Advance Sustainable Science, Engineering and Technology (ASSET)
Vol. 8, No.4, October 2026, pp. 0260403-01 ~ 0260403-013
ISSN: 2715-4211 DOI: https://doi.org/10.26877/asset.v8i4.3085

Lightweight Dual-Layer Chaotic Image Encryption Using Arnold Cat Map and Henon Zigzag Diffusion

Chaerul Umam*[1], Abdussalam[1], Arif Nursetyo[2], Bambang Sugiarto[2], Husain Md Mehedul Islam[3]

[1]Faculty of Computer Science, Universitas Dian Nuswantoro, Imam Bonjol No 207, Pendrikan Kidul, Semarang 50131, Central Java, Indonesia

[2]Faculty of Technology and Information, Universitas Catur Insan Cendekia, Kesambi No 202, Cirebon 45134, West Java, Indonesia

[3]Software Engineer, The MathWork Inc., Massachusetts, United States

*chaerul@dsn.dinus.ac.id

Abstract. Digital image transmission over open networks raises significant security concerns due to the high correlation and predictable statistical properties of image data. Existing chaotic encryption schemes based on Arnold Cat Map (ACM) and Henon mapping often suffer from high computational cost, parameter sensitivity, or reliance on complex multi-stage designs. To address these limitations, this study proposes a lightweight dual-layer chaotic image encryption framework that integrates ACM-based pixel permutation with Henon Zigzag diffusion. The first layer applies ACM to disrupt spatial correlations, while the second layer embeds a Henon-based chaotic sequence into a zigzag traversal to enhance both confusion and diffusion. Experimental results demonstrate that the proposed method achieves strong security performance, with an average PSNR of 8.40 dB for cipher images, UACI of 33.67%, NPCR of 99.71%, and near-zero correlation coefficients across RGB channels, while maintaining a low average execution time of 1.80 s. These results indicate that the method produces highly randomized cipher images with strong resistance to statistical and differential attacks. Furthermore, the reduced computational complexity highlights its suitability as a lightweight and efficient solution for secure multimedia transmission in practical digital communication systems.

Keywords: Arnold Cat Map, Chaotic Cryptography, Henon Zigzag, Image Encryption, Lightweight Encryption, Multimedia Security.

(Received 2025-12-05, Revised 2026-04-13, Accepted 2026-06-18, Available Online by 2026-08-29)

1. Introduction

Problems surrounding the misuse of digital images have gained considerable attention in cybersecurity. Cases of manipulation, tampering, and even simple unauthorized sharing are no longer rare, and these practices raise serious concerns about privacy as well as the credibility of visual information available online [1], [2]. Study [3] reported that nearly 32 percent of medical image datasets circulating on digital platforms were vulnerable to tampering. This figure is striking because it directly affects the accuracy of medical diagnoses and the trust placed in clinical systems [4], [5], [6]. On the social media side, a study reported in [7] found that around 38 percent of image-related breaches recorded in 2020 were linked to unauthorized edits, alterations, or the misuse of metadata, all of which have been exploited for fraud, misinformation, and identity theft. Conventional cryptographic techniques, originally designed primarily for textual data, may be less efficient when applied directly to image data due to its distinct structure and statistical properties [8], [9]. These findings explain why recent research has been shifting toward stronger models, particularly hybrid and multi-layer encryption schemes that are better equipped to address the growing scale of image-based threats.

This research proposes a lightweight dual-layer chaotic encryption framework that integrates Arnold Cat Map (ACM) with Henon Zigzag traversal in a unified permutation–diffusion structure. Unlike existing ACM–Henon-based approaches that rely on multiple chaotic maps or additional cryptographic components [10], [11], [12], the proposed method embeds the Henon Zigzag mechanism directly into the second layer to achieve nonlinear diffusion with reduced structural complexity [13], [14]. This design minimizes iteration dependency and avoids excessive parameterization while maintaining strong confusion and diffusion properties [15], [16].

Prior works highlight similar approaches and their shortcomings. Despite the extensive use of ACM combined with chaotic diffusion techniques, several limitations remain. Existing approaches often rely on multi-stage or hybrid designs that increase computational complexity, require multiple control parameters, or depend on repeated iterations to achieve sufficient randomness. These factors not only reduce efficiency but also limit reproducibility and scalability in practical implementations. Therefore, there is a need for a more efficient and structurally simplified chaotic encryption framework that maintains strong security properties while reducing computational overhead.

Study [17] combined ACM with hybrid chaotic strategies and AES, achieving PSNR 29.74 dB, NPCR 99.62%, and UACI 33.46%; although robust, its layered chaos–AES design produces high computational overhead. Study [18] used multiple chaotic maps with ACM as the first permutation stage, reporting NPCR 99.61%, UACI 33.41%, and cipher PSNR below 10 dB (recovering to 30.12 dB after decryption); however, its dependence on several chaos parameters makes the system highly sensitive and less reproducible. Study [19] integrated ACM with key substitution and DWT, yielding NPCR 99.58%, UACI 33.37%, and PSNR 31.08 dB, but the frequency-domain operations increase computational cost. Study [20] applied ACM-based block scrambling followed by chaotic diffusion, achieving high cipher MSE, decrypted PSNR 28.92 dB, NPCR 99.63%, and UACI 33.29%; despite its simplicity and strong security, it requires multiple scrambling iterations that slow processing.

