

Design and Evaluation of a Hybrid Hénon-Logistic Chaotic Generator for Image Encryption: A Comparative Study with Traditional Encryption Methods for Digital Data Protection.

Abstract :

This paper presents a Hybrid Chaotic Encryption System (HCES) for image encryption based on the coupling of a two-dimensional Hénon map and a one-dimensional Logistic map. The Hénon dynamics modulate the Logistic control parameter, generating a hybrid chaotic sequence used to construct a dynamic substitution box (S-box) and perform confusion and diffusion operations. The proposed scheme was implemented in Python and evaluated using six standard test images through visual inspection, Shannon entropy, correlation coefficients, chi-square testing, the Number of Pixels Change Rate (NPCR), and the Unified Average Changing Intensity (UACI). The experimental results show that the encrypted images exhibit noise-like patterns, with entropy values approaching 8 bits and correlation coefficients generally close to zero. A comparative evaluation using the Lena image and an identical data size of 268,098 bytes was also conducted against AES-128 and AES-256. The proposed scheme achieved an entropy of 7.9993, a correlation coefficient of 0.0004, and an encryption throughput of 3.93 Mbit/s under the reported experimental conditions. The selected NIST statistical tests yielded p-values above 0.01. These findings indicate promising statistical characteristics and computational performance for image encryption.

Keywords: Chaotic image encryption; Hénon map; Logistic map; Dynamic S-box; NPCR; UACI; AES-128; AES-256.

1. Introduction

The widespread adoption of digital communication and multimedia technologies has increased the need for reliable protection of digital images. Although AES provides strong security, its

fixed components computational structure may limit its adaptability to image encryption. Consequently, Chaotic systems have attracted attention because of their sensitivity to initial conditions. Huo et al. [1] improved AES by using a three-dimensional hyperchaotic system to generate dynamic cryptographic components, whereas Khan et al. [2] combined chaotic maps with AES-GCM, SHA-256, and dynamic initialization vectors. Vamsikrishna et al. [3] developed a lightweight Logistic-map-based framework for IoT devices with post-quantum cryptography, while Helmy and Torkey [4] combined two-dimensional Baker map with audio encryption and steganography. ALEXAN et al. [5] proposed a complex image-encryption scheme using a 5D hyperchaotic system, Arnold's cat map, Langton's Ant, and a dynamic S-box. Muhammed et al. [6] compared conventional encryption algorithms for image protection, whereas Naim and Ali Pacha [7] combined a 3D Lorenz system with modified AES and a dynamic S-box.

These studies demonstrate the potential of chaotic systems for enhancing image-encryption security; however, existing approaches involve different trade-offs between randomness, computational complexity, key sensitivity, and adaptability. Some rely on a single low dimensional chaotic system, while others employ high-dimensional or multi-stage architectures that may increase implementation complexity. In addition, several AES-based approaches retain conventional cryptographic components rather than dynamically generating them from hybrid chaotic sequences. Therefore, there remains a need for a balanced hybrid approach that can increase nonlinear complexity and randomness without introducing excessive architectural complexity.

The present study proposes a hybrid chaos-based encryption framework for image and text encryption that integrates a one-dimensional Logistic map with a two-dimensional Hénon map through bidirectional coupling, rather than relying on conventional AES components. The resulting unified chaotic sequence is used to construct a dynamic substitution box (S-box), replacing fixed cryptographic structures entirely. The proposed method is evaluated using encryption and decryption time, key-space characteristics, entropy, correlation, coefficient, NPCR, UACI. These metrics are used to assess computational efficiency, randomness key sensitivity, and resistance to statistical and differential attacks.

2. Mathematical Model of the Hybrid Generator

2.1. Hénon Map

The Hénon map is a two-dimensional discrete-time system whose state at iteration n is denoted by $(x^{(H)}_n, y^{(H)}_n)$. The reference configuration adopted in the experiments is $a=1.4$ et $b=0.3$, with $(x^{(H)}_0, y^{(H)}_0)=(0.1 ; 0.1)$.

$$x^{(H)}_{n+1} = 1 - a \left(x^{(H)}_n \right)^2 + y^{(H)}_n, \quad y^{(H)}_{n+1} = b x^{(H)}_n \quad (1)$$

With $a=1.4$ and $b=0.3$, the Hénon map constitutes the two-dimensional source of the hybrid generator. This configuration is adopted as the reference for the simulations because it provides rich dynamics that can subsequently be transferred to the logistic subsystem. Nevertheless, these parameter values should be regarded as a reference experimental choice, and the chaotic nature of the resulting dynamics should be confirmed using the dynamical indicators presented later in this section. In particular, the variable $x^{(H)}_n$ plays a central role, as it directly contributes to the modulation of the control parameter of the logistic map.

$$J_n = \begin{bmatrix} -2ax^{(H)}_n & 1 \\ b & 0 \end{bmatrix} \quad (2)$$

The Jacobian matrix J_n describes the local tangent dynamics of the Hénon map and makes it possible to track the evolution of an infinitesimal perturbation around the nominal trajectory. It therefore constitutes the fundamental matrix used for the numerical estimation of the Lyapunov exponents. In the context of the hybrid generator, this characterization first allows the intrinsic dynamics of the Hénon map to be evaluated before analyzing the influence of its trajectory on the logistic component. To ensure reproducibility, the numerical method used to compute the Lyapunov exponents, the number of iterations, and the length of the transient phase should be explicitly specified in the experimental protocol.

