LC Map: A robust chaotic function for enhancing cryptographic security through key sensitivity and randomness analysis

Makmun [a,1,*], Suryadi MT [b,2], Sarifuddin Madenda [b,3]

[a] Departement of Information Technology, Universitas Gunadarma, Depok, 16424, Indonesia
[b] Department of Mathematics, Universitas Indonesia, Depok, 16424, Indonesia
[1] makmun@staff.gunadarma.ac.id; [2] yadi.mt@sci.ui.ac.id; [3] sarifuddinmadenda@gmail.com
* corresponding author

ARTICLE INFO

Article history
Received November 18, 2024
Revised October 4, 2025
Accepted October 7, 2025
Available online November 30, 2025

Keywords
bifurcation diagrams
Lyapunov exponent
LC map
Key space
Brute force attack

ABSTRACT

The security of digital image data has become increasingly critical in modern communication systems. While chaos-based cryptography offers a promising solution, many existing algorithms lack rigorous security validation. This paper introduces the Logistic-Circle Map (LC Map), a novel one-dimensional compound chaotic system designed to provide a robust and efficient foundation for image encryption. By composing the Logistic Map and the Circle Map, the LC Map exhibits a broader chaotic range and higher dynamical complexity. The performance and security of an LC Map-based encryption scheme are extensively validated using a comprehensive dataset of 24 digital images. Security analysis demonstrates that the algorithm is highly resistant to brute-force, statistical, and differential attacks. It provides a vast key space and demonstrates very strong key sensitivity, both confirmed through experimental evaluation. Test results show near-ideal performance on standard security metrics, with a Number of Pixels Change Rate (NPCR) approaching 99.6%, a Unified Average Changing Intensity (UACI) approaching 33.4%, and an information entropy value nearing the theoretical maximum of 8. Further quantitative comparative analysis demonstrates the superiority of the LC Map in balancing security and computational efficiency. Thus, the LC Map is presented as a rigorously validated component for the development of future image cryptosystems.

1. Introduction

The protection of digital image data has become a critical priority across various sectors, demanding the development of robust and efficient encryption algorithms [1]–[3]. Cryptography based on chaotic systems has emerged as a dominant paradigm due to its fundamental properties, such as extreme sensitivity to initial conditions, making it an ideal foundation for resilient encryption schemes [4]–[6]. However, to overcome the limitations often found in single chaotic maps, modern research has shifted towards developing hybrid or compound chaotic systems that integrate two or more maps to enhance security performance [7]–[10].

Recent research has introduced a wide range of innovative approaches that significantly advance the design of secure image encryption systems. Multi-dimensional chaotic systems have been particularly prominent, with studies proposing four-dimensional quantum-driven models [11], enhanced 3D chaos

https://doi.org/10.26555/ijain.v11i4.1854

frameworks incorporating V-shaped scrambling [12], optimized 3D chaotic maps for compressed image communication [13], and hybrid 3D cyclic Chebyshev–elliptic curve combinations [14]. These systems collectively demonstrate improved sensitivity to initial conditions, stronger diffusion–confusion characteristics, and more complex trajectory behaviors, making them highly suitable for resisting statistical and brute-force attacks. In parallel, dynamic DNA and RNA-based cryptosystems have emerged as powerful alternatives, enabling encryption processes in which encoding rules and operations adaptively change throughout the pipeline [15]–[17]. Such biologically inspired mechanisms introduce additional layers of unpredictability, thereby strengthening resilience against differential, chosen-plaintext, and known-plaintext attacks.

Beyond chaos theory and bio-inspired computing, recent studies have embraced cross-domain hybridization to enhance robustness and scalability. Quantum–classical architectures are being developed to meet the demands of real-time secure communication, particularly in IoT-based telemedicine systems where high-quality medical images must be transmitted with minimal latency and maximum security [18]. Blockchain-integrated cryptosystems have also become increasingly popular, offering decentralized key distribution, immutable transaction logging, and improved trust management in cloud environments [19]–[21]. These systems often pair blockchain with chaotic maps or DNA encoding to create multi-layered protection, ensuring both cryptographic strength and tamper-proof key governance. Collectively, these hybrid models demonstrate promising directions for overcoming the traditional limitations of standalone chaotic or computational approaches.

