image using matlab. In *2024 35th Conference of Open Innovations Association (FRUCT)*, pages 222–231, Tampere, Finland, April 2024. IEEE.

12. M. Y. Abdullah, L. B. Salman, A. S. Obaed, and A. M. Jawad. Innovations and applications of nanostructured energy storage materials. *Radioelectronics. Nanosystems. Information Technologies*, 16:779–792, 2024.

13. D. Chicco, V. Starovoitov, and G. Jurman. The benefits of the matthews correlation coefficient (mcc) over the diagnostic odds ratio (dor) in binary classification assessment. *IEEE Access*, 9:47112–47124, 2021.

14. M. Alhayani, N. Alallaq, and M. Al-Khiza'ay. Optimize one max problem by pso and csa. In X. S. Yang, R. S. Sherratt, N. Dey, and A. Joshi, editors, *Proceedings of Eighth International Congress on Information and Communication Technology*, volume 693 of *Lecture Notes in Networks and Systems*. Springer, Singapore, 2023.

15. P. V. Jaswanth, B. R. Reddy, M. S. P. Kumar, and M. J. P. Priyadarsini. Color image encryption using aes and rsa. *The International Journal of Engineering and Advanced Technology*, 9(5):547–550, 2020.

16. P. Sarosh, S. A. Parah, and G. M. Bhat. An efficient image encryption scheme for healthcare applications. *Multimedia Tools and Applications*, 81(5):7253–7270, 2022.

17. N. Sethi and S. Vijay. Comparative image encryption method analysis using new transformed-mapped technique. In *Conference on Advances in Communication and Control Systems (CAC2S 2013)*, pages 46–50. Atlantis Press, April 2013.

18. M. H. N. Azam, F. Ridzuan, and M. Sayuti. A new method to estimate peak signal to noise ratio for least significant bit modification audio steganography. *Pertanika Journal of Science & Technology*, 30(1), 2022.

19. A. C. Sparavigna. Entropy in image analysis. *Entropy*, 21(5):502, 2019.

20. A. Sheykhi. Barrow entropy corrections to friedmann equations. *Physical Review D*, 103(12):123503, 2021.

*Rana Raad Shaker Alnaily,*
*Department of Mathematics,*
*Collage of Education, University of Al-Qadisiyah,*
*Iraq.*
*E-mail address:* rana.alnaily@qu.edu.iq