2.2. Logistic Map

The logistic component is a one-dimensional map whose dynamics depend on the parameter r . In the proposed generator, r is not kept constant; instead, it is driven by the trajectory of the Hénon map.

$$x^{(L)}_{n+1} = r_n x^{(L)}_n (1 - x^{(L)}_n), \quad 0 < x^{(L)}_n < 1 \quad (3)$$

Equation (3) defines the logistic component of the proposed generator. In the classical logistic map, the parameter r is constant; in the present architecture, it becomes a dynamic quantity, denoted by r_n , and depends on the state of the Hénon map. The value $r=4$ is recalled as an analytical reference, since, for the classical logistic map, it yields a Lyapunov exponent of $\lambda=\ln(2)\approx 0,693147$. However, this value should not be directly associated with that of the hybrid generator, since its effective dynamics depend on the temporal modulation of r_n). The constraint $0 < x_n^{(L)} < 1$ corresponds to the usual invariant domain of the logistic map.

2.3. Dynamic Hénon-Logistic Coupling

After a warm-up phase, an X_{max} boundary is determined based on the Hénon trajectory. The logistic parameter is then modulated within the interval $[3,57 ; 4]$.

$$r_n = r_{min} + (r_{max} - r_{min}) \cdot \min\left(\frac{|x_n^{(H)}|}{X_{max}}, 1\right), \quad r_{min} = 3.57, \quad r_{max} = 4 \quad (4)$$

Equation (4) formalizes the Henon-Logistic coupling mechanism. The variable $x_n^{(H)}$ is first normalized by the bound X_{max} , then used to generate a parameter r_n in the range $r_{min}=3.57$ to $r_{max}=4$. The operator $\min(\cdot, 1)$ imposes a saturation when the normalized value exceeds one, thereby ensuring that the parameter remains within the specified interval. The coupling is strictly unidirectional: the Henon system drives the logistic map, while the logistic variable does not alter the dynamics of the Henon system. The logistic subsystem is therefore non-autonomous when considered in isolation, whereas the complete generator constitutes a deterministic cascade driven by the state of the Henon system. This distinction is essential for interpreting the dynamics and for correctly formulating the calculation of the Lyapunov exponents of the complete system.

This distinction is important for scientific interpretation: the complexity of the generator stems from the temporal modulation of the logistic parameter by a variable derived from a two-dimensional system. The study therefore does not simply consist of juxtaposing two independent sequences.

2.4. Dynamic Characterization

The dynamical characterization is conducted at several complementary levels in order to relate qualitative observations to quantitative indicators. Time series are used to examine the evolution of the state variables, phase portraits describe the geometry of the trajectories, bifurcation diagrams illustrate the effects of the control parameters, and Lyapunov exponents quantify the dynamical sensitivity. This combination is particularly important for a hybrid generator, since the complexity observed in the output results from both the intrinsic dynamics of the Hénon map and the temporal modulation of the control parameter of the logistic map.

The six representations presented in Figure 1 provide a coherent view of the dynamics of the hybrid generator. The time series of the Hénon map (a) highlights a bounded yet highly irregular evolution of the dynamical variables, while the phase portrait of the Hénon attractor (b) reveals a complex structure characteristic of chaotic dynamics. The bifurcation diagram of the logistic map (c) then situates the dynamics of the logistic subsystem within a regime where periodic behaviors coexist with chaotic regions as the parameter r varies. The temporal evolution of the parameter r_n , modulated by the Hénon dynamics (d), highlights the central role of the Hénon-Logistic coupling, since the control parameter is no longer constant but varies over time according to the state of the Hénon system. The time series of the hybrid logistic subsystem (e) directly reflects the effect of this dynamic modulation and exhibits an irregular evolution of the logistic variable. Finally, the sensitivity to a perturbation of the initial conditions (f) reveals a rapid divergence of the trajectories, a behavior consistent with the sensitivity to initial conditions generally associated with chaotic systems. Taken together, the results presented in panels (a)-(f) provide a complementary qualitative characterization of the dynamics of the proposed hybrid generator.