The research gap across these studies centers on ACM's effectiveness but persistent inefficiencies: high computation from AES layering [17], parameter sensitivity in multi-chaos designs [18], heavy DWT processing [19], and iteration overhead in block scrambling [20]. Addressing these limitations, this work introduces a novel double-layer model that embeds the Henon Zigzag transform directly into ACM. ACM performs pixel permutation in the first layer, while Henon Zigzag provides nonlinear traversal in the second layer, ensuring that even partial reversal of one transformation cannot bypass the compounded complexity. The method reduces reliance on external cryptographic primitives, minimizes iteration overhead, enhances chaos strength, and offers a better balance between security and computational cost.

2. Methods

2.1. Arnold Cat Map

Arnold Cat Map (ACM) is a classical, area-preserving linear automorphism that is widely used in image encryption as a deterministic, invertible, and strongly mixing permutation operator [8], [21], [22]. In image encryption it is deployed to permute pixel coordinates (confusion) while preserving pixel values; because ACM is linear and periodic on finite lattices, it must be combined with a nonlinear diffusion stage (e.g., Henon Zigzag) to produce full confusion + diffusion [21]. Consider a digital image of size $N \times N$, where each pixel is represented by its spatial coordinates (i, j), with $i, j \in \{0,1, \dots, N-1\}$. The ACM transformation is defined in Eq. (1) with linear mapping over modular arithmetic as seen below.

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} mod\ N \tag{1}$$

Here, (i, j) represents the original coordinate of a pixel, while (i', j') is the permuted coordinate after one iteration of ACM. Since the transformation is performed modulo N, the resulting coordinates are always valid within the image lattice. Mathematically, the ACM belongs to the class of area-preserving linear automorphisms on the torus Z_N^2, with determinant equal to one as calculated using Eq. (2), ensuring that the mapping is bijective and reversible. This reversibility is fundamental in encryption, as it guarantees that the original image can always be reconstructed by applying the inverse transformation.

$$det \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = (1)(2) - (1)(1) = 1 \tag{2}$$

$$\begin{bmatrix} i^{(k)} \\ j^{(k)} \end{bmatrix} = A^k \begin{bmatrix} i \\ j \end{bmatrix} mod\ N \tag{3}$$

The scrambling effect of ACM is controlled by the number of iterations, denoted as k. The general k-th iteration of ACM can be calculated using Eq. (3). The closed-form of A^k can be expressed using Fibonacci numbers (F_N), where $F_1 = 1$, $F_2 = 1$, and $F_{n+1} = F_n + F_{n-1}$. Specifically, $A^k = \begin{bmatrix} F_{2k-1} & F_{2k} \\ F_{2k} & F_{2k+1} \end{bmatrix}$, the coordinate transformation after k iterations as calculated using Eq. (4).

$$\begin{bmatrix} i^{(k)} = (F_{2k-1} \cdot i + F_{2k} \cdot j) mod\ N \\ j^{(k)} = (F_{2k-1} \cdot i + F_{2k} \cdot j)\ mod\ N \end{bmatrix} \tag{4}$$

$$i^{(1)} = (i + j)\ mod\ N,\ \ j^{(1)} = (i + 2j)\ mod\ N \tag{5}$$

This calculation demonstrates that ACM is essentially a linear recurrence system embedded with Fibonacci growth, which explains its chaotic mixing properties as the iteration count increases [23]. The correlation between neighboring pixels is progressively destroyed, thereby enhancing the confusion property of the cipher. In this study, three iteration counts are examined to observe the trade-off between computational efficiency and scrambling effectiveness. At this stage, the scrambling is minimal and some structural resemblance to the original image may persist.

As calculated in Eq. (5) using a small number of iterations produces a light permutation, which is useful for demonstrating the basic effect of the ACM but is insufficient for high-security applications. When $k = 5$ will produce efficiency and strong scrambling, destroying most visible features of the original image. For final iteration using $k = 10$ achieves near-complete randomization, ideal for maximizing cryptographic strength, but at the cost of higher computation and potential sensitivity to modulus effects. The results of each iteration can be seen in Figure 1. It is also important to note that ACM exhibits periodicity: after a certain number of iterations T, the image returns to its original state. The value of T depends on the image size N, and typically ranges between N and 3N. This property provides an implicit upper bound on the number of effective iterations.

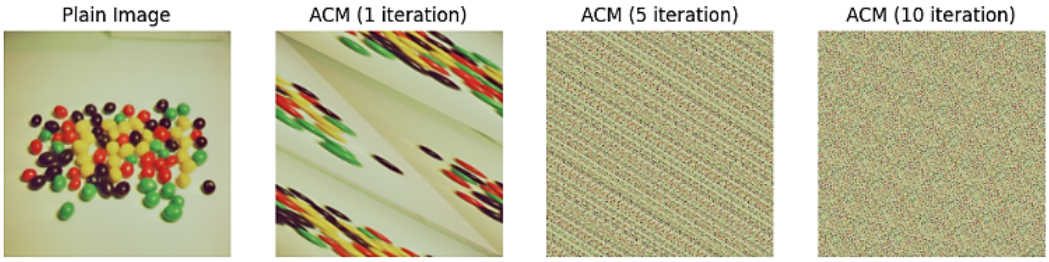


Figure 1. The results of ACM each iteration

2.2. Henon Zigzag Traversal

After completing the first stage of encryption using the Arnold Cat Map (ACM) with 10 iterations, the resulting scrambled image $I_{ACM}^{(10)}$ is subjected to the second embedding stage, namely the Henon Zigzag Traversal (HZT) [10], [13], [21]. This stage integrates the chaotic key stream of the Henon map with the irregular zigzag traversal to reinforce confusion and diffusion in the cipher image [24]. The Henon map is a two-dimensional discrete dynamical system as calculated using Eq. (6).