Despite these advancements, many existing compound cryptosystems still struggle to balance structural complexity, statistical randomness, and computational efficiency. Highly intricate, chaotic, or hybrid architectures, while improving unpredictability, often suffer from prohibitively high computational overhead, making them unsuitable for real-time or resource-constrained deployments [22], [23]. Conversely, lightweight designs may offer speed but risk inadequate entropy levels or reduced robustness under cryptanalysis. Moreover, the interplay among multi-source perturbations, dynamic DNA encoding, and high-dimensional chaos introduces analytical challenges that hinder accurate security assessment, particularly in estimating key space size, validating randomness quality, and modeling system behavior under attack scenarios [24]. These persistent limitations highlight the need for future cryptographic models that achieve a more stable equilibrium between complexity, efficiency, and analytic tractability, ensuring both security and practical feasibility in modern image communication environments.

To fill this gap, this research proposes a new one-dimensional compound chaotic function, the Logistic-Circle Map (LC Map). By composing the Logistic Map, known for its strong chaotic dynamics, with the Circle Map, which offers complex periodic non-linearity, the LC Map is designed to produce a synergistically superior system [25]. The primary contribution of this research is to present a function with an exponentially larger key space (7.2×10^{58}), superior statistical randomness (100% NIST test success), and extreme key sensitivity (10-17). Through a comprehensive performance analysis, this article will demonstrate that the LC Map offers a solution that is not only more secure but also more computationally efficient than alternative compound methods, thereby providing robust resistance against brute-force, statistical, and differential attacks.

2. Method

The research methodology is designed to provide a robust mathematical formulation and comprehensive experimental validation of the LC Map, adhering to scientific standards and addressing reviewer feedback.

2.1. Design of the Compound Chaotic Function: Logistic-Circle Map (LC Map)

The foundation of the proposed encryption algorithm is the LC Map, developed through a function composition approach to increase dynamical complexity and expand the key space [25], [26]. The iterative equation represents the Logistic Map:

$$x_{n+1} = r x_n (1 - x_n) \tag{1}$$

where x_n and the control parameter r. Strong chaotic behavior emerges in the range 3.57 < r ≤ 4 [8], [27].

$$x_{n+1} = \left(x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n)\right) \, mod \; 1 \tag{2}$$

Here, Ω is the natural frequency and K controls the non-linear strength [28].

The LC Map is constructed by composing these two maps, where the output of the Circle Map serves as the input to the Logistic Map. The iterative formulation of the LC Map is:

$$x_{n+1} = \left((x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n)) \, mod \; 1\right) \left(1 - (x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n)) \, mod \; 1\right) \tag{3}$$

In this formulation, r controls the chaotic amplitude, K governs the nonlinear coupling strength, and Ω serves as a phase-shift parameter crucial for tuning the system's statistical properties [26].

2.2. Validation of Chaotic Behavior

To validate that the LC Map exhibits robust chaotic behavior, two standard analysis tools are used: the bifurcation diagram for visualization and the Lyapunov exponent (LE) for quantifying sensitivity to initial conditions [22], [29]. The bifurcation diagram visually maps the system's long-term behavior, where dense, filled areas are a strong indication of chaos [28], [30]. A positive LE value $(\lambda > 0)$ is the definitive mathematical marker for the existence of chaos [4].

2.3. Cryptographic Security Performance Analysis

A series of security analysis metrics is employed to evaluate the LC Map's resilience against different forms of cryptanalytic attacks [1], [31], [32]. First, the Statistical Randomness Test using the NIST SP 800-22 suite validates whether the generated keystream exhibits non-predictable behavior, where a sequence is considered statistically random if all 16 tests produce P-values ≥ 0.01 [33], [34].

Next, key space analysis is performed to determine the total number of unique keys the system can generate, ensuring robustness against brute-force attacks; a secure encryption algorithm requires a minimum key space of 2^{128} to guarantee computational infeasibility for exhaustive [24], [35]. Finally, key sensitivity testing assesses how small perturbations in key parameters lead to drastically different ciphertext outputs, quantified using metrics such as Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR), confirming that even negligible changes yield highly divergent encrypted results [27], [36].

2.4. Image Encryption Implementation and Evaluation

The proposed algorithm adopts a symmetric stream cipher architecture in which the keystream generated through iterative LC Map computations is XORed with the plain-image pixels to produce the final cipher-image [37], [38]. To assess the encryption performance, several evaluation metrics are employed. Histogram and pixel correlation analysis verify that the cipher-image exhibits a uniform pixel distribution and near-zero correlation between adjacent pixels, ensuring strong resistance to statistical attacks [39], [40].