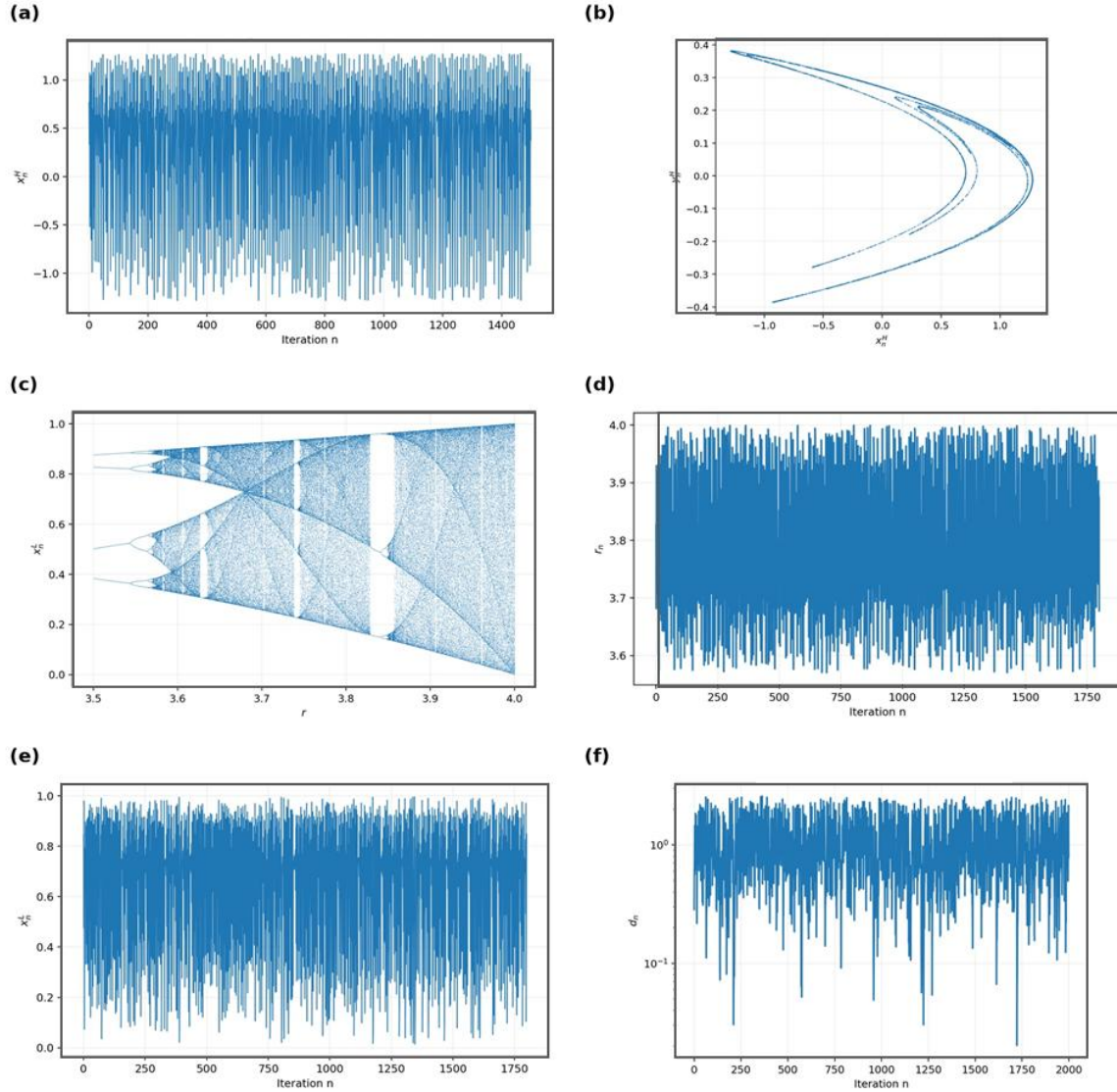


Figure 1. Initial dynamic characterization of the generator: (a) time series of the Henon map; (b) phase portrait; (c) bifurcation diagram of the logistic map; (d) evolution of the dynamic parameter r_n ; (e) time series of the hybrid logistic subsystem; (f) sensitivity to an initial perturbation.

The six complementary representations in Fig. 2 provide a comprehensive characterization of the dynamical behavior of the hybrid generator. The temporal evolution of the Hénon variables in Fig. 2(a) exhibits bounded but highly irregular fluctuations, indicating a complex underlying dynamic, while the bifurcation diagram in Fig. 2(b) reveals a broad parameter region characterized by a dense distribution of states, consistent with the coexistence of complex and

chaotic regimes. The parameter-sweep results shown in Fig. 2(c) and Fig. 2(d), obtained by varying the Hénon parameters a and b , respectively, demonstrate that the irregular dynamics persist over extended parameter intervals, although the structure and density of the generated states vary with the control parameters. These results indicate that the chaotic behavior is not restricted to a single parameter configuration. More importantly, the Lyapunov-exponent diagrams presented in Fig. 2(e) and Fig. 2(f) provide a quantitative characterization of the dynamics: the predominantly positive values of the largest Lyapunov exponent over the investigated ranges of a and r confirm the presence of sensitive dependence on initial conditions and support the chaotic nature of the generated dynamics. Taken together, Figs. 2(a)-2(f) show that the hybrid generator exhibits complex and robust chaotic behavior over a non-negligible parameter region, while the Lyapunov analysis provides the quantitative evidence required to complement the qualitative observations obtained from the temporal and bifurcation representations.