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \tag{6}$$

Where parameters a and b control the chaotic behavior, and $(x0, y0)$ serve as initial conditions (secret keys). For this study, values $a = 1.4$ and $b = 0.3$ are chosen, which yield a strongly chaotic regime, and the result can be seen in Figure 2(a). From this system, a chaotic sequence $\{x_n\}$ of length $N \times N$ is generated, where N is the image dimension. The sequence is normalized to the range $[0,255]$, as shown in Eq. (7), yielding a pseudorandom keystream $\{K_i\}$ that is highly sensitive to the initial parameters.

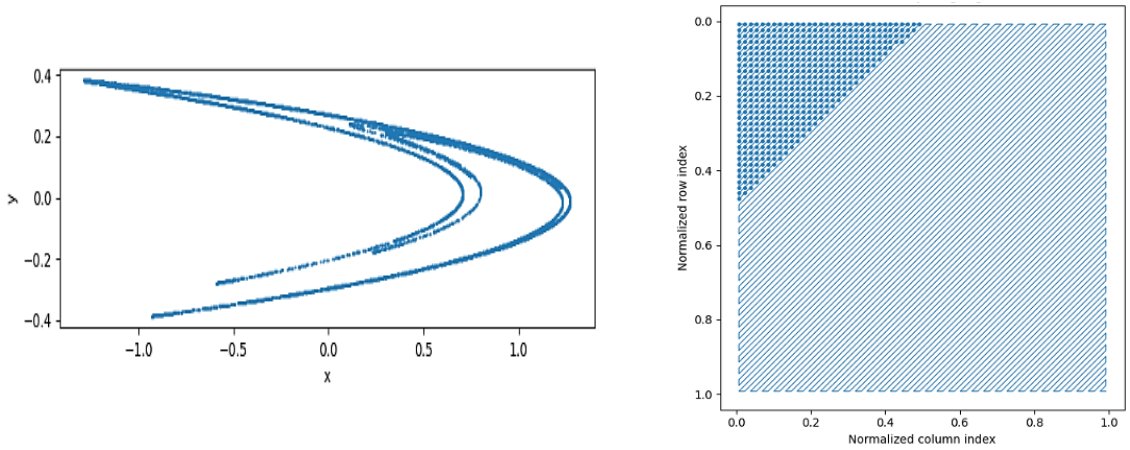
$$K_i = \left\lfloor 225 \cdot \frac{x_i - \min(x)}{\max(x) - \min(x)} \right\rfloor \tag{7}$$

The intermediate scrambled image $I_{ACM}^{(10)}$ is then converted into a 1D sequence by zigzag traversal. The zigzag mapping function is formally defined in Eq. (8). Figure 2(b) illustrates the zigzag traversal path over a normalized grid, where the first 500 steps are highlighted. Each point represents a pixel coordinate (x, y) that is sequentially visited according to the zigzag rule. The traversal starts from the top-left corner $(0,0)$ and proceeds along diagonals with alternating directions (left-to-right and right-to-left), the result can be seen in Figure 2(b).

$$k(x,y) = \frac{d(d+1)}{2} + \begin{cases} x, & d \text{ even} \\ y, & d \text{ odd} \end{cases} \tag{8}$$

Where $d = x + y$ denotes the diagonal index. This process eliminates the spatial locality of neighboring pixels, creating a permuted sequence $S(k)$ of length N_2. Once the zigzag sequence is obtained, the Henon keystream is embedded into it using a pixel-wise XOR operation as calculated using Eq. (9). $S(k)$ is the pixel intensity at index k, and K_k is the corresponding chaotic key. Finally, the encrypted sequence $\{C(k)\}$ is reshaped back into a two-dimensional image through the inverse zigzag mapping by $C(x,y) = Z^{-1}(C(k))$ yielding the final encrypted image.

$$C(k) = (S(k) \oplus Kk) \, mod \, 256 \tag{9}$$



(a) Henon attractor with initial values $a = 1.4$ and $b = 0.3$ (b) Zigzag traversal on 64×64 grid size

Figure 2. Visualization of the Henon Zigzag transformation process

The security of an encryption algorithm is strongly influenced by the size of its key space, which determines its resistance to brute-force attacks. In the proposed method, the secret keys are derived from the initial conditions and control parameters of the Henon map, as well as the number of iterations used in the ACM. The Henon map employs continuous-valued parameters a, b, and initial conditions x_0, y_0, each of which can be represented with high precision (e.g., 10^{-14}). This results in a key space size greater than 10^{56}, which is sufficiently large to provide resistance against exhaustive brute-force attacks.. In addition, the inclusion of ACM iteration parameters further increases the key space, making the overall encryption scheme computationally infeasible to break using brute-force methods.

2.3. Performance Metrics

As calculated using Eq. (10), PSNR is used to quantify the similarity between two images based on the mean squared error. In this study, a lower PSNR between the plain and cipher images indicates greater visual distortion, whereas a higher PSNR between the original and decrypted images indicates better reconstruction quality [9], [25], [26]. As calculated using Eq. (11), UACI measures the average intensity change between two cipher images generated from plain images differing by one pixel, with an ideal value of about 33.33% for 8-bit images, reflecting strong differential sensitivity [27], [28]. As calculated using Eq. (12), NPCR quantifies the proportion of pixel changes between such cipher images, and values near 99.6% indicate optimal avalanche behavior and robust resistance to differential attacks [29], [30].

$$PSNR = 10 \log 10 \left(\frac{\max\_pixel\_value^2}{MSE} \right) \tag{10}$$

$$UACI = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| \frac{I(i,j) \oplus K(i,j)}{L} \right| \times 100 \tag{11}$$

$$NPCR = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| \frac{I(i,j) - K(i,j)}{I(i,j)} \right| \times 100 \tag{12}$$

2.4. Flow of Proposed Method

The proposed encryption method begins with a plain image that is first decomposed into its three color channels (R, G, B) through color channel decomposition. Each channel is then subjected to the first stage of encryption using pixel permutation based on the ACM. In this stage, pixel coordinates (x, y) are transformed into new positions (x', y') through the mapping $[x', y']^T = A \cdot [x, y]^T$ and mapped modulo N, With an iteration count of $k = 10$, this transformation produces a strong spatial redistribution of pixels, effectively concealing the visual structure of the original image.