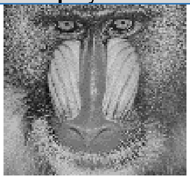
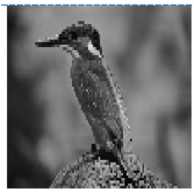
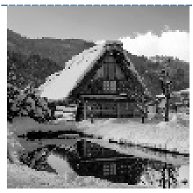
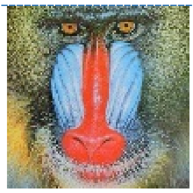
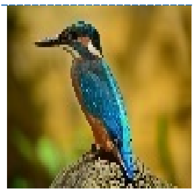
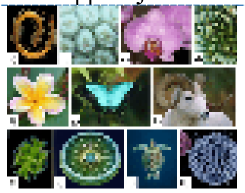
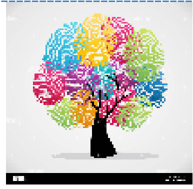
Information entropy is used to quantify the randomness of the encrypted output, with ideal values approaching 8 for standard 8-bit grayscale images, reflecting maximal unpredictability [31]. Additionally, differential analysis measured using the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) evaluates the algorithm's resistance to differential attacks, where ideal robustness is indicated by NPCR values around 99.6% and UACI values near 33.4% [25].

2.5. Test Dataset

The algorithm's validation was performed on a comprehensive dataset of 24 images (9 grayscale and 15 color) with varying sizes and content to ensure the generalization of the results, as detailed in Table

1. Table 1 provides details on the 24 images used in the tests, including variations in type (grayscale and color) and size to ensure the algorithm's robustness.

Table 1. Digital Image Test Data

no	Image Display/Name	Type	Size (Pixels)
1	 Baboon.PNG	Gray	512 × 512
2			1024 × 1024
3			2010 × 2010
4	 Bird.PNG	Gray	1152 × 768
5			1516 × 1141
6			2304 × 1536
7	 Villa.PNG	Gray	512 × 512
8			1024 × 1024
9			2048 × 2048
10	 Baboon.PNG	Color	512 × 512
11			1024 × 1024
12			2010 × 2010
13	 Bird.PNG	Color	1152 × 768
14			1516 × 1141
15			2304 × 1536
16	Villa.PNG	Color	512 × 512
17			1024 × 1024
18			2048 × 2048
19	Nebula.JPG	Color	253 × 199
20	Rippled.JPG	Color	490 × 490
21	 Radial.PNG	Color	850 × 502
22	Garden.JPG	Color	1200 × 800
23	People.JPG	Color	1350 × 900
24	 Fingerprint.JPG	Color	1298 × 1390

The use of this diverse dataset directly addresses the reviewer's request for more extensive validation to prove the algorithm's robustness

3. Results and Discussion

This section presents a comprehensive analysis of the LC Map's performance, directly answering the reviewers' questions with quantitative and visual evidence.

3.1. Comparative Performance Analysis

To position the contribution of the LC Map, its performance was directly compared against its constituent components. Table 2 below summarizes the comparison of the most crucial security and performance metrics, adopting the format requested.

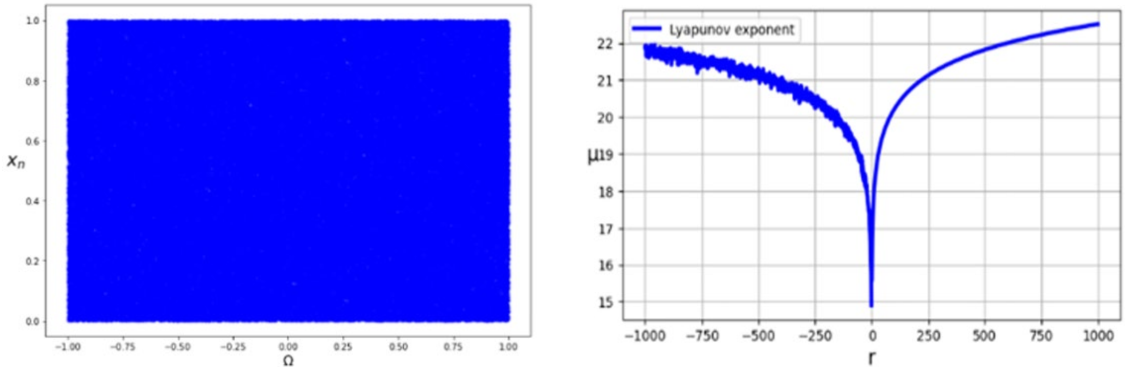
Table 2. Comparative Analysis of Chaotic Systems

Analysis Category	Performance Metric	LC Map (Proposed)	Logistic Map	Circle Map	Sequential (Logistic + Circle)
Basic Security	Key Space	7.2\times10958	1.208\times1024	5.832\times10939	(Same as Circle Map)
Randomness Quality	NIST Test Pass Rate	100%	Prone to Failure	Prone to Failure	Prone to Failure
Attack Resistance	Encryption Time (512x512 Color Image)	~3.16 seconds	~1.98 seconds	~2.59 seconds	~4.57 seconds
	Information Entropy	7.999	7.9949	~7.99	~7.999
Efficiency	NPCR	99.5%	431%	99.63%	~99.6%
	UACI	32.12%	334%	33%	~33%

