Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 10, No. 1, February, Pp. 75-82

A hybrid encryption using advanced encryption standard and arnold scrambling for 3D color images

Wellia Shinta Sari[1], Erna Zuni Astuti*[1], Cahaya Jatmoko[1]
University of Dian Nuswantoro, Indonesia[1]

Article Info

Keywords:
Advanced Encryption Standard, Arnold Scrambling, Encryption, Entropy, UACI, NPCR

Article history:
Received: July 14, 2024
Accepted: November 04, 2024
Published: February 01, 2025

Cite:
W. S. Sari, E. Z. Astuti, and C. Jatmoko, "A Hybrid Encryption using Advanced Encryption Standard and Arnold Scrambling for 3D Color Images", *KINETIK*, vol. 10, no. 1, Feb. 2025.
https://doi.org/10.22219/kinetik.v10i1.2058

*Corresponding author.
Erna Zuni Astuti
E-mail address:
erna.zuni.astuti@dsn.dinus.ac.id

Abstract

Digital security ensuring the confidentiality and integrity of visual data remains a paramount challenge. The escalating sophistication of cyber threats necessitates robust encryption methods to safeguard sensitive information from unauthorized access and manipulation. Despite the development of various encryption techniques, inherent vulnerabilities exist within conventional methods that can be exploited by attackers. Therefore, this research aims to investigate the effectiveness of the combined approach of Arnold Scrambling and Advanced Encryption Standard (AES) in mitigating these vulnerabilities and providing a more secure solution. The primary goal of this research is to enhance the security of digital images by mitigating vulnerabilities associated with conventional encryption methods. Arnold Scrambling introduces chaotic mapping to disperse pixel values, while Advanced Encryption Standard (AES) provides robust cryptographic strength through its substitution-permutation network. By combining these methods in an ensemble fashion, the encryption process achieves heightened resilience against various cryptographic attacks. The proposed methodology was evaluated by using standard metrics including Unified Average Changing Intensity (UACI), Number of Pixels Change Rate (NPCR), and entropy analysis. Results indicate consistent performance across multiple test images, namely: Lena, Mandrill, Cameraman, and Plane with Unified Average Changing Intensity (UACI) averaging 33.6% and Number of Pixels Change Rate (NPCR) nearing 99.8%. Entropy values approached maximum, affirming the efficacy of the encryption in generating highly randomized outputs.

1. Introduction

Digital image security is the process of securing images by converting the original image data into a form that is not easily readable without the appropriate key or password [1], [2], [3], [4], [5]. This involves using cryptographic algorithms to convert the image pixels into a format that cannot be directly understood by unauthorized persons [6], [7]. One of the main goals of image encryption is to protect privacy and reduce the risk of unauthorized manipulation or access to sensitive visual data [8], [9], [10]. Digital security has become a significant issue affecting individuals, businesses and governments. Security attacks such as cyberattacks, malware, ransomware and identity theft are increasingly sophisticated and diverse, leading to significant financial losses and widespread privacy violations [11], [12]. In addition, with more and more sensitive data being stored and transmitted online, the need for robust and effective security protocols becomes more urgent. Inadequate digital security can pose significant risks, including operational disruption, loss of customer trust and serious legal and reputational impacts. While various methods exist for image encryption, a growing focus has been placed on combining techniques to enhance security, especially in an era where cyberattacks and data breaches are becoming more sophisticated.

Two prominent techniques in image encryption are Arnold Scrambling and the Advanced Encryption Standard (AES). Arnold scrambling, a chaotic transformation, is particularly useful for rearranging pixel positions within an image, making it nearly impossible for attackers to interpret the original data without the correct scrambling parameters [13]. On the other hand, AES, a symmetric encryption algorithm, is widely recognized for its high efficiency and strong security. It encrypts data in fixed block sizes using a series of substitution and permutation operations to ensure that the original information is not recoverable without the correct decryption key [14]. While these methods are powerful on their own, they each have limitations, such as the periodicity of Arnold scrambling and the key management complexities of AES [15], [16].

In response to these challenges, this research proposes a hybrid encryption approach that combines Arnold scrambling with AES to address the shortcomings of each method when used individually [17], [18], [19], [20]. The primary objective of this study is to enhance digital image security by leveraging the strengths of both techniques, namely Arnold scrambling's high diffusion properties and AES's robust encryption [17], [18]. This hybrid approach is expected to provide a more secure and efficient solution to the rising threat of cyberattacks targeting visual data. Specifically, the combination of these methods is designed to ensure that images remain protected even in cases of unauthorized access, by introducing both pixel-level scrambling and cryptographic encryption, thus complicating any attempts to reverse-engineer or decrypt the image.

