

REVIEWER'S REPORT

Manuscript No.: IJAR-59434

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

Recommendation:

Accept as it is

Accept after minor revision.....

Accept after major revision ...✓.....

Do not accept (*Reasons below*)

Reviewer's ID: JPR- **098**

Rating	Excel.	Good	Fair	Poor
Originality		✓		
Techn. Quality		✓		
Clarity		✓		
Significance		✓		

Detailed Reviewer's Report

Decision: Accept after Major Revision

Major Comments

1. Novelty and Research Contribution Require Stronger Justification

The manuscript proposes a hybrid Hénon–Logistic chaotic generator with a dynamic S-box. However, similar hybrid chaotic maps and dynamic S-box-based encryption schemes already exist. The authors should clearly distinguish the proposed method from existing Hénon–Logistic approaches and demonstrate its specific technical contribution.

2. Mathematical Formulation of the Hybrid Generator Needs Clarification

The manuscript describes the coupling as bidirectional in the introduction but later explicitly defines it as unidirectional, with the Hénon map driving the Logistic parameter. This inconsistency must be resolved. All governing equations, parameter ranges, initialization values, normalization procedures, and boundary conditions should be stated consistently.

3. Reproducibility of the Encryption and Decryption Algorithms Is Insufficient

The algorithm outlines chaotic initialization, S-box generation, keystream generation, and pixel diffusion, but important implementation details are

REVIEWER'S REPORT

missing. The authors should provide complete encryption and decryption pseudocode, including byte conversion, feedback operations, inverse transformations, and handling of different image dimensions and color channels.

4. Security of the Dynamic S-Box Requires Deeper Analysis

The S-box is generated using a double-sorting procedure, but bijectivity alone does not establish cryptographic strength. The manuscript itself identifies nonlinearity, the Strict Avalanche Criterion (SAC), the Bit Independence Criterion (BIC), and differential probabilities as relevant criteria. These properties should be evaluated quantitatively and compared with established S-box benchmarks.

5. Effective Key Space and Key Sensitivity Need Rigorous Validation

The manuscript reports a nominal key space of 320 bits for the proposed scheme. However, the effective key space depends on the actual independent secret parameters, their precision, valid parameter ranges, and implementation constraints. The authors should justify the reported value and investigate key sensitivity, weak-key possibilities, and finite-precision effects.

6. Statistical Results Contain Values That Require Verification

Table 1 reports a substantially lower NPCR value for the green channel of the Peppers image than for the other channels. Some reported UACI values also vary considerably across images and channels. The authors should verify the calculations, explain deviations, and report reproducible results using clearly defined experimental procedures. Summary statistics should be recalculated where necessary.

7. NPCR and UACI Results Need a More Rigorous Interpretation

Although the manuscript reports NPCR and UACI values, these metrics alone do not establish resistance to differential cryptanalysis. The authors should explain how the measurements were obtained, provide appropriate theoretical reference values or statistical tests, and discuss the implications of deviations from expected behavior.

8. NIST Statistical Testing Is Insufficiently Documented

The manuscript reports selected NIST statistical-test p-values but does not adequately describe the tested sequences, sequence lengths, number of

REVIEWER'S REPORT

independent trials, significance threshold, or pass-rate criteria. The authors should provide a reproducible testing protocol and avoid treating a few passing tests as proof of cryptographic security.

9. Comparison with AES-128 and AES-256 Requires Fairer Experimental Conditions

The comparison reports differences in entropy, correlation, statistical metrics, and throughput. However, the implementation details, software libraries, hardware environment, timing procedure, and treatment of encryption modes are not sufficiently specified. The authors should conduct a controlled comparison and clarify that statistical image metrics alone cannot establish superiority over standardized AES encryption.

10. Security Claims and Practical Applicability Should Be Reconsidered

The manuscript concludes that the proposed method has promising potential, while acknowledging that further security analysis is required. The discussion should more explicitly address known risks associated with finite-precision chaotic systems, possible chosen-plaintext and chosen-ciphertext attacks, key management, and the absence of a formal cryptographic security argument. Claims should be limited to what the experiments actually demonstrate.

Minor Comments**1. Correct the Title and Scope Consistency**

The title focuses on image encryption, whereas the introduction also mentions text encryption. Please clarify the actual scope of the implemented and evaluated system.

2. Improve the Abstract

The abstract should briefly identify the research gap, explain the principal algorithmic innovation, summarize the evaluation protocol, and state the main findings without implying stronger security guarantees than the evidence supports.

3. Standardize Mathematical Notation

The manuscript uses inconsistent notation for the Hénon and Logistic state variables and contains formatting issues in equations and parameter values. All

REVIEWER'S REPORT

symbols, subscripts, superscripts, and decimal conventions should be standardized.

4. Explain the Warm-Up and Normalization Procedures

The authors should specify the number of discarded transient iterations and explain how ($X_{\max}$) is calculated. The normalization expression used to convert chaotic values into the interval required for S-box generation should also be clearly defined.

5. Improve the Presentation of Figures 1 and 2

The figures should use legible axis labels, consistent notation, clearly identified parameter ranges, and adequate resolution. The Lyapunov-exponent plots should include sufficient information to interpret their numerical values.

6. Clarify the Image Dataset

The manuscript refers to six standard test images, but the selection criteria and image properties are not fully documented. Please report image dimensions, bit depth, color format, and source, and explain whether all images were processed under identical conditions.

7. Correct Table Formatting and Statistical Reporting

Table 1 contains repeated caption wording and inconsistent decimal precision. Please standardize the formatting, clearly identify channel-wise results, and explain how the average values were calculated.

8. Define Performance Metrics Precisely

The terms “Flow Rate” and “Nominal space” should be replaced or accompanied by clear definitions. The throughput measurement should specify whether preprocessing, key generation, S-box construction, and decryption are included.

9. Strengthen the Literature Review and References

The literature review should more directly compare the proposed scheme with closely related chaotic image-encryption methods. Please ensure that all cited works are accurately referenced and that the relevant prior Hénon–Logistic approaches are discussed critically.

10. Improve Language, Structure, and Section Numbering

The manuscript contains grammatical errors, inconsistent capitalization, and

International Journal of Advanced Research

Publisher's Name: Jana Publication and Research LLP

www.journalijar.com

REVIEWER'S REPORT

section-numbering problems. Please proofread the complete document, correct typographical errors, and ensure consistent terminology throughout.