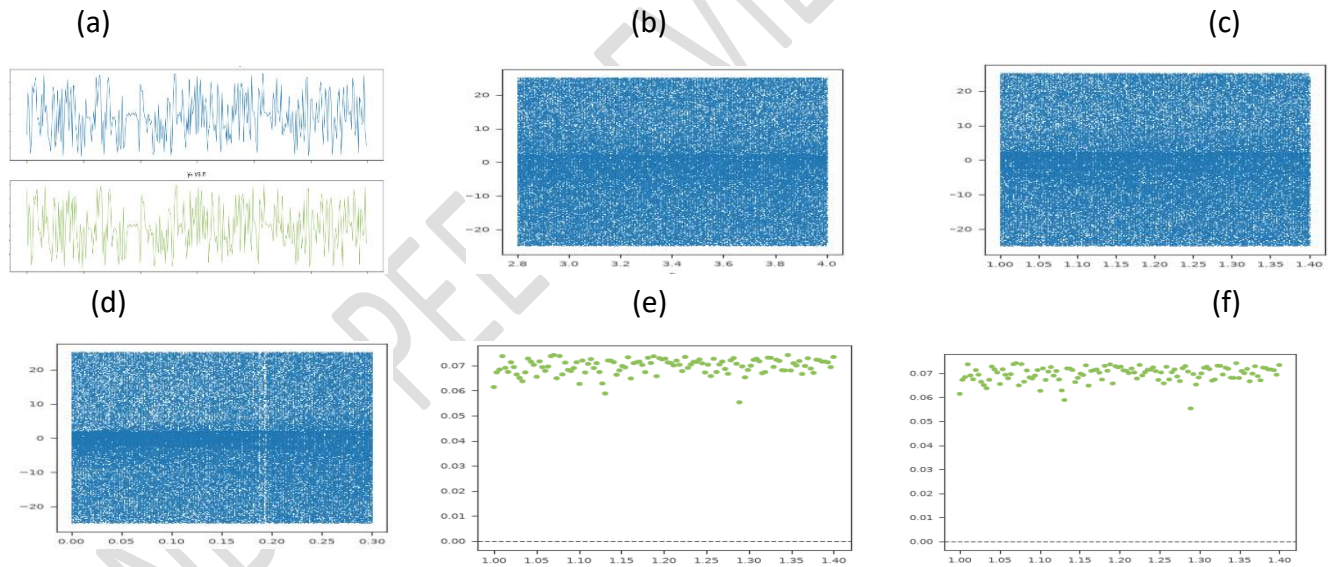


Figure 2. Dynamic validation and parametric analysis of the hybrid system: (a) time traces of x_n and y_n ; (b) bifurcation diagram as a function of r ; (c) bifurcation diagram as a function of a ; (d) bifurcation diagram as a function of b ; (e) Lyapunov exponent as a function of a ; (f) Lyapunov exponent as a function of r .

3. Construction of the Dynamic S-Box

The construction of the S-box is based on a two-step sorting procedure applied to the 256 normalized chaotic values $s = (s_0, \dots, s_{255})$. The first sorting operation establishes an order among the chaotic values, while the second transforms this order into a permutation of integers. Thus, expression (5) ensures that each integer value between 0 and 255 appears only once, which gives the S-box the bijectivity property necessary for the reversibility of the substitution. This construction also has the advantage of preserving the order information derived from the chaotic sequence while converting it into a discrete representation that can be directly used in a cryptographic system. The inverse permutation S^{-1} can then be obtained by inverting this correspondence, thereby enabling the decryption operation. However, bijectivity is a necessary but not sufficient condition for guaranteeing the cryptographic properties of an S-box; the quality of the substitution must therefore be evaluated subsequently using quantitative criteria such as nonlinearity, the Strict Avalanche Criterion (SAC), the Bit Independence Criterion (BIC), and differential probabilities.