Many researchers have leveraged Arnold scrambling in their investigations to enhance the security of digital images. Research [21] introduces an innovative chaos-based image encryption technique, utilizing recent advancements in multimedia data security. The study employed a logistic map and S-box for improved key expansion and incorporated ACM for image permutation, effectively scrambling the image data. Research [22] presents a novel image encryption and decryption method combining Arnold cat transformation and elliptic curve hill cipher cryptography. The Arnold cat transformation was used to perform chaotic pixel mapping, while the elliptic curve Hill cipher provided robust security through the use of elliptic curves in the encryption process. Research [23] introduces a multi-layered approach combining RMAC, RP2DFrHT, and a two-dimensional Arnold map for enhanced image encryption. Initially, RMAC secured both coordinate and geometrical domains, ensuring that pixel knowledge alone is insufficient for decryption. The second stage used RP2DFrHT to convert complex-valued coefficients to real-valued ones, facilitating easier display, storage, and transmission. Lastly, the 2D Arnold map was applied to further enhance security and expand the key space.

Different from three related studies above, this study offers a new approach in image encryption based on the combination of Arnold scrambling with Advanced Encryption Standard (AES). This method utilizes the strength of Arnold scrambling in providing high diffusion and chaos to scramble image pixels, making them difficult to understand without the right key. On the other hand, AES is known for its strong encryption capabilities and efficiency in securing data. This hybrid approach is expected to overcome the weaknesses of each method when used separately and provide a more practical solution to increasingly complex cybersecurity threats.

The remainder of this paper is organized as follows: Section 2 provides a detailed explanation of the hybrid encryption methodology, including the integration of Arnold scrambling and AES. Section 3 discusses the experimental setup and presents the results of applying the hybrid encryption technique to various digital images. Section 4 offers an analysis of the findings, comparing the security and efficiency of the hybrid method with other encryption approaches. Finally, Section 5 concludes with a summary of the contributions, implications for future research, and potential real-world applications of the proposed method.

2. Research Method

The encryption method in this study involves a combination of Arnold Scrambling and Advanced Encryption Standard (AES). Arnold Scrambling was selected for its ability to introduce high levels of diffusion by randomizing pixel positions based on chaotic mappings, while AES was chosen for its strong cryptographic properties, providing robust security through well-established encryption standards. This combination aims to address the limitations of each method when used independently, ensuring higher levels of security for digital images.

The process begins by separating the image into its three primary color components: red, green, and blue (RGB). Each component undergoes Arnold Scrambling using Arnold’s cat map, a well-documented technique that effectively disrupts pixel positions in a reversible manner, making the image unrecognizable without proper decryption keys. After scrambling, the three-color components are recombined and then encrypted using AES with a specific encryption key. Arnold Scrambling introduces chaos into the pixel arrangement, which strengthens the encryption process by increasing resistance to cryptographic attacks that rely on pixel correlation. AES, with its substitution-permutation network, further reinforces the encryption by altering the pixel values, making brute-force attacks infeasible. The rationale for combining these techniques lies in the complementary nature of Arnold Scrambling's diffusion properties and AES's confusion capabilities. Together, they create a highly secure encryption scheme that is computationally efficient while enhancing security robustness.

The encryption process was tested on standard benchmark images, including Lena, Mandrill, Cameraman, and Plane, to evaluate its performance using established metrics like UACI, NPCR, and entropy. The flow of the proposed encryption method is illustrated in Figure 1, with additional layers of AES encryption depicted in Figure 3 to clarify how the AES steps modify the state matrix.

