

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 yes...

Do not accept (*Reasons below*)

Rating	Excel.	Good	Fair	Poor
Originality			Y	
Techn. Quality			Y	
Clarity			Y	
Significance			y	

Reviewer's ID: JPR-Dr.Shaweta Sachdeva

Detailed Reviewer's Report

1. The manuscript proposes a hybrid Hénon–Logistic chaotic encryption scheme for image encryption. However, the novelty of the proposed approach relative to existing chaos-based image encryption techniques is not sufficiently established. The authors should clearly identify the specific methodological contributions and explain how the proposed system differs from previously published hybrid chaotic encryption frameworks.
2. The mathematical formulation of the hybrid chaotic generator requires further clarification. In Section 2.3, the Logistic parameter is modulated by the Hénon trajectory, but the normalization procedure involving $(X_{\max})$ is not described in sufficient detail. The authors should specify how this bound is calculated, how it affects the generated sequence, and whether the same procedure remains valid across different initial conditions and parameter settings.
3. The authors should provide a more rigorous mathematical validation of the chaotic behaviour of the proposed generator. Although Figures 1 and 2 present time series, phase portraits, bifurcation diagrams, and Lyapunov-exponent plots, the numerical values of the Lyapunov exponents and the precise computational procedures are not adequately reported. The number of transient iterations, total iterations, parameter ranges, and numerical estimation method should be specified to ensure reproducibility.
4. The manuscript describes the proposed Hénon–Logistic coupling as a hybrid generator. However, Section 2.3 explicitly indicates that the coupling is unidirectional rather than bidirectional, whereas the Introduction refers to bidirectional coupling. This inconsistency must be resolved, and the system architecture and terminology should be revised accordingly.
5. The construction of the dynamic S-box using the double-sorting procedure ($S = \text{argsort}(\text{argsort}(s))$) guarantees a permutation under appropriate conditions, but bijectivity alone does not establish cryptographic strength. The authors should evaluate the S-box using established criteria, including nonlinearity, the Strict Avalanche Criterion (SAC), the Bit Independence Criterion (BIC), and differential uniformity or differential probability. These results are important for assessing the security of the proposed substitution mechanism.

REVIEWER'S REPORT

6. The key-space analysis requires substantial strengthening. The reported nominal key space of 320 bits appears to be based on the selected key parameters, but the effective key space may be significantly smaller because of finite numerical precision, parameter constraints, and equivalent initial conditions. The authors should explain the assumed precision and entropy of each key component and calculate the effective key space rather than relying solely on the nominal number of bits.
7. The security analysis is primarily based on statistical measures such as entropy, correlation coefficients, NPCR, UACI, and chi-square tests. Although these metrics are useful, they do not independently establish resistance to cryptographic attacks. The authors should analyse the proposed algorithm against relevant threats, including chosen-plaintext attacks, known-plaintext attacks, brute-force attacks, and differential attacks. A clear threat model and a discussion of the algorithm's limitations are required.
8. The comparison with AES-128 and AES-256 requires a more rigorous and transparent experimental methodology. The authors should specify the implementation libraries, hardware configuration, software environment, operating conditions, and timing methodology used for all algorithms. In particular, the comparison should distinguish between a custom image-encryption procedure and standardized AES implementations, including the mode of operation and any associated initialization or authentication mechanisms.
9. There are inconsistencies in the statistical results that require careful verification. For example, Table 1 reports an average UACI of 33.7690%, whereas several individual entries are substantially lower, including the values for the Barbara image. Similarly, the green channel of the Peppers image has an NPCR of 96.5825%, which is notably lower than most other reported values. The authors should recalculate the aggregate statistics, verify the underlying experimental results, and explain any deviations from expected values.
10. The interpretation of the NPCR and UACI results requires further clarification. Table 2 reports differential NPCR and UACI values for the proposed method and AES variants, but the manuscript does not sufficiently explain the procedure used to generate these measurements. The authors should describe how the one-pixel plaintext modification was introduced, how many trials were conducted, and whether the reported values are averages over repeated experiments.
11. The NIST statistical testing results should be reported more comprehensively. The manuscript presents p-values for selected tests, but it does not sufficiently describe the sequence length, number of tested sequences, significance level, pass proportions, or testing configuration. The authors should provide enough information to reproduce the tests and avoid interpreting acceptable p-values as conclusive proof of cryptographic security.
12. The experimental evaluation is limited to six standard images. The authors should consider expanding the evaluation to include images of different dimensions, textures, intensity distributions, and colour characteristics. Repeated experiments and additional image datasets would provide a more reliable assessment of the generalizability and robustness of the proposed encryption scheme.
13. The paper claims improved computational performance based on the reported throughput of 3.93 Mbit/s compared with AES-128 and AES-256. However, the manuscript does not adequately explain whether the measurements include chaotic sequence generation, S-box construction, encryption, and other preprocessing operations. The authors should report the complete computational cost and compare the algorithms under equivalent implementation conditions.
14. The proposed encryption and decryption algorithms require more detailed implementation specifications. The authors should provide complete pseudocode, define all variables and indexing conventions, explain the conversion of chaotic values into bytes, and clarify the feedback mechanism used during diffusion. These details are essential for independent implementation and verification of the reported results.

REVIEWER'S REPORT

15. The manuscript's claims regarding image encryption and text encryption should be made consistent. The Introduction refers to both image and text encryption, whereas the experimental evaluation focuses primarily on image encryption. The authors should either provide appropriate experimental validation for text encryption or restrict the scope and claims of the manuscript to the application that has actually been evaluated.
16. The literature review should be strengthened through a more systematic comparison with recent chaos-based image encryption methods. A comparative table should summarize the underlying chaotic maps, S-box construction techniques, security evaluation criteria, computational complexity, and reported limitations of representative approaches. This would help establish the research gap and demonstrate the practical significance of the proposed method.
17. The figures and tables require technical revision. Figures 1 and 2 should include clearly readable axis labels, parameter values, units where applicable, and sufficient resolution. Table 1 should be checked for numerical consistency and formatting, while Table 2 should clearly distinguish statistical randomness, differential sensitivity, computational performance, and key-space estimates. Duplicate table numbering and inconsistencies in figure references should also be corrected.
18. The conclusion should provide a more balanced assessment of the findings. Rather than emphasizing favourable statistical results alone, the authors should discuss the principal limitations of the proposed scheme, the unresolved security questions, and the additional cryptanalysis required before practical deployment. The conclusions should remain proportional to the evidence presented in the experiments.

Overall recommendation

Major Revision

The manuscript addresses a relevant problem in image encryption and presents a potentially interesting hybrid chaotic framework. However, substantial revisions are necessary to establish the novelty, mathematical correctness, reproducibility, and cryptographic security of the proposed method. Particular attention should be given to the inconsistency concerning unidirectional versus bidirectional coupling, the validation of the dynamic S-box, the effective key-space calculation, and the verification of the statistical results reported in Tables 1 and 2.