$$S = \text{argsort}(\text{argsort}(s)) \quad (5)$$

4. Henon-Logistic Hybrid Cryptosystem

The proposed hybrid Hénon-Logistic cryptosystem combines the complex dynamics of the Hénon map with the nonlinear behavior of the logistic map to generate key-dependent chaotic sequences for image encryption. The overall encryption architecture consists of successive stages, including chaotic sequence generation, dynamic S-box construction, confusion, and diffusion. The Hénon map serves as the primary chaotic source, while its dynamical state is used to modulate the control parameter of the logistic subsystem, thereby generating a time-varying hybrid chaotic sequence. This sequence is normalized and transformed into a permutation through the dynamic S-box construction procedure described in Section 3, which is then used to perform nonlinear substitution of the image data. In parallel, the generated chaotic sequences are employed during the diffusion stages to modify pixel values and reduce the statistical dependence between neighboring pixels. The complete encryption process therefore relies on the interaction between nonlinear substitution and iterative diffusion, with the secret key determining

the initial conditions and control parameters of the chaotic generator. As illustrated in Fig. 3, the overall architecture summarizes the successive processing stages, from secret-key initialization and the interaction between the Hénon and logistic maps to the generation of the hybrid chaotic sequence, dynamic S-box, and key stream, ultimately transforming the plaintext image into the ciphertext. The corresponding decryption procedure applies the inverse S-box and inverse diffusion operations in the appropriate reverse order to recover the original image. The mathematical formulation and detailed implementation of each processing stage are presented in the following subsections.

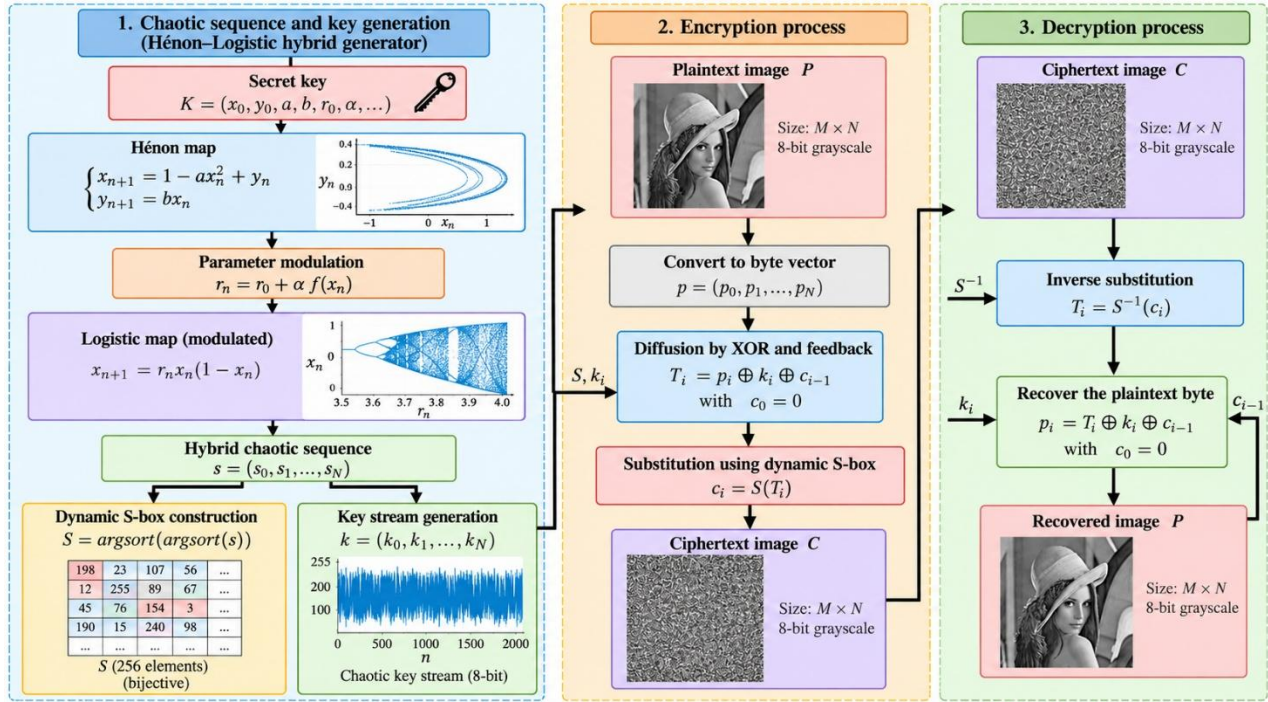


Fig. 3: Hénon-Logistic Hybrid Cryptosystem

5. Algorithm: Hybrid Logistic-Hénon Encryption

The following steps describe the proposed Hybrid Logistic-Hénon encryption process, including chaotic initialization, dynamic S-box generation, and Keystream generation

1. Initialise $x=x_0$, $y=y_0$, and $Z=x_0$.
2. Execute the chaotic warm-up phase.
3. Generate 256 chaotic values using the coupled Logistic-Hénon system.
4. Normalize the generated values using $S_i = |x_i| \bmod 1$.
5. Rank the 256 values to generate the dynamic S-box.

6. Construct the inverse S-box.
7. Continue the coupled chaotic process to generate keystream.
8. Convert chaotic states into byte values
9. Initialize $C_0=0$
10. For each plaintext byte calculate $T_i = p_i \oplus KS_i \oplus C_{i-1}$
11. Apply the dynamic S-box $C_i = S_{box}[T_i]$
12. Store C_i as the ciphertext byte

7. Experimental Results

The proposed Hybrid Logistic-Henon encryption algorithm was evaluated using six standard test images. The experiments include visual analysis of the original encrypted, and decrypted images, followed by statistical evaluation using NPCR, UACI entropy, correlation coefficient, and chi-square(χ^2) tests.