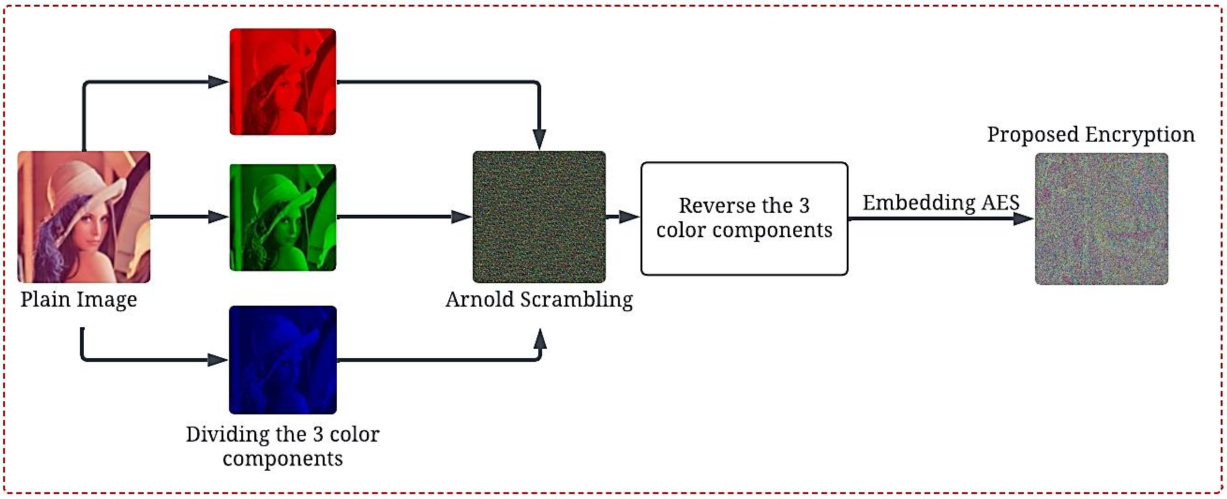

Plain Image
Dividing the 3 color components
Arnold Scrambling
Reverse the 3 color components
Embedding AES
Proposed Encryption

Figure 1. Proposed Encryption

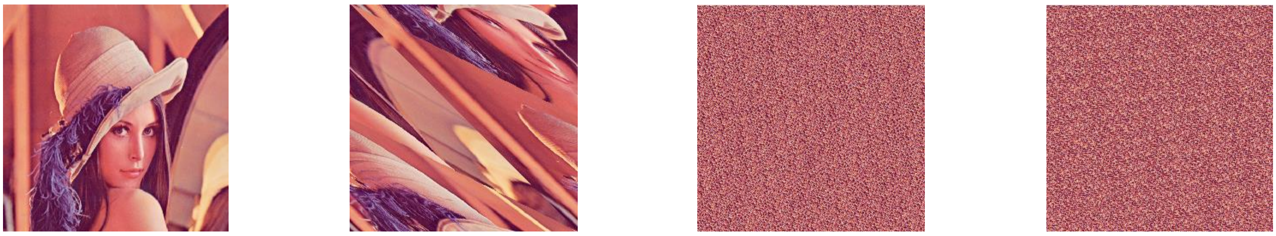
2.1 Arnold Scrambling

Arnold Scrambling is a technique used in image encryption to randomize the position of pixels in an image, resulting in an image that cannot be recognized without performing a reverse decryption process [24], [25]. This technique is named after mathematician Vladimir Arnold, who introduced the concept through the Arnold's cat map. An Arnold’s cat map is a repeated linear transformation of the pixel coordinates in an image, which causes a cyclical shift in the pixel positions [26]. The Arnold Scrambling process begins by applying a mathematical transformation to the coordinates of each pixel in the original image [27]. Each new coordinate is calculated using a specific equation that combines addition and modulo operations. After a certain number of iterations, the positions of the pixels in the image become highly scrambled, making the resulting image appear to be a random collection of pixels with no discernible pattern. However, because this process is deterministic and reversible, the original image can be recovered by applying the reverse transformation with the same number of iterations. The Arnold scrambling equation can be seen in Equation 1 and Equation 2. For a given pixel at coordinates (x, y) in image $(N\ x\ N)$, the new coordinates (x', y') after Arnold randomization iteration are calculated using Equation 1, and to descramble the image and recover the original pixel positions, the inverse transformation are calculated using Equation 2.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \tag{1}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \bmod N \tag{2}$$

The Arnold scrambling results in 1x, 10x, and 100x iterations can be seen in Figure 2. This figure shows that the original image undergoes significant changes in pixel positions after going through different numbers of iterations. On the first iteration (1x), the image begins to show signs of clutter, while on the tenth iteration (10x), the clutter increases and the original pattern becomes increasingly difficult to discern. After one hundred iterations (100 times), the image becomes very blurred, making it almost unrecognizable without appropriate backscatter processing.



(a) Plain Image (Lena.bmp) (b) 1x Iteration (c) 10x Iteration (d) 100x Iteration

Figure 2. Arnold Scrambling Per-iteration

Cite: W. S. Sari, E. Z. Astuti, and C. Jatmoko, “A Hybrid Encryption using Advanced Encryption Standard and Arnold Scrambling for 3D Color Images”, KINETIK, vol. 10, no. 1, Feb. 2025. https://doi.org/10.22219/kinetik.v10i1.2058

2.2 Advanced Encryption Standard (AES)

AES works by dividing data into fixed-size blocks (128 bits) and encrypting each block using a cryptographic key that can be 128, 192, or 256 bits long [28], [29]. The AES encryption process involves a series of transformations such as SubBytes, ShiftRows, MixColumns, and AddRoundKey that are repeated in multiple rounds to increase security [30], [31]. In the context of image encryption, combining AES with Arnold scrambling provides double protection. Arnold scrambling first scrambles the positions of pixels in the image, making them difficult to recognize, and then AES secures this scrambled data with strong encryption. This combination ensures that even if one layer of security is compromised, the other layers still protect the image from unauthorized access. The mathematical equations for AES can be seen in Equations 3–6.