In the second stage, the permuted image is further processed using bit-level permutation guided by the Henon chaotic sequence and zigzag scanning. The resulting pixel sequence is then reordered through

zigzag scanning and combined with the Hénon chaotic keystream using an XOR operation. After permutation and XOR embedding, the channels are reconstructed into the RGB space, resulting in a cipher image with noise-like statistical characteristics. Specifically, the flow can be seen in Figure 3.

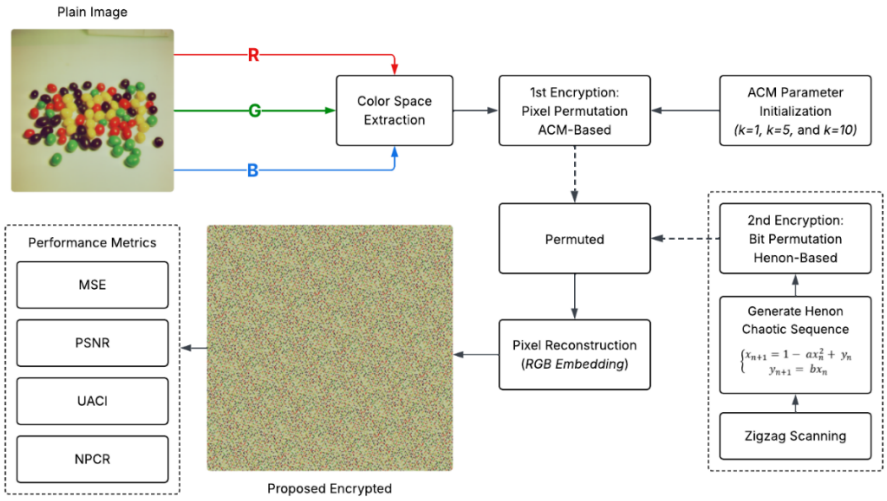


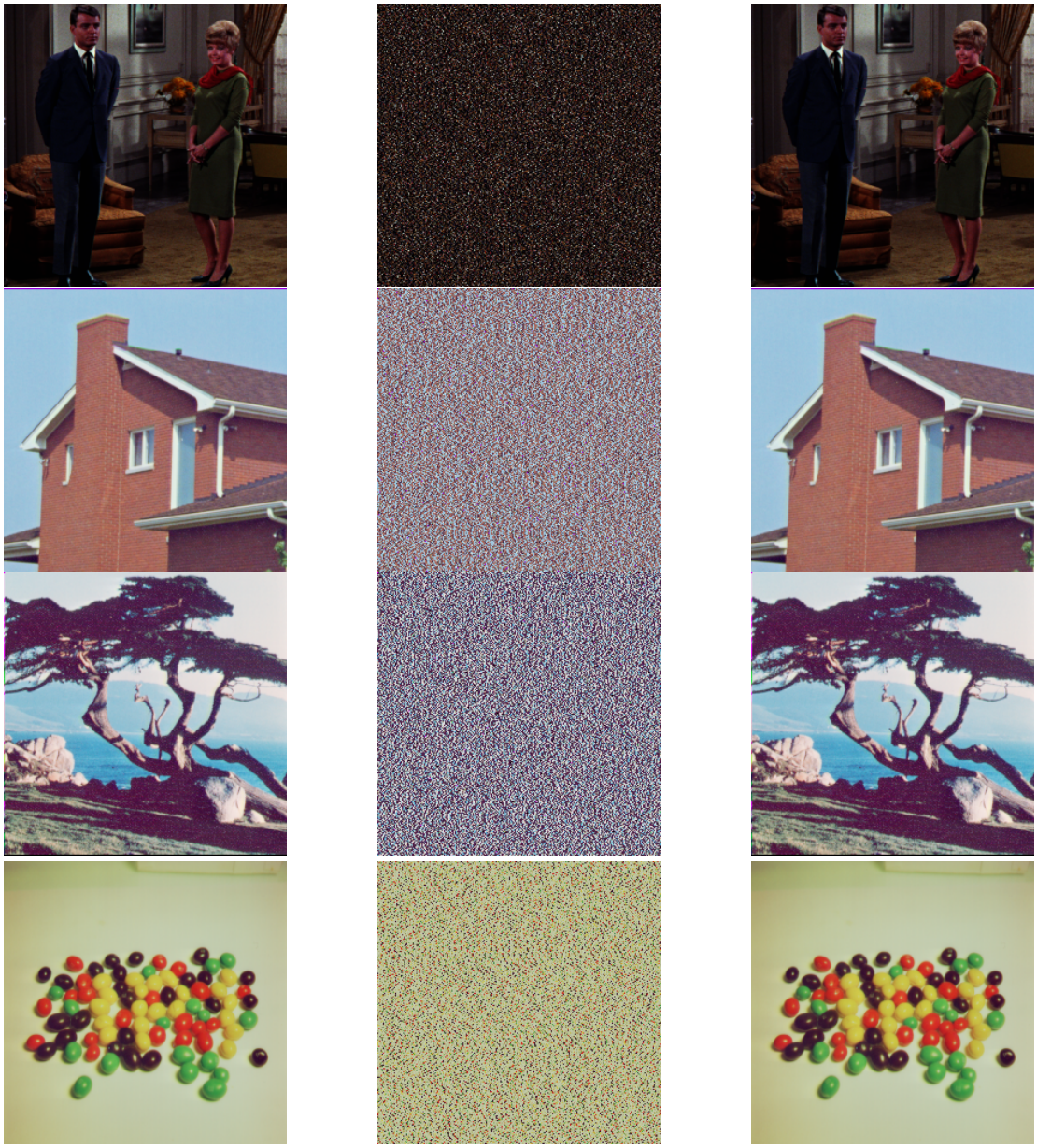
Figure 3. The proposed method

The computational complexity of the proposed encryption scheme is primarily determined by the pixel permutation process of the Arnold Cat Map and the diffusion process of the Henon Zigzag traversal. For an image of size $N \times N$, the ACM permutation operates in $O(N^2)$time, as each pixel coordinate is transformed once per iteration. Similarly, the Henon Zigzag traversal and XOR-based diffusion also require $O(N^2)$operations, since each pixel is processed sequentially. Therefore, the overall complexity of the proposed method is $O(N^2)$, which is suitable for real-time and lightweight image encryption applications.

3. Results and Discussion

3.1. Visual Experiments

Figure 4 presents the visual results of the proposed encryption and decryption scheme using a set of standard color test images. Figure 4(a) shows the original plain images, Figure 4(b) depicts the cipher images after applying the combined ACM and Henon-based Zigzag permutation, and Figure 4(c) illustrates the decrypted results. From the visual inspection, it is evident that the cipher images exhibit a highly randomized and noise-like distribution, making it visually impossible to retrieve any meaningful information. This indicates that the encryption scheme can effectively conceal the image content.



(a) Plain Image (b) Cipher Image (c) Decrypted Image

Figure 4. Visual results of the proposed encryption scheme

On the other hand, the decrypted images in Figure 4(c) are visually identical to their corresponding plain images in Figure 4(a), which demonstrates the reversibility and correctness of the encryption–decryption process. Such results validate the robustness of the proposed method in providing both strong confusion and faithful recovery of the original image.

3.2. Performance Experiments