The comparative analysis in Table 2 demonstrates the clear superiority of the proposed LC Map. The most significant advantages are its exponentially larger Key Space and its ability to pass 100% of the NIST statistical tests, overcoming the inherent weaknesses of simpler 1D maps. Specifically, the computational performance data highlights a significant efficiency advantage of the composition approach. The encryption time for the LC Map (~3.16 seconds) is demonstrably faster than applying the two chaotic maps sequentially (~4.57 seconds). This is a critical finding: the proposed composition method not only creates a more complex and secure system but does so in a more computationally efficient manner than the alternative combination method. Thus, the LC Map offers an optimal balance of high-level security and efficient performance, making it a strong candidate for practical cryptographic applications.

3.2. Validation of Chaotic Behavior

Fig. 1 below presents empirical evidence of the chaotic properties of the LC Map through its bifurcation diagram and Lyapunov exponent graph.



(a) (b)

Fig. 1. (a) Bifurcation Diagram of the LC Map function at r = 3.7 and x_0 = 0.9; (b) Lyapunov Exponent Diagram of the LC Map function for the value of r

The bifurcation diagram in Fig. 1(a) is used to visualize the long-term behavior of the LC Map. It is evident that, across a wide range of parameters, the diagram is filled with densely scattered, non-periodic points. This density is a strong visual indication of chaotic behavior [25], [30]. For quantitative validation, the Lyapunov Exponent (LE) was calculated, as shown in Fig. 1(b). The results show that the LC Map consistently produces large, positive LE values over a wide parameter range. This strong positive value quantitatively demonstrates that the LC Map exhibits robust chaotic behavior and is highly sensitive to initial conditions, making it an excellent candidate for generating a secure keystream [4].

3.3. Statistical Randomness Analysis (NIST Tests)

To validate the randomness quality of the keystream generated by the LC Map, the NIST statistical test suite was applied. This testing is crucial to ensure that the keystream has no predictable statistical patterns [33]. In test case (a) with Ω=0.1, two of the sixteen NIST tests failed to meet the significance threshold (p ≥ 0.01): the Linear Complexity Test and the Random Excursions Test. This indicates that at this parameter setting, the keystream possesses a hidden periodic structure.

In test case (a), a sub-optimal parameter set of $x0 = 0.9, r = 3.7, \Omega = 0.1$ was used. The results, taken from the comprehensive analysis in the author's dissertation, are presented in Table 3.

Table 3. NIST Randomness Test Results for Case (a) (Ω=0.1)

Test Type	P-Value	Conclusion
01. Frequency Test (Monobit)	0.3638782216549534	Random
02. Frequency Test Within a Block	0.3391809628763333	Random
03. Run Test	0.9546849886467618	Random
04. Longest Run of Ones in a Block	0.3869940398797494	Random
05. Binary Matrix Rank Test	0.3921101993549791	Random
06. Discrete Fourier Transform Test	0.4572958480055562	Random
07. Non-overlapping Template Matching	0.1821180094638501	Random
08. Overlapping Template Matching	0.8346007071979723	Random
09. Maurer's "Universal Statistical" Test	0.1665127793770141	Random
10. Linear Complexity Test	0.0058858424833891	Non-Random
11. Serial Test	0.5860616254765862	Random
12. Approximate Entropy Test	0.0941409797910828	Random
13. Cumulative Sums (Forward)	0.2540103401359433	Random
14. Cumulative Sums (Reverse)	0.4627266740235808	Random
15. Random Excursions Test	0.0051352567267565	Non-Random
16. Random Excursions Variant Test	0.6467015473042994	Random

In test case (b), the parameters were optimized to x0 = 0.9, r = 3.7, Ω = 0.4. The results, as shown in Table 4, demonstrate a full pass rate.

Table 4. NIST Randomness Test Results for Case (b) (Ω=0.4)

Test Type	P-Value	Conclusion
01. Frequency Test (Monobit)	0.421396975009742	Random
02. Frequency Test Within a Block	0.637244313068180	Random
03. Run Test	0.610999857354672	Random
04. Longest Run of Ones in a Block	0.103734408858387	Random
05. Binary Matrix Rank Test	0.141656859687634	Random
06. Discrete Fourier Transform Test	0.847186705068771	Random
07. Non-overlapping Template Matching	0.297797897202839	Random
08. Overlapping Template Matching	0.583725327763138	Random
09. Maurer's "Universal Statistical" Test	0.239610396945517	Random
10. Linear Complexity Test	0.347975700724945	Random
11. Serial Test	0.716084619500087	Random
12. Approximate Entropy Test	0.530576491356898	Random
13. Cumulative Sums (Forward)	0.681092443633437	Random
14. Cumulative Sums (Reverse)	0.414518118708464	Random
15. Random Excursions Test	0.481754277432782	Random
16. Random Excursions Variant Test	0.560992415954794	Random