$$SubBytes(S) = \begin{pmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{pmatrix} \tag{3}$$

$$ShiftRows(S) = \begin{pmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,2} & S'_{1,3} & S'_{1,0} \\ S'_{2,2} & S'_{2,3} & S'_{2,0} & S'_{2,1} \\ S'_{3,3} & S'_{3,0} & S'_{3,1} & S'_{3,2} \end{pmatrix} \tag{4}$$

$$MixColumns(S) = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S'_{0,0} \\ S'_{1,0} \\ S'_{2,0} \\ S'_{3,0} \end{pmatrix} \tag{5}$$

$$AddRoundKey(S, K) = S \oplus K \tag{6}$$

By applying the equations above, the AES layer can be seen in Figure 3. The figure illustrates the data transformation process that occurs during the encryption process using AES. Steps such as SubBytes, ShiftRows, MixColumns, and AddRoundKey are visually represented in the diagram to clarify how each step modifies the state matrix at each round of encryption.

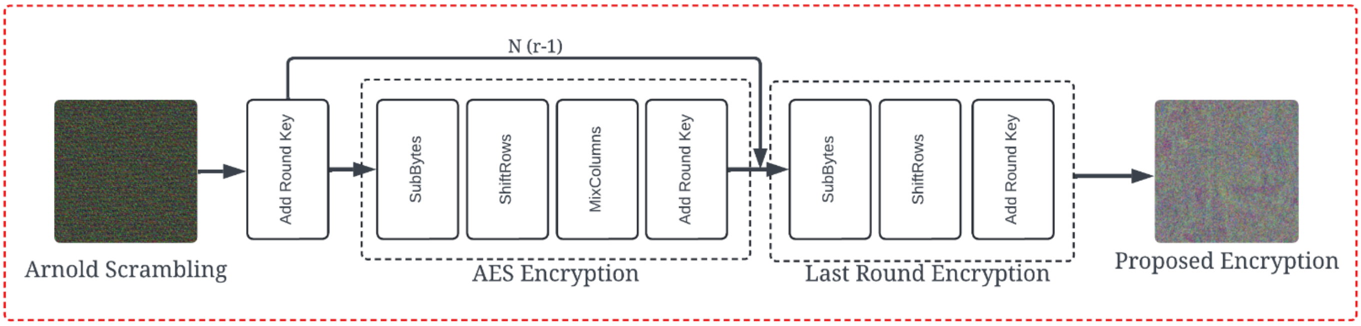
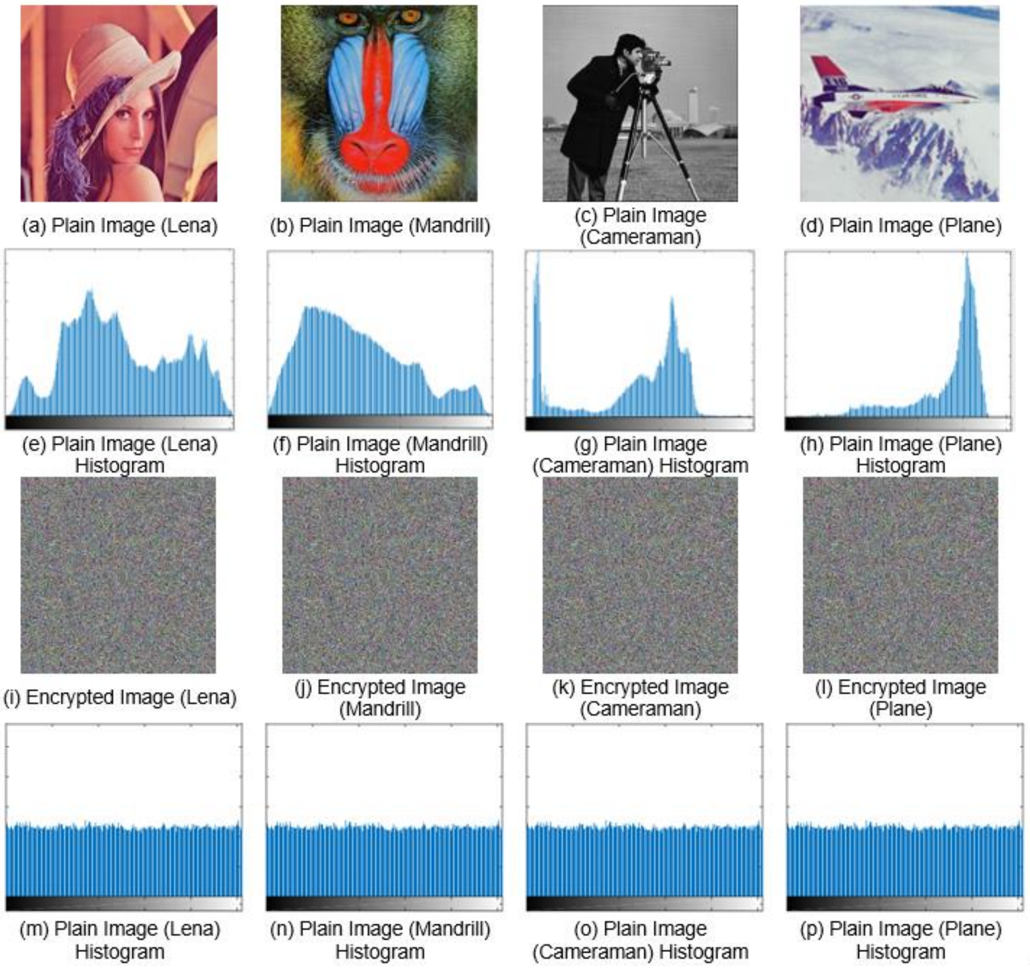