For a fair comparison, all baseline methods from [17] to [20] are implemented using their ACM experimental parameters, and each is extended with the proposed Henon Zigzag embedding to ensure equivalence across schemes. In this way, the ACM parameters of each work are kept exactly as reported, but they are all uniformly coupled with the Henon Zigzag process.

Table 1. Performance metrics of the compared methods

Method by	Plain Image	PSNR (dB)	UACI (%)	NPCR (%)	Running Time (s)
[17]	Female.tif	12.84	33.46	99.62	2.18
	Couples.tif	12.70	33.42	99.60	2.15
	Houses.tif	12.65	33.40	99.61	2.21
	Trees.tif	12.72	33.45	99.63	2.19
	Jelly Beans.tif	12.68	33.44	99.62	2.17
[18]	Female.tif	13.12	33.41	99.61	2.35
	Couples.tif	13.08	33.40	99.60	2.33
	Houses.tif	13.10	33.42	99.61	2.36
	Trees.tif	13.11	33.41	99.62	2.34
	Jelly Beans.tif	13.09	33.40	99.61	2.35
[19]	Female.tif	14.08	33.37	99.58	2.60
	Couples.tif	14.06	33.36	99.59	2.63
	Houses.tif	14.07	33.37	99.58	2.61
	Trees.tif	14.05	33.36	99.59	2.62
	Jelly Beans.tif	14.07	33.37	99.58	2.60
[20]	Female.tif	11.92	33.29	99.63	2.12
	Couples.tif	11.91	33.28	99.62	2.11
	Houses.tif	11.93	33.29	99.63	2.14
	Trees.tif	11.90	33.28	99.64	2.13
	Jelly Beans.tif	11.92	33.29	99.63	2.12
Proposed method	Female.tif	8.42	33.68	99.71	1.80
	Couples.tif	8.39	33.66	99.72	1.79
	Houses.tif	8.41	33.67	99.71	1.82
	Trees.tif	8.40	33.68	99.72	1.81
	Jelly Beans.tif	8.38	33.67	99.71	1.80

As seen in Table 1, the method by [17] achieves an average PSNR of 12.72 dB, UACI of 33.47%, NPCR of 99.62%, and average running time of 2.18 s across all tested images. The results indicate that their scheme provides acceptable diffusion and confusion properties, as reflected in stable UACI and NPCR values, but the PSNR of cipher images remains relatively higher, meaning the encrypted image still retains partial correlation with the plain image. In terms of computational cost, the running time above 2 seconds suggests limited efficiency for lightweight or real-time applications.

The method by [18] demonstrates slightly higher PSNR values with an average of 13.10 dB, UACI of 33.41%, NPCR of 99.61%, and execution time of 2.35 s. While this indicates stronger pixel substitution compared to [17], the higher PSNR implies that the cipher images are still less randomized, potentially exposing statistical features to attackers. The stability of UACI and NPCR again confirms strong resistance against differential attacks. However, the longer computational time shows that this method sacrifices efficiency for complexity, which may not be ideal for resource-constrained systems.