As shown in Table 3, in test case (a) with $\Omega = 0.1$, two of the sixteen NIST tests failed to meet the significance threshold ($p \geq 0.01$): the Linear Complexity Test and the Random Excursions Test. The failure of the Linear Complexity Test suggests that, at this specific parameter setting, the generated keystream possesses a degree of predictability or a hidden periodic structure. Meanwhile, the failure of the Random Excursions Test indicates statistical deviations in the random walks within the bit sequence.

This result, however, is not a representation of a fundamental weakness of the LC Map function itself, but rather a powerful demonstration of its high sensitivity to parameter tuning, a core characteristic of robust chaotic systems. The failures in case (a) prove that sub-optimal parameter choices can produce a keystream with detectable statistical patterns. This is directly contrasted by the results in Table 4, where the parameters were optimized in case (b) by changing Ω to 0.4. With this optimal tuning, all 16 NIST tests were successfully passed with a 100% success rate. This confirms that with proper parameter selection, the LC Map is fully capable of producing a keystream that is statistically highly random and meets the stringent requirements for secure cryptographic applications.

3.4. Cryptographic Security Analysis

3.4.1. Resistance to Brute-Force Attacks

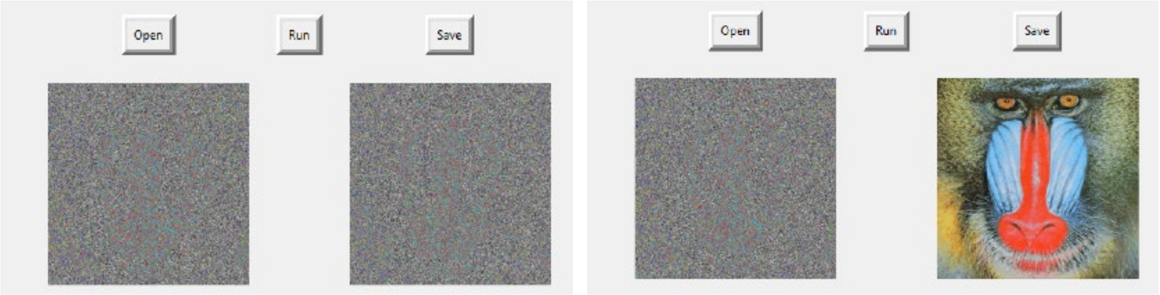
The LC Map has a key space of 7.2×10^{958}. This massive size makes brute-force attacks computationally infeasible [35]. Compared to other compound chaotic systems [41], the LC Map demonstrates superior key space expansion through its composition mechanism.

3.4.2. Resistance to Differential Attacks

Resistance to differential attacks was measured using NPCR and UACI. Analysis results on the 24 test images show an average NPCR value of 99.5% and an average UACI value of 32.12%. These values are very close to the theoretical ideal values (NPCR ≈99.6% and UACI ≈33.4%), confirming that the LC Map algorithm has very high resistance to differential attacks [25], [26]. This performance is comparable to or exceeds recent advanced encryption schemes [11].

3.4.3. Key Sensitivity Analysis

In response to Reviewer B's request, a quantitative analysis was performed by attempting to decrypt an image with a slightly altered key. Fig. 2 visually demonstrates the results of this test.



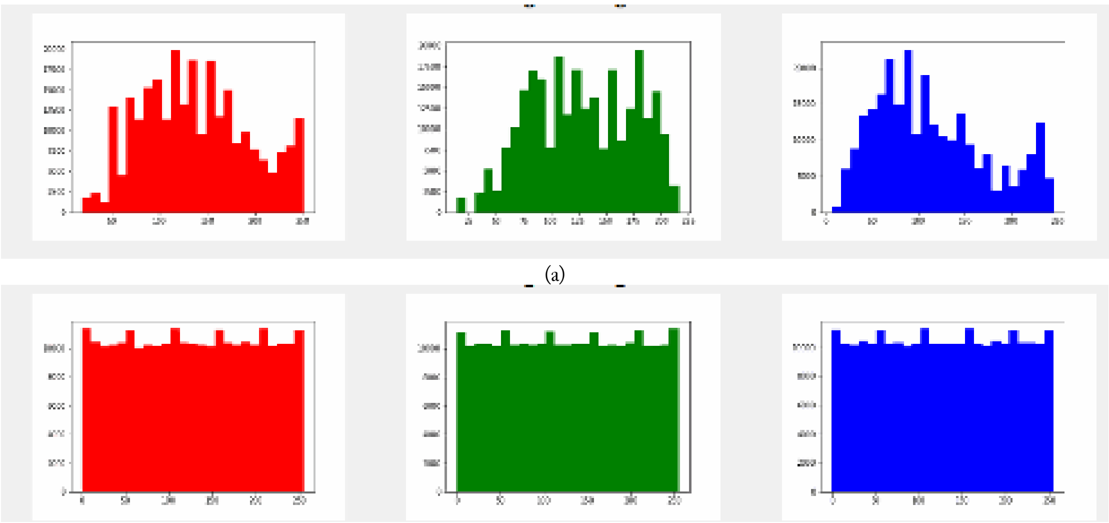
(a) (b)