Figure 3. AES Layers

3. Results and Discussion

In this study, the plain images used include four images namely Lena, Mandrill, Cameraman and Plane. In this test, an RGB image with a resolution of 256 x 256 x 3 was used. To measure the image encryption performance, analysis is performed using histogram, NPCR, UACI and Entropy. The entire testing and analysis process is performed using MATLAB 2020a software, which provides many functions and tools necessary to implement and evaluate the proposed encryption algorithm. Experimental results based on the proposed method are shown in Figure 4. Results depicted in Figure 4 undergoes a multi-layered encryption process utilizing both Arnold Scrambling and AES, as detailed in Algorithm 1 and Algorithm 2, respectively. Algorithm 1, representing Arnold Scrambling, disperses the pixel positions through chaotic mapping, thereby introducing a high level of randomness and initial security. Following this, Algorithm 2, which represents AES, encrypts the scrambled image, ensuring robust cryptographic security.



(a) Plain Image (Lena) (b) Plain Image (Mandrill) (c) Plain Image (Cameraman) (d) Plain Image (Plane)

(e) Plain Image (Lena) Histogram (f) Plain Image (Mandrill) Histogram (g) Plain Image (Cameraman) Histogram (h) Plain Image (Plane) Histogram

(i) Encrypted Image (Lena) (j) Encrypted Image (Mandrill) (k) Encrypted Image (Cameraman) (l) Encrypted Image (Plane)

(m) Plain Image (Lena) Histogram (n) Plain Image (Mandrill) Histogram (o) Plain Image (Cameraman) Histogram (p) Plain Image (Plane) Histogram

Figure 4. Results Experiment

1st Algorithm: Arnold Scrambling

```
$Input$: Image matrix img, Number of iterations iter
$Output$: Scrambled image matrix $scrambled\_img$

$N \leftarrow$ number of rows in img
$M \leftarrow$ number of columns in img
$scrambled\_img \leftarrow img$

for $i$ from 1 to iter do
    $temp\_img \leftarrow scrambled\_img$
    for $x$ from $0$ to $N - 1$ do
        for $y$ from $0$ to $M - 1$ do
            $new\_x \leftarrow (x + y) \bmod N$
            $new\_y \leftarrow (x + 2 * y) \bmod M$
            $scrambled\_img[new\_x][new\_y] \leftarrow temp\_img[x][y]$
        end for
    end for
end for
return $scrambled\_img$
```

2nd Algorithm: AES

```
$Input$: Plaintext block P, Cipher key K
$Output$: Encrypted block C

SubBytes (state):
    for each byte in state do
        $byte = S - box[byte]$
    end for
ShiftRows (state):
    for each row r in state do
        $left - rotate\ row\ r\ by\ r\ bytes$
    end for
MixColumns (state):
    for each column c in state do
        $column\ c = MultiplyWithMatrix(column\ c, fixed\_matrix)$
    end for
AddRoundKey (state, roundKey):
    for each byte in state do
        $byte = byte\ XOR\ roundKey$
    end for
```

3.1 UACI and NPCR Evaluation

UACI measures the average difference in pixel intensities between the original image and the encrypted image, giving an idea of how much the pixel values change after the encryption [32], [33]. On the other hand, NPCR measures the percentage of pixels that change value between the original image and the encrypted image when small changes occur in the original image, thereby indicating the sensitivity of the encryption algorithm to such changes. Based on the UACI and NPCR equations, it can be seen in Equation 7 and Equation 8. Results of the image encryption performance are shown in Table 1. This table shows the UACI and NPCR values for each test image, namely Lena, Mandrill, Cameraman, and Plane.

$$UACI = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{I(i,j) \oplus K(i,j)}{L}\right| \times 100 \tag{7}$$

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{I(i,j)-K(i,j)}{I(i,j)}\right| \times 100 \tag{8}$$

Based on the analysis for four test images, each image obtained UACI of 33.6% and NPCR of 99.8%. The NPCR value approaching 100% indicates that most pixels in the image change their values after the encryption process.