7.1. Statistical results for the six images

The statistical analysis evaluates the effectiveness of the proposed HCES encryption scheme in generating ciphertext images with high randomness and low statistical dependence. The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) quantify the sensitivity of the encryption scheme to small changes in the plaintext, while Shannon entropy measures the randomness of the encrypted pixel distribution. The correlation coefficient assesses the statistical dependence between adjacent pixels, and the chi-square test evaluates the uniformity of the ciphertext pixel-value distribution. Figure 4 presents representative visual results of the encryption and decryption processes, including the original plaintext images, their corresponding ciphertext images, and the recovered images. Table 1 summarizes the statistical security metrics for the grayscale and RGB test images, with the RGB images evaluated separately across their red, green, and blue channels. Together, these visual and quantitative evaluations provide complementary evidence of the encryption scheme's performance.

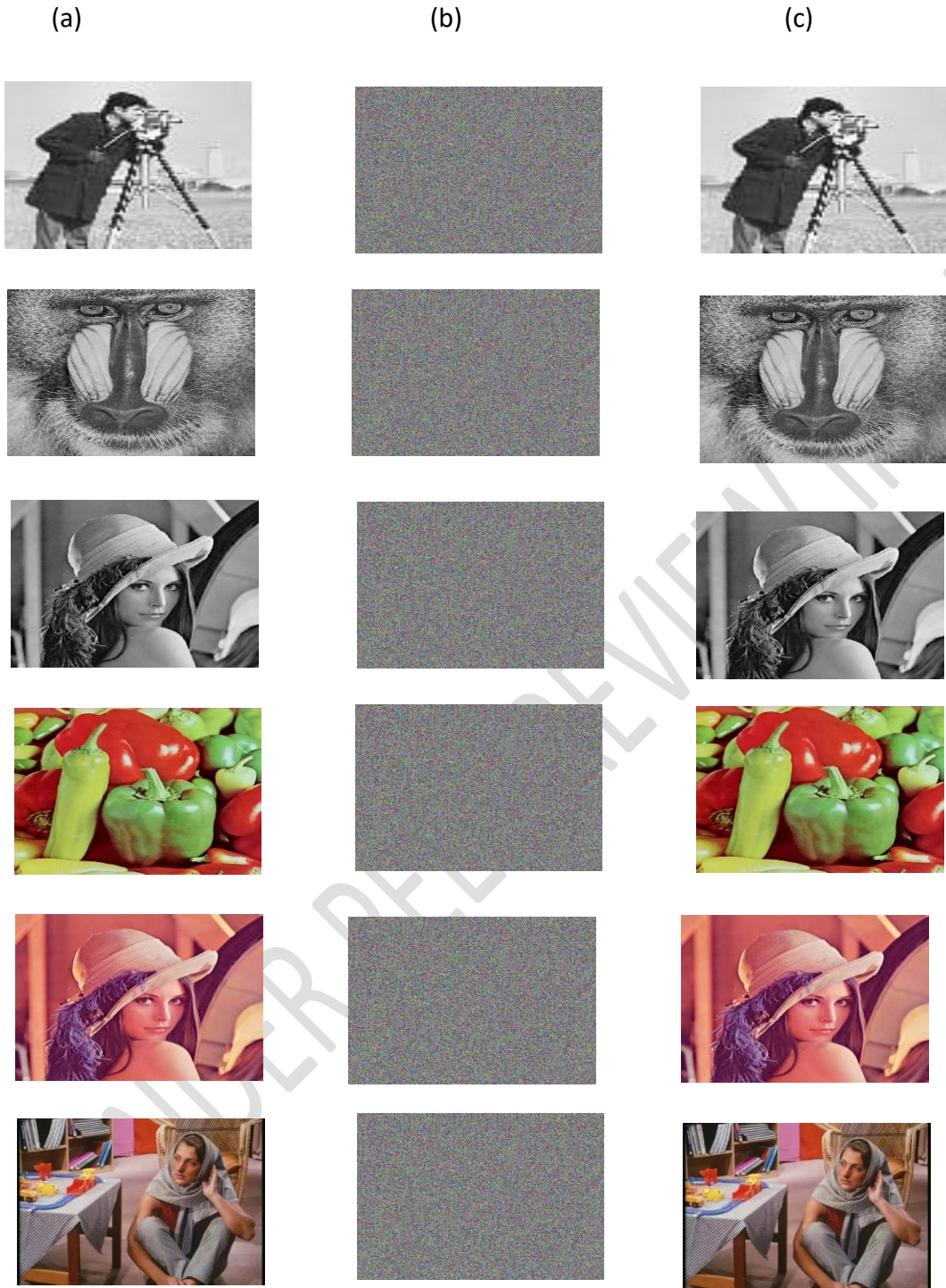


Fig 4. Visual evaluation of the proposed HCES image encryption and decryption scheme. (a) Original plaintext images; (b) corresponding encrypted ciphertext images exhibiting noise-like visual patterns; (c) decrypted images recovered using the proposed decryption procedure.