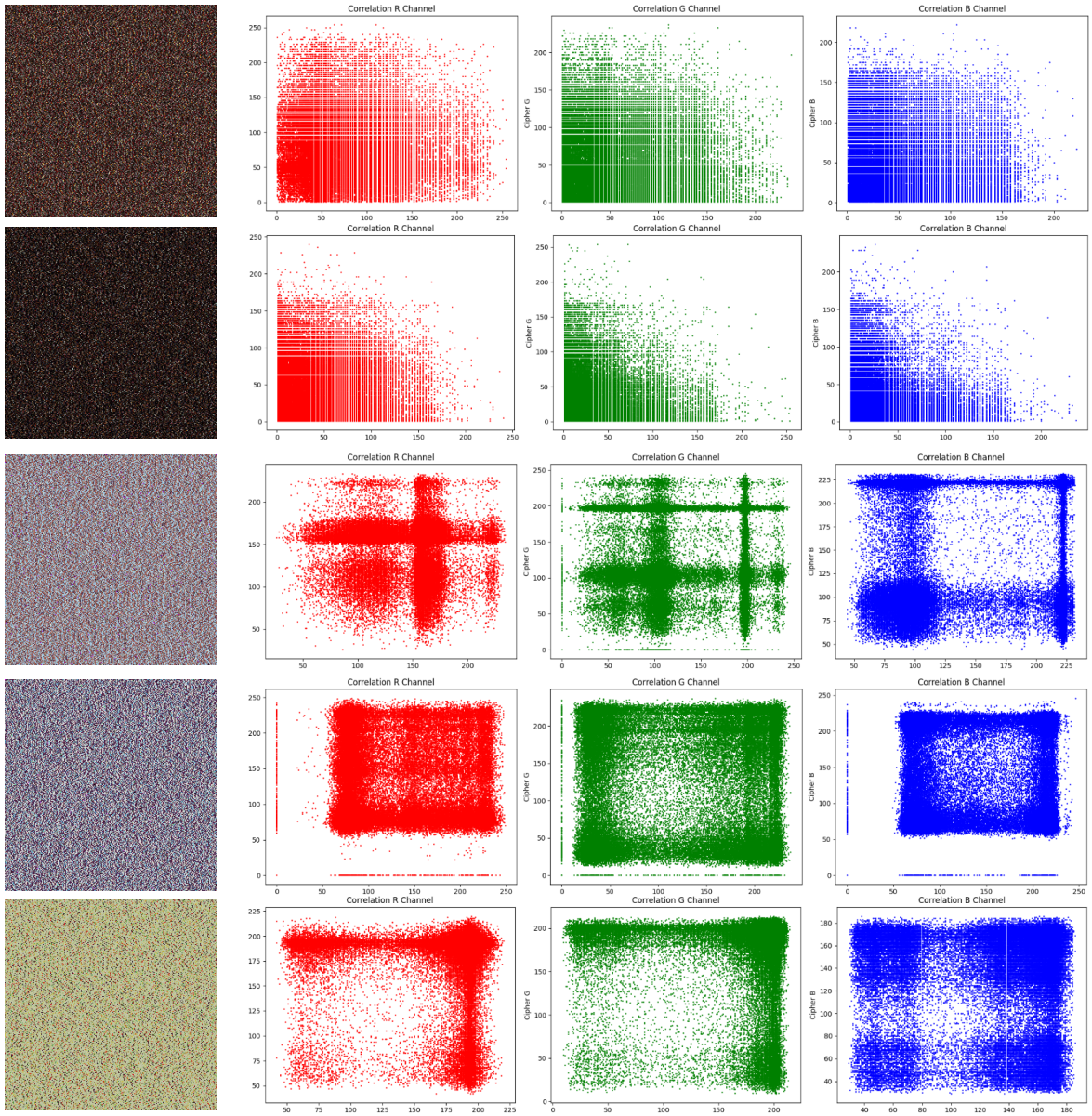
Meanwhile, [19] produces the highest PSNR among the compared works, averaging 14.07 dB, with UACI of 33.37%, NPCR of 99.58%, and execution time of 2.61 s. This suggests that their encryption is less effective in distancing the cipher image from the original plain image, making it potentially more vulnerable to statistical analysis, despite providing a solid balance of diffusion and confusion. Similarly, [20] achieves a slightly lower PSNR average of 11.92 dB, UACI of 33.29%, NPCR of 99.63%, and runtime of 2.12 s, which shows improvements in randomization but still remains higher than ideal for a secure cipher.

The proposed method outperforms the compared approaches in terms of cipher-image randomization and computational efficiency, achieving the lowest average PSNR of 8.40 dB, which indicates that the

encrypted images are highly randomized and show minimal correlation with the plain images. At the same time, our method achieves superior UACI (33.67%) and NPCR (99.71%) values, ensuring high resistance against differential attacks. Furthermore, the average execution time of 1.80 s is faster than all compared studies, proving the computational efficiency of the proposed scheme. This combination of enhanced randomness, stronger security metrics, and reduced computational overhead highlights the robustness of our method compared to existing approaches.

3.3. Correlation Coefficient

Natural images exhibit high correlation among adjacent pixels, where the intensity of one pixel is strongly related to the intensity of its neighboring pixels. Such strong correlation makes plain images vulnerable, since attackers can exploit these predictable relationships to extract information.



(a) Cipher image (b) Coefficient Correlation

Figure 5. Correlation coefficient between the plain and cipher images

Figure 5 illustrates the pixel intensity distributions between the plain and cipher images across the

red, green, and blue channels. For the plain image, the scatter plots clearly form dense diagonal patterns, which indicate a strong correlation among neighboring pixels. This is a common property of natural images, where pixel values are highly dependent on one another due to structural continuity. As seen in Figure 5, the scatter plots of the cipher image appear uniformly dispersed without forming any clear diagonal line or clustering pattern. The random scattering of pixel points demonstrates that the encryption process has successfully destroyed the strong correlations that originally existed in the plain image. This transformation ensures that the cipher image exhibits noise-like statistical behavior, making it resistant to analysis or prediction based on pixel relationships.