Table 1. Results of UACI and NPCR

Researcher	Method	Tested Image	UACI (%)	NPCR (%)
Our Study	Ensemble Arnold Scrambling + AES	Lena	33.61	99.82
		Mandrill	33.61	99.81
		Cameraman	33.61	99.82
		Plane	33.58	99.80
[21]	Ensemble Arnold Scrambling + S-Box	Lena	33.40	99.62
		Mandrill	33.35	99.60
		Cameraman	33.54	99.61
[22]	Ensemble Arnold Scrambling + Hill Cipher	Lena	33.48	99.78
		Mandrill	33.42	99.61

3.2 Entropy Analysis

Entropy analysis is a method used to measure the degree of randomness or chaos in an encrypted image, reflecting the degree of uncertainty in the information contained in the data [34], [35]. The higher the entropy value, the better the encryption quality, as it indicates that the encrypted data is more random and unpredictable. The entropy equation can be seen in Equation 9. The results of the entropy analysis can be seen in Table 2. This table shows the entropy values for the encrypted test images including Lena, Mandrill, Cameraman, and Plane. Based on the analysis for four test images, the entropy value almost reaches the maximum value of 8, such as 7.9999 for Lena, Mandrill and Plane, and 7.9997 for Cameraman, indicating that the encrypted image has a very random and irregular pixel distribution.

$$Entropy = -\sum_{i=0}^{255} p\,(x_i)\,log_2\,p\,(x_i) \tag{9}$$

Table 2. Results of Entropy Analysis

Research	Method	Tested Image	Entropy (AVG)
Our Study	Ensemble Arnold Scrambling + AES	Lena	7.9999
		Mandrill	7.9999
		Cameraman	7.9997
		Plane	7.9999
[21]	Ensemble Arnold Scrambling + S-Box	Lena	7.9990
		Mandrill	7.9997
		Cameraman	7.9989
[22]	Ensemble Arnold Scrambling + Hill Cipher	Lena	7.9989
		Mandrill	7.9982

4. Conclusion

In this study, the proposed hybrid approach combining Arnold Scrambling and AES for image encryption was rigorously evaluated across four test images: Lena, Mandrill, Cameraman, and Plane. The results of this evaluation demonstrated the effectiveness of the encryption scheme through key metrics such as the Unified Average Changing

Intensity (UACI) and the Number of Pixels Change Rate (NPCR). With UACI values consistently around 33.6% and NPCR values approximately 99.8%, the algorithm exhibited high sensitivity to pixel changes, ensuring that even small alterations in the input led to significant modifications in the encrypted output, thus strengthening resistance to differential cryptanalysis. Additionally, the entropy analysis, with values approaching 8 for each image, indicated a near-optimal level of randomness in the encrypted images. This suggests that the combination of Arnold's chaotic pixel diffusion and AES's robust cryptographic transformations resulted in highly randomized and secure outputs, further reducing the likelihood of pattern recognition by attackers. These findings support the research objective by confirming that the hybrid method successfully addresses the limitations inherent in using Arnold Scrambling and AES independently. By leveraging the strengths of both techniques—Arnold's chaotic scrambling of pixels and AES's cryptographic efficiency—this combined approach offers an enhanced level of security for digital images without sacrificing computational efficiency. The improved diffusion and confusion properties make the proposed method particularly suitable for applications requiring high security, such as secure image transmission, encrypted data storage, and protection of personal privacy in digital communications.

For future research, there is a need to explore further enhancements to the encryption process, including optimizing the algorithm's performance for real-time applications and exploring the integration of multi-layered encryption techniques. Addressing resilience against more advanced cryptographic attacks, such as quantum-based threats, will be crucial in continuing to adapt to the evolving landscape of digital security challenges. The findings of this research lay the groundwork for these future developments, which are essential for ensuring robust protection in the face of increasingly complex cybersecurity threats.