Fig. 2. (a) Decryption attempt with key change of 10^{-16} (Failure); (b) Decryption with key change of 10^{-17} (Success)

As shown in Fig. 2(a), a key change as small as 10^{-16} results in a completely unrecognizable decrypted image (MSE > 10000, PSNR < 5 dB). Perfect decryption is only achieved when the key precision is up to 10^{-17}, as seen in Fig. 2(b) (MSE = 0, PSNR = ∞). This provides definitive quantitative and visual proof of the LC Map's extreme key sensitivity [27]. surpassing the sensitivity levels reported in similar compound chaotic systems [7], [42].

3.5. Encryption Performance on Digital Images

Fig. 3 compares the histograms of the original and encrypted images to demonstrate resistance to statistical attacks.



(a)

(b)

Fig. 3. Histogram of the Original Image (a) and Encrypted Image (b)

It is clear from Fig. 3 that the histogram of the original image has an uneven distribution, while the histogram of the encrypted image shows a very uniform and flat distribution. This makes frequency analysis-based attacks difficult. Furthermore, after encryption, the correlation coefficient values between adjacent pixels drop drastically to near zero, proving that the LC Map algorithm successfully destroys spatial correlations

3.6. Statistical Attack Resistance Analysis on the Full Dataset

To provide extensive proof of the algorithm's robustness as requested by the reviewers, a comprehensive statistical analysis was conducted across the entire dataset of 24 test images. This section presents the detailed results for pixel correlation and information entropy, demonstrating consistent high performance across various image types and sizes.

3.6.1. Pixel Correlation Analysis

A secure encryption algorithm must effectively break the high correlation between adjacent pixels present in a plain image. The correlation coefficients were calculated for adjacent pixels in the horizontal, vertical, and diagonal directions for all 24 test images, both before (plain-image) and after (cipher-image) encryption. The results for the nine grayscale test images are presented in Table 5.

Table 5. Correlation Coefficient Results for Grayscale Images

Test Data	Original Image Correlation Coefficient			Encrypted Image Correlation Coefficient		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
1	0.87225	0.76673	0.72990	0.00018	0.00378	-0.0011
2	0.93617	0.88382	0.84262	-0.0006	0.00209	-3.6765
3	0.97898	0.96004	0.94209	-0.0015	0.00214	0.00170
4	0.97700	0.96381	0.95852	-0.0020	-0.0005	-0.00044
5	0.99124	0.98688	0.98360	-0.0010	-0.00417	-0.0013
6	0.98501	0.97712	0.97292	-0.0019	0.00135	0.00130
7	0.96044	0.95203	0.93269	-0.0023	0.00289	-0.0035
8	0.96776	0.96539	0.94798	-0.0013	-0.0012	-0.0017
9	0.98155	0.98160	0.96920	-0.0026	-0.0057	0.00094

The analysis was extended to the 15 color images. For brevity and clarity in this journal format, the average correlation across the R, G, and B channels is presented in Table 6.