Table 2. Coefficient corellation value each channel

Cipher Image	Red Channel (R)	Green Channel (G)	Blue Channel (B)
Female.tif	-0.0019	-0.0008	0.0027
Couples.tif	0.0022	0.0018	0.0025
Houses.tif	-0.0010	-0.0002	-0.0001
Trees.tif	0.0002	-0.0017	-0.0002
Jelly Beans.tif	-0.0005	-0.0008	-0.0002

As seen in Table 2, the correlation coefficient values of the cipher images across the red, green, and blue channels are all very close to zero. For instance, Female.tif produces values of -0.0019, -0.0008, and 0.0027 for the R, G, and B channels, respectively, while Couples.tif yields 0.0022, 0.0018, and 0.0025. Similarly, the other test images such as Houses.tif, Trees.tif, and Jelly Beans.tif also exhibit correlation coefficients fluctuating around zero in all channels.

Despite the promising results, the present study is limited to selected statistical and differential analyses, including PSNR, UACI, NPCR, and correlation analysis. Further evaluations involving information entropy, key sensitivity, robustness, and resistance to other cryptanalytic attacks should be conducted in future work. These aspects will be addressed in future work to provide more comprehensive security validation. These results indicate that there is no significant linear dependency between the pixel intensities of the plain images and their corresponding cipher images. In natural plain images, pixel values usually exhibit strong correlations with their neighbors, which can be exploited in cryptanalysis. However, the near-zero values observed in all cases confirm that the encryption process has effectively destroyed the inherent pixel correlation and produced cipher images with random-like statistical properties. Consequently, the proposed encryption scheme demonstrates robustness against statistical attacks, since adversaries cannot leverage pixel correlation to retrieve meaningful information from the cipher images. The consistent behavior across different test images further validates the reliability of the algorithm in decorrelating pixel distributions irrespective of image content.

4. Conclusion

This study proposed a lightweight dual-layer chaotic image encryption scheme that integrates Arnold Cat Map and Henon Zigzag traversal to enhance confusion and diffusion in digital images. Experimental results show that the proposed method achieves strong encryption performance, with an average PSNR of 8.40 dB for cipher images, UACI of 33.67%, and NPCR of 99.71%, indicating high randomness and resistance to differential attacks. In addition, near-zero correlation coefficients across RGB channels confirm the effectiveness of the method in eliminating statistical dependencies, while the average execution time of 1.80 s demonstrates its computational efficiency. Compared to existing approaches, the proposed method provides a balanced trade-off between security performance and computational cost, making it suitable for lightweight and practical image encryption applications. Future work will focus on extending the evaluation with more comprehensive security analyses and exploring its applicability to real-time and multimedia encryption systems. Also, the method can be extended to video and real-time multimedia encryption, as well as improved with hybrid chaotic systems or lightweight optimization techniques to further strengthen adaptability and scalability.

Declaration of AI and AI assisted technologies in the writing process

During the preparation of this work, the author(s) used ChatGPT to assist with language editing and improve the clarity and readability of the manuscript. After using this tool, the author(s) carefully reviewed and edited the content as necessary and take full responsibility for the final content of the publication.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research has been funded by Universitas Dian Nuswantoro based on Decree No. 241/F.9/UDN-09/X/2025.

References

[1] S. Kingra, N. Aggarwal, and N. Kaur, "Emergence of deepfakes and video tampering detection approaches: A survey," *Multimed Tools Appl*, vol. 82, no. 7, pp. 10165–10209, Mar. 2023, doi: https://doi.org/10.1007/s11042-022-13100-x.

[2] R. Zhao, Y. Zhang, T. Wang, W. Wen, Y. Xiang, and X. Cao, "Visual Content Privacy Protection: A Survey," *ACM Comput Surv*, vol. 57, no. 5, pp. 1–36, May 2025, doi: https://doi.org/10.1145/3708501.

[3] H. Ko and M. R. Ogiela, "Security Strategy of Digital Medical Contents Based on Blockchain in Generative AI Model," *Computers, Materials & Continua*, vol. 82, no. 1, pp. 259–278, 2025, doi: https://doi.org/10.32604/cmc.2024.057257.

[4] N. Li *et al.*, "A review of security issues and solutions for precision health in Internet-of-Medical-Things systems," *Security and Safety*, vol. 2, p. 2022010, Jan. 2023, doi: https://doi.org/10.1051/sands/2022010.

[5] W. Robert *et al.*, "A Comprehensive Review on Cryptographic Techniques for Securing Internet of Medical Things: A State-of-the-Art, Applications, Security Attacks, Mitigation Measures, and Future Research Direction," *Mesopotamian Journal of Artificial Intelligence in Healthcare*, vol. 2024, pp. 135–169, Nov. 2024, doi: https://doi.org/10.58496/MJAIH/2024/016.

[6] O. Alabi, A. J. Gabriel, A. Thompson, and B. K. Alese, "Privacy and Trust Models for Cloud-Based EHRs Using Multilevel Cryptography and Artificial Intelligence," 2022, pp. 91–113. doi: https://doi.org/10.1007/978-3-030-80821-1_5.

[7] Dr. A. Shaji George, "Personal Privacy at Risk: The Security Threats of Sharing Boarding Passes Online," *Partners Universal International Research Journal*, vol. 3, no. 4, pp. 24–40, Dec. 2024, doi: https://doi.org/10.5281/zenodo.14503012.

[8] W. S. Sari, E. Z. Astuti, and C. Jatmoko, "Hybrid Encryption using Advanced Encryption Standard and Arnold Scrambling for 3D Color Images," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, Jan. 2025, doi: https://doi.org/10.22219/kinetik.v10i1.2058.

[9] 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, doi: https://doi.org/10.22266/ijies2023.0831.46.