Table 1. Statistical Security Analysis of the Proposed HCES Encryption Scheme on Standard Grayscale and RGB Test Images

Image	channel	NPCR (%)	UACI (%)	Entropy	Correlation	χ^2
cameraman (Gray)		99.58	33.4	7.9201	-0.023	275.29
Badoon (Gray)		99.6	33.65	7.9925	0.0074	245.9
Lena (Gray)		99.5777	31.9522	7.9978	-0.0031	222.37
Peppers	R	99.605	33.45	7.9959	-0.0045	252.77
	G	96.5825	33.3119	7.9949	0.0019	253.98
	B	99.5475	33.566	7.9956	0.008	249.47
Lena(color)	R	99.5773	33.434	7.9964	-0.0075	267.09
	G	99.6175	33.445	7.9965	-0.0021	266.98
	B	99.6234	33.412	7.9965	-0.0008	268.76
Barbara	R	99.6095	29.6291	7.9964	-0.0075	227.58
	G	99.6175	29.7659	7.9965	-0.0021	219.45
	B	99.6234	31.1576	7.9965	-0.0008	228.76
Average		99.3944	33.7690	7.9980	-0.0028	-

7.2. Additional Comparison with AES-128 and AES-256

To further evaluate the performance of the proposed Hénon-Logistic encryption scheme, a comparative analysis was conducted against the AES-128 and AES-256 algorithms. All three methods were evaluated using the same Lena image and an identical data size of 268,098 bytes. The comparison considers several performance indicators, including NPCR, UACI, Shannon entropy, correlation coefficient, chi-square statistics, selected NIST statistical tests, encryption throughput, and nominal key-space size. These metrics provide complementary insights into the

statistical properties, sensitivity to plaintext changes, randomness, and computational performance of the proposed scheme relative to the two AES configurations. The comparative results are summarized in Table 2.

Table 2. Comparative Statistical Security and Performance Evaluation of the Proposed Hénon-Logistic Encryption Scheme, AES-128, and AES-256 Using the Lena Image.

Metric	Hénon-Logistic	AES-128	AES-256
Bytes	268098	268098	268098
NPCR (%)	99.5957	99.6330	99.6184
UACI (%)	33.5034	33.4824	33.5235
Entropy	7.9993	7.9994	7.9994
Correlation	0.0004	0.0003	-0.0018
χ^2	222.37	237.93	236.32
χ^2 critique	293.25	293.25	293.25
χ^2 : pass	Yes	Yes	Yes
NPCR diff. (%)	99.988	99.63	99.58
UACI diff. (%)	33.76	33.49	33.61
NIST Frequency p	0.4981	0.2138	0.6196
NIST Block Frequency p	0.7021	0.1011	0.3177
NIST Runs p	0.2379	0.6383	0.3665
NIST Longest Run p	0.8252	0.0927	0.7303

Metric	Hénon-Logistic	AES-128	AES-256
Flow Rate (Mbit/s)	3.93	3.16	3.83
Nominal space (bits)	320	128	256

8. Conclusion

This study proposed a hybrid Hénon-Logistic chaotic encryption scheme (HCES) combining dynamically coupled chaotic maps, a dynamic S-box, and confusion-diffusion operations for image encryption. Dynamical analysis and experiments on six standard test images demonstrated promising results, including ciphertext entropy approaching 8 bits and correlation coefficients close to zero. In comparison with AES-128 and AES-256, the proposed scheme achieved an entropy of 7.9993, a correlation coefficient of 0.0004, and an encryption throughput of 3.93 Mbit/s under the reported experimental conditions. These findings highlight its potential for image encryption. However, further investigations into effective key space, S-box security, resistance to cryptographic attacks, and performance on resource-constrained devices are necessary before practical deployment can be recommended.