References

[1] F. Varghese and P. Sasikala, "A Detailed Review Based on Secure Data Transmission Using Cryptography and Steganography," Apr. 01, 2023, *Springer*. https://doi.org/10.1007/s11277-023-10183-z

[2] A. Jan, S. A. Parah, M. Hussan, and B. A. Malik, "Double layer security using crypto-stego techniques: a comprehensive review," Jan. 01, 2022, *Springer Science and Business Media Deutschland GmbH*. https://doi.org/10.1007/s12553-021-00602-1

[3] M. S. Taha, M. S. Mohd Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of Steganography and Cryptography: A short Survey," in *IOP Conference Series: Materials Science and Engineering*, Institute of Physics Publishing, Jun. 2019. https://doi.org/10.1088/1757-899X/518/5/052003

[4] V. Sathananthavathi, K. Ganesh Kumar, and M. Sathish Kumar, "Secure visual communication with advanced cryptographic and ımage processing techniques," *Multimed Tools Appl*, 2023. https://doi.org/10.1007/s11042-023-17224-6

[5] W. Alexan, N. Alexan, and M. Gabr, "Multiple-Layer Image Encryption Utilizing Fractional-Order Chen Hyperchaotic Map and Cryptographically Secure PRNGs," *Fractal and Fractional*, vol. 7, no. 4, Apr. 2023. https://doi.org/10.3390/fractalfract7040287

[6] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "A Good Performance OTP encryption image based on DCT-DWT steganography," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 15, no. 4, pp. 1987–1995, Dec. 2017. https://doi.org/10.12928/TELKOMNIKA.v15i4.5883

[7] C. A. Sari, M. H. Dzaki, E. H. Rachmawanto, R. R. Ali, and M. Doheir, "High PSNR Using Fibonacci Sequences in Classical Cryptography and Steganography Using LSB," *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 4, pp. 568–580, 2023. https://doi.org/10.22266/ijies2023.0831.46

[8] D. R. I. M. Setiadi, E. H. Rachmawanto, and R. Zulfiningrum, "Medical Image Cryptosystem using Dynamic Josephus Sequence and Chaotic-hash Scrambling," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 9, pp. 6818–6828, Oct. 2022. https://doi.org/10.1016/j.jksuci.2022.04.002

[9] E. A. Sofyan, C. A. Sari, H. Rachmawanto, and R. D. Cahyo, "High-Quality Evaluation for Invisible Watermarking Based on Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD)," *Advance Sustainable Science, Engineering and Technology (ASSET)*, vol. 6, no. 1, 2024. https://doi.org/10.26877/asset.v6i1.17186

[10] G. Ardiansyah, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm," in *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 2017, pp. 249–254. https://doi.org/10.1109/ICITISEE.2017.8285505

[11] M. Rohini, M. A. Srikanth, M. Prajwal, P. R. Kumar, M. Basavaraj, and M. U. Vinay, "Advanced Data Security Using Modulo Operator and LSB Method," *Journal of Scholastic Engineering Science and Management*, vol. 2023, no. 5, pp. 26–37, 2023. https://doi.org/10.5281/zenodo.7890771ï

[12] A. Mozo, A. Karamchandani, L. de la Cal, S. Gómez-Canaval, A. Pastor, and L. Gifre, "A Machine-Learning-Based Cyberattack Detector for a Cloud-Based SDN Controller," *Applied Sciences (Switzerland)*, vol. 13, no. 8, Apr. 2023. https://doi.org/10.3390/app13084914

[13] E. J. G, H. M. A, and F. H. M. S, "Enhanced Security: Implementation of Hybrid Image Steganography Technique using Low-Contrast LSB and AES-CBC Cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, p. 2022, 2022. https://doi.org/10.14569/IJACSA.2022.01308104

[14] J. Shankar and C. Nandini, "Hybrid Hyper Chaotic Map with LSB for Image Encryption and Decryption," *Scalable Computing: Practice and Experience*, vol. 23, no. 4, pp. 181–192, Dec. 2022. https://doi.org/10.12694/scpe.v23i4.2018

[15] H. Liu, B. Zhao, and L. Huang, "Quantum image encryption scheme using Arnold transform and S-box scrambling," *Entropy*, vol. 21, no. 4, Apr. 2019. https://doi.org/10.3390/e21040343

[16] P. Bagane and S. Kotrappa, "Enriching aes through the key generation from genetic algorithm," *Indian Journal of Computer Science and Engineering*, vol. 12, no. 4, pp. 955–963, Jul. 2021. https://doi.org/10.21817/indjcse/2021/v12i4/211204141

[17] S. Srisakthi and A. P. Shanthi, "Towards the Design of a Stronger AES: AES with Key Dependent Shift Rows (KDSR)," *Wirel Pers Commun*, vol. 114, no. 4, pp. 3003–3015, Oct. 2020. https://doi.org/10.1007/s11277-020-07514-9

[18] W. Alexan, A. Hamza, and H. Medhat, "An AES Double–Layer Based Message Security Scheme," in *2019 International Conference on Innovative Trends in Computer Engineering (ITCE)*, IEEE, Feb. 2019, pp. 86–91. https://doi.org/10.1109/ITCE.2019.8646461