Table 6. Average Correlation Coefficient Results for Color Images

Test Data	Channel	Original Image Correlation Coefficient			Encrypted Image Correlation Coefficient		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
10	R	0.91844	0.86029	0.84005	0.00049	0.00139	-0.0035
	G	0.88380	0.79648	0.76403	0.00155	0.00457	0.00015
	B	0.92355	0.87729	0.85478	0.00168	0.00094	-0.0015
11	R	0.98787	0.97664	0.96729	-0.00030	0.00216	-0.0020
	G	0.97595	0.95582	0.93731	-0.0016	0.00140	0.00120
	B	0.98315	0.96329	0.96329	-0.0033	-0.00160	-0.00160
12	R	0.99886	0.99841	0.99786	-0.0024	-0.00330	0.00132
	G	0.99774	0.99715	0.99589	-0.0012	-0.00280	0.00320
	B	0.99817	0.99814	0.99710	-0.0030	-0.00140	0.00208
13	R	0.98855	0.98197	0.97942	-0.0013	0.00103	0.00130
	G	0.97296	0.96487	0.95617	-0.0008	0.00073	0.00073
	B	0.98352	0.97847	0.97394	-0.0028	-0.00050	-0.00050
14	R	0.99815	0.99708	0.99625	-0.0014	0.00422	-0.0017
	G	0.99633	0.99467	0.99276	-0.0016	0.00452	-0.0012
	B	0.99712	0.99666	0.99512	-0.0029	0.00405	-0.0032
15	R	0.91844	0.86029	0.84005	0.00049	0.00139	-0.0035
	G	0.88380	0.79648	0.76403	0.00155	0.00457	0.00015
	B	0.92344	0.87729	0.85478	0.00168	0.00094	-0.0015
16	R	0.95736	0.94880	0.92784	-0.0023	0.00239	-0.0052
	G	0.96032	0.95168	0.93255	-0.0021	0.00231	-0.0036
	B	0.96554	0.95802	0.94071	-0.0003	0.00222	-0.0026
17	R	0.96440	0.96200	0.94288	-0.0014	-0.0009	-0.0019
	G	0.96807	0.96562	0.94843	-0.0015	-0.0013	-0.0013
	B	0.97290	0.97080	0.95600	-0.0022	-0.0013	-0.0021
18	R	0.97956	0.97970	0.96603	-0.0023	-0.0051	0.00102
	G	0.98169	0.98170	0.96941	-0.0027	-0.0055	0.00097
	B	0.98456	0.98457	0.97412	-0.0025	-0.0050	0.00121
19	R	0.96628	0.95570	0.93483	-0.0039	-0.0107	0.00153
	G	0.95646	0.94164	0.91683	0.00180	-0.0086	0.00645
	B	0.94978	0.92715	0.89866	-0.0051	-0.0056	0.00508
20	R	0.89300	0.89954	0.83252	0.00049	-0.0028	-0.0030
	G	0.88858	0.89721	0.82634	0.00068	-0.0016	-0.0035
	B	0.90833	0.91448	0.85792	-0.0017	7.04370	-0.0032
21	R	0.95985	0.96243	0.93508	-0.0033	-0.0011	0.00201
	G	0.95768	0.96053	0.93051	-0.0037	0.00090	0.00044
	B	0.95862	0.96189	0.93599	-0.0034	0.00094	0.00078
22	R	0.89740	0.90212	0.85936	-0.0016	-0.0004	-0.0007
	G	0.83980	0.84770	0.78305	-0.0020	0.00097	-0.0002
	B	0.68500	0.69975	0.59439	-0.0034	0.00171	-0.0030
23	R	0.98967	0.98860	0.98130	-0.0015	-0.0038	-0.0034
	G	0.98784	0.98653	0.97820	-0.0023	-0.0035	-0.0022
	B	0.98618	0.98487	0.97512	-0.0025	-0.0040	-0.0022
24	R	0.95659	0.95371	0.93004	-0.0026	0.00107	0.00359
	G	0.94843	0.94898	0.91253	-0.0028	0.00118	0.00359
	B	0.94769	0.95128	0.91047	-0.0023	0.00066	0.00371

The correlation analysis results presented in Table 5 and Table 6 are definitive. For all 24 test images, the correlation coefficients in the plain images are consistently high (approaching 1). After encryption with the LC Map algorithm, these correlation values drop drastically to values near zero. This demonstrates that the algorithm successfully destroys the spatial correlation, proving its high resistance to statistical analysis attacks

4. Conclusion

This research has successfully developed and validated the LC Map as a foundation for a robust and efficient digital image encryption algorithm. The comprehensive analysis has proven that the LC Map offers significant advantages over conventional single-dimensional chaotic maps. The main contributions of this research have been confirmed through a series of tests. First, the LC Map exhibits strong chaotic behavior, as evidenced by dense bifurcation diagrams, consistently positive Lyapunov Exponent values, and a 100% pass rate on all 16 NIST statistical tests under optimal parameters. Second, from a security perspective, the LC Map-based encryption algorithm demonstrates superior resistance to various types of attacks. This is evidenced by a computationally infeasible key space (7.2×10958), extreme key sensitivity (10–17), and near-ideal NPCR and UACI values. Functionally, the algorithm has been proven effective and lossless, with the decryption process perfectly restoring the original image (MSE = 0 and PSNR = ∞). These findings, combined with better computational efficiency compared to sequential combination methods, position the LC Map as a significant contribution to the field of chaos-based cryptography. Future research could focus on exploring hardware implementations of the LC Map and extending its application to other types of multimedia data.