Reference

- [1] M. Huo, Y. Zheng, and J. Huang, "Enhancing AES image encryption with a three-dimensional hyperchaotic system for increased security and efficiency," *PLoS One*, vol. 20, no. 7, p. e0328297, Jul. 2025, doi: 10.1371/journal.pone.0328297.
- [2] R. V. Chothé, S. P. Ugale, D. M. Chandwadkar, and S. V. Shelke, "Authenticated image encryption using robust chaotic maps and enhanced advanced encryption standard," *IJECS*, vol. 37, no. 3, p. 1543, Mar. 2025, doi: 10.11591/ijeecs.v37.i3.pp1543-1554.
- [3] M. Vamsikrishna *et al.*, "A Modified Chaos-Driven Enhanced Cryptographic Framework for Lightweight and Robust IoT Security in Resource-Constrained Devices," *Int J Comput Intell Syst*, vol. 19, no. 1, p. 71, Feb. 2026, doi: 10.1007/s44196-026-01181-7.
- [4] M. Helmy and H. Torkey, "Secured Audio Framework Based on Chaotic-Steganography Algorithm for Internet of Things Systems," *Computers*, vol. 14, no. 6, p. 207, May 2025, doi: 10.3390/computers14060207.
- [5] W. Alexan, N. H. E. Shabasy, N. Ehab, and E. A. Maher, "A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations," *Sci Rep*, vol. 15, no. 1, p. 31246, Aug. 2025, doi: 10.1038/s41598-025-15794-z.
- [6] R. K. Muhammed *et al.*, "Comparative Analysis of AES, Blowfish, Twofish, Salsa20, and ChaCha20 for Image Encryption," *KJAR*, vol. 9, no. 1, pp. 52–65, May 2024, doi: 10.24017/science.2024.1.5.
- [7] M. Naim and A. Ali Pacha, "A new chaotic image encryption algorithm based on a modified version of the AES algorithm," *Multimed Tools Appl*, vol. 84, no. 18, pp. 19693–19722, Jul. 2024, doi: 10.1007/s11042-024-19842-0.
- [8] Farah Tawfiq Abdul Hussien and Teaba Wala Aldeen Khairi, "Performance Evaluation of AES, ECC and Logistic Chaotic Map Algorithms in Image Encryption," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 10, pp. 193–211, May 2023, doi: 10.3991/ijim.v17i10.38787.
- [9] M. S. Khan, A. Al-Dubai, J. Ahmad, N. Pitropakis, and B. Ghaleb, "A Novel Feature-Aware Chaotic Image Encryption Scheme For Data Security and Privacy in IoT and Edge Networks," in *2025 International Joint Conference on Neural Networks (IJCNN)*, Rome, Italy: IEEE, Jun. 2025, pp. 1–7. doi: 10.1109/IJCNN64981.2025.11227573.

- [10] U. Zia *et al.*, “Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains,” *Int. J. Inf. Secur.*, vol. 21, no. 4, pp. 917–935, Aug. 2022, doi: 10.1007/s10207-022-00588-5.
- [11] T. Umar, M. Nadeem, and F. Anwer, “Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage,” *Expert Systems with Applications*, vol. 257, p. 125050, Dec. 2024, doi: 10.1016/j.eswa.2024.125050.
- [12] D. Alexandru and F. Madalin, “Image encryption using chaotic maps: Development, application, and analysis,” *Mathematics*, vol. 13, no. 16, p. 2588, 2025.
- [13] F. Asiri and W. A. Malwi, “Enhancing Post-Quantum Information Security: A Novel Two-Dimensional Chaotic System for Quantum Image Encryption,” *CMES*, vol. 143, no. 2, pp. 2053–2077, 2025, doi: 10.32604/cmes.2025.064348.
- [14] A. Al-Hyari, M. Abu-Faraj, C. Obimbo, and M. Alazab, “Chaotic Hénon–Logistic Map Integration: A Powerful Approach for Safeguarding Digital Images,” *JCP*, vol. 5, no. 1, p. 8, Feb. 2025, doi: 10.3390/jcp5010008.
- [15] B. Yogi, R. Majumdar, P. Ghosh, L. Sharma, and S. Roy, “SCD-CHAOS: dynamic S-box and chaotic hybrid adaptive image encryption using multi-map diffusion,” *Sci Rep*, vol. 16, no. 1, p. 15818, Apr. 2026, doi: 10.1038/s41598-026-43981-z.
- [16] S. Mohi Ud Din, T. Shah, F. Alblehai, S. Nooh, and S. S. Jamal, “A combinatory approach of non-chain ring and henon map for image encryption application,” *Sci Rep*, vol. 15, no. 1, p. 1781, Jan. 2025, doi: 10.1038/s41598-025-85814-5.
- [17] “A Modified Henon Map Based Image Encryption Framework | SN Computer Science | Springer Nature Link.” Accessed: Aug. 05, 2026. [Online]. Available: <https://link.springer.com/article/10.1007/s42979-025-04216-6>
- [18] R. Amutha and A. V. Phamila, “Chaotic cosine and logistic map based robust image encryption with dual-stage confusion–diffusion architecture,” *Sci Rep*, vol. 16, no. 1, p. 16951, Apr. 2026, doi: 10.1038/s41598-026-40337-5.
- [19] F. Nujumudeen *et al.*, “A hybrid chaos-based cryptographic framework for lightweight IoT security: enhancing efficiency and security in low-power devices,” *Peer-to-Peer Netw. Appl.*, vol. 19, no. 2, p. 53, Feb. 2026, doi: 10.1007/s12083-025-02188-1.