[19] K. N. Madhusudhan and P. Sakthivel, "A secure medical image transmission algorithm based on binary bits and Arnold map," May 01, 2021, *Springer Science and Business Media Deutschland GmbH*. https://doi.org/10.1007/s12652-020-02028-5

[20] F. Masood *et al.*, “A novel image encryption scheme based on Arnold cat map, Newton-Leipnik system and Logistic Gaussian map,” *Multimed Tools Appl*, vol. 81, no. 21, pp. 30931–30959, Sep. 2022. https://doi.org/10.1007/s11042-022-12844-w

[21] D. E. Supriyo, N. Bhanja, S. K. Dhara, S. Paul, and S. Das, “Color image encryption scheme based on key dependent s-box and arnold’s cat map,” *International Journal of Engineering Research and Technology (IJERT)*, 2021.

[22] D. Vamsi and R. Ch, “Color Image Encryption Based on Arnold Cat Map-Elliptic Curve Key and A Hill Cipher,” *J Theor Appl Inf Technol*, vol. 15, no. 9, 2024.

[23] S. Sabir and V. Guleria, “Multi-layer color image encryption using random matrix affine cipher, RP2DFrHT and 2D Arnold map,” *Multimed Tools Appl*, vol. 80, no. 18, pp. 27829–27853, Jul. 2021. https://doi.org/10.1007/s11042-021-11003-x

[24] H. Liu, B. Zhao, and L. Huang, “Quantum image encryption scheme using Arnold transform and S-box scrambling,” *Entropy*, vol. 21, no. 4, p. 343, 2019. https://doi.org/10.3390/e21040343

[25] K. M. Hosny, S. T. Kamal, and M. M. Darwish, “A color image encryption technique using block scrambling and chaos,” *Multimed Tools Appl*, vol. 81, no. 1, pp. 505–525, 2022. https://doi.org/10.1007/s11042-021-11384-z

[26] K. Kumar, S. Roy, U. Rawat, and S. Malhotra, “IEHC: An efficient image encryption technique using hybrid chaotic map,” *Chaos Solitons Fractals*, vol. 158, p. 111994, 2022. https://doi.org/10.1016/j.chaos.2022.111994

[27] H. Tora, E. Gokcay, M. Turan, and M. Buker, “A generalized Arnold’s Cat Map transformation for image scrambling,” *Multimed Tools Appl*, vol. 81, no. 22, pp. 31349–31362, 2022. https://doi.org/10.1007/s11042-022-11985-2

[28] M. N. Alenezi, H. Alabdulrazzaq, H. M. Alhatlani, and F. A. Alobaid, “On the performance of AES algorithm variants,” *International Journal of Information and Computer Security*, vol. 23, no. 3, pp. 322–337, 2024. https://doi.org/10.1504/IJICS.2024.138494

[29] V. Kolate and R. B. Joshi, “An information security using DNA cryptography along with AES algorithm,” *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 1S, pp. 183–192, 2021.

[30] R. H. Prayitno, S. A. Sudiro, S. Madenda, and S. Harmanto, “A modified MixColumn-InversMixColumn in AES algorithm suitable for hardware implementation using FPGA device,” *Communications in Science and Technology*, vol. 8, no. 2, pp. 198–207, 2023. https://doi.org/10.21924/cst.8.2.2023.1257

[31] M. Bedoui, H. Mestiri, B. Bouallegue, B. Hamdi, and M. Machhout, “An improvement of both security and reliability for AES implementations,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 9844–9851, 2022. https://doi.org/10.1016/j.jksuci.2021.12.012

[32] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, “A new algorithm for digital image encryption based on chaos theory,” *Entropy*, vol. 23, no. 3, p. 341, 2021. https://doi.org/10.3390/e23030341

[33] F. Naz, I. A. Shoukat, R. Ashraf, U. Iqbal, and A. Rauf, “An ASCII based effective and multi-operation image encryption method,” *Multimed Tools Appl*, vol. 79, pp. 22107–22129, 2020. https://doi.org/10.1007/s11042-020-08897-4

[34] N. Chaudhary, T. B. Shahi, and A. Neupane, “Secure image encryption using chaotic, hybrid chaotic and block cipher approach,” *J Imaging*, vol. 8, no. 6, p. 167, 2022. https://doi.org/10.3390/jimaging8060167

[35] M. Ahmad *et al.*, “An image encryption algorithm based on new generalized fusion fractal structure,” *Inf Sci (N Y)*, vol. 592, pp. 1–20, 2022. https://doi.org/10.1016/j.ins.2022.01.042