Declarations

Author contribution. All authors contributed equally to the primary contributor to this paper. All authors read and approved the final paper.

Funding statement. None of the authors has received any funding or grants from any institution or funding body for the research.

Conflict of interest. The authors declare no conflict of interest.

Additional information. No additional information is available for this paper.

References

[1] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, “Medical Image Encryption: A Comprehensive Review,” *Computers*, vol. 12, no. 8, pp. 1–45, 2023, doi: 10.3390/computers12080160.

[2] F. Asiri *et al.*, “Enhancing medical image privacy in IoT with bit-plane level encryption using chaotic map,” *Front. Comput. Neurosci.*, vol. 19, pp. 1–15, Jun. 2025, doi: 10.3389/fncom.2025.1591972.

[3] S. Choudhary, “Analysis of Cryptography Encryption for Network Security and Image Steganography Technique,” *Int. J. Sci. Res. Eng. Manag. (IJSREM*, no. October, p. 7, 2023, doi: 10.55041/IJSREM26359.

[4] A. A. Shukur, A. A. Neamah, V. T. Pham, and G. Grassi, “A novel chaotic system with one absolute term: stability, ultimate boundedness, and image encryption,” *Heliyon*, vol. 11, no. 1, p. e37239, 2025, doi: 10.1016/j.heliyon.2024.e37239.

[5] Y. Niu, H. Zhou, and X. Zhang, “Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators,” *Sci. Rep.*, vol. 14, no. 1, pp. 1–21, 2024, doi: 10.1038/s41598-024-57756-x.

[6] D. Ravichandran, W. S. L. Jebarani, H. Mahalingam, P. V. Meikandan, P. Pravinkumar, and R. Amirtharajan, “An efficient medical data encryption scheme using selective shuffling and inter-intra pixel diffusion IoT-enabled secure E-healthcare framework,” *Sci. Rep.*, vol. 15, no. 1, pp. 1–25, 2025, doi: 10.1038/s41598-025-85539-5.

[7] K. Song, N. Imran, J. Y. Chen, and A. C. Dobbins, “A Hybrid Chaos-Based Cryptographic Framework for Post-Quantum Secure Communications,” *arXiv*, pp. 1–17, 2025, [Online]. Available at: https://arxiv.org/abs/2504.08618.

[8] A. Al-Hyari, M. Abu-Faraj, C. Obimbo, and M. Alazab, “Chaotic Hénon–Logistic Map Integration: A Powerful Approach for Safeguarding Digital Images,” *J. Cybersecurity Priv.*, vol. 5, no. 1, pp. 1–30, 2025, doi: 10.3390/jcp5010008.

[9] S. Mohi, U. 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, pp. 1–21, 2025, doi: 10.1038/s41598-025-85814-5.

[10] L. J. Ibrahim, J. B. Idoko, and A. M. Alwhelat, “Robust Chaos Image Encryption System using Modification Logistic Map, Gingerbread Man and Arnold Cat Map,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 6, pp. 1305–1316, 2024, doi: 10.14569/IJACSA.2024.01506132.

[11] X. D. Liu *et al.*, “Quantum image encryption algorithm based on four-dimensional chaos,” *Front. Phys.*, vol. 12, no. March, pp. 1–12, 2024, doi: 10.3389/fphy.2024.1230294.

[12] L. Wang, W. Song, J. Di, X. Zhang, and C. Zou, “Image Encryption Method Based on Three-Dimensional Chaotic Systems and V-Shaped Scrambling,” *Entropy*, vol. 27, no. 1, 2025, doi: 10.3390/e27010084.

[13] A. Tiwari, P. Diwan, T. D. Diwan, M. Miroslav, and S. P. Samal, “A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication,” *Sci. Rep.*, vol. 15, no. 1, pp. 1–16, 2025, doi: 10.1038/s41598-025-95995-8.

[14] S. Kanwal, S. Inam, S. Al-Otaibi, J. Akbar, N. Siddiqui, and M. Ashiq, “An efficient image encryption algorithm using 3D-cyclic chebyshev map and elliptic curve,” *Sci. Rep.*, vol. 14, no. 1, pp. 1–15, 2024, doi: 10.1038/s41598-024-77955-w.

[15] S. Zhou, Y. Wei, S. Wang, H. H. C. Iu, and Y. Zhang, “Novel chaotic image cryptosystem based on dynamic RNA and DNA computing,” *J. Appl. Phys.*, vol. 136, no. 18, 2024, doi: 10.1063/5.0235336.

[16] X. Xie *et al