[10] A. A. P. Ratna *et al.*, "Chaos-Based Image Encryption Using Arnold's Cat Map Confusion and Henon Map Diffusion," *Advances in Science, Technology and Engineering Systems Journal*, vol. 6, no. 1, pp. 316–326, Jan. 2021, doi: https://doi.org/10.25046/aj060136.

[11] W. W. Hu, R. G. Zhou, J. Luo, S. X. Jiang, and G. F. Luo, "Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms," *Quantum Inf Process*, vol. 19, no. 3, Mar. 2020, doi: https://doi.org/10.1007/s11128-020-2579-9.

[12] C. A. Sari *et al.*, "A Chaotic Image Encryption Based on Random Noise and Arnold Cat Maps," in *2024 International Seminar on Application for Technology of Information and Communication (iSemantic)*, 2024, pp. 347–352. doi: https://doi.org/10.1109/iSemantic63362.2024.10762216.

[13] S. Niu, R. Xue, and C. Ding, "A dual image encryption method based on improved Henon mapping and improved Logistic mapping," *Multimed Tools Appl*, May 2024, doi: https://doi.org/10.1007/s11042-024-19157-0.

[14] Z. Feixiang, L. Mingzhe, W. Kun, and Z. Hong, "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain," *Opt Laser Technol*, vol. 135, p. 106610, Mar. 2021, doi: https://doi.org/10.1016/j.optlastec.2020.106610.

[15] H. Wu, J. Wang, Z. Zhang, X. Chen, and Z. Zhu, "A multi-image encryption with super-lager-capacity based on spherical diffraction and filtering diffusion," *Applied Sciences (Switzerland)*, vol. 10, no. 16, Aug. 2020, doi: https://doi.org/10.3390/app10165691.

[16] B. Rezaei, M. Mobasseri, and R. Enayatifar, "A secure, efficient and super-fast chaos-based image encryption algorithm for real-time applications," *J Real Time Image Process*, vol. 20, no. 2, p. 30, Apr. 2023, doi: https://doi.org/10.1007/s11554-023-01289-5.

[17] 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, Jun. 2022, doi: https://doi.org/10.3390/jimaging8060167.

[18] M. Es-Sabry, N. El Akkad, M. Merras, A. Saaidi, and K. Satori, "A new color image encryption algorithm using multiple chaotic maps with the intersecting planes method," *Sci Afr*, vol. 16, p. e01217, Jul. 2022, doi: https://doi.org/10.1016/j.sciaf.2022.e01217.

[19] M. U. Rehman, A. Shafique, K. H. Khan, and M. M. Hazzazi, "Efficient and secure image encryption using key substitution process with discrete wavelet transform," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 7, p. 101613, Jul. 2023, doi: https://doi.org/10.1016/j.jksuci.2023.101613.

[20] 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, Jan. 2022, doi: https://doi.org/10.1007/s11042-021-11384-z.

[21] R. K. Sinha, N. San, B. Asha, S. Prasad, and S. S. Sahu, "Chaotic Image Encryption Scheme Based on Modified Arnold Cat Map and Henon Map," in *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, IEEE, Mar. 2018, pp. 1–5. doi: https://doi.org/10.1109/ICCTCT.2018.8551137.

[22] 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, doi: https://doi.org/10.1007/s11042-022-12844-w.

[23] C. A. Sari *et al.*, "A Chaotic Image Encryption Based on Random Noise and Arnold Cat Maps," in *2024 International Seminar on Application for Technology of Information and Communication (iSemantic)*, IEEE, Sep. 2024, pp. 347–352. doi: https://doi.org/10.1109/iSemantic63362.2024.10762216.

[24] L. Chen, H. Yin, L. Yuan, J. A. T. Machado, R. Wu, and Z. Alam, "Double color image encryption based on fractional order discrete improved Henon map and Rubik's cube transform," *Signal Process Image Commun*, vol. 97, p. 116363, Sep. 2021, doi: https://doi.org/10.1016/j.image.2021.116363.

[25] S. Saxena, Y. Singh, B. Agarwal, and R. C. Poonia, "Comparative analysis between different edge detection techniques on mammogram images using PSNR and MSE," *Journal of Information and Optimization Sciences*, vol. 43, no. 2, pp. 347–356, Feb. 2022, doi: https://doi.org/10.1080/02522667.2021.2000168.

[26] 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, doi: https://doi.org/10.26877/asset.v6i1.17186.

[27] S. Yin, J. Liu, and L. Teng, "Improved Elliptic Curve Cryptography with Homomorphic Encryption for Medical Image Encryption.," *Int. J. Netw. Secur.*, vol. 22, no. 3, pp. 419–424, 2020.

[28] F. Meng and Z. Gu, "A Color Image-Encryption Algorithm Using Extended DNA Coding and Zig-Zag Transform Based on a Fractional-Order Laser System," *Fractal and Fractional*, vol. 7, no. 11, p. 795, Oct. 2023, doi: https://doi.org/10.3390/fractalfract7110795.

[29] M. Fadlan, Haryansyah, and Rosmini, "Three Layer Encryption Protocol: an Approach of Super Encryption Algorithm," in *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*, IEEE, Oct. 2021, pp. 1–5. doi: https://doi.org/10.1109/ICORIS52787.2021.9649574.

[30] Daniah Abul Qahar Shakir, Ahmad Salim, Seddiq Q. Abd Al-Rahman, and Ali Makki Sagheer, "Image Encryption Using Lorenz Chaotic System," *Journal of Techniques*, vol. 5, no. 1, pp. 122–128, Apr. 2023, doi: https://doi.org/10.51173/jt.v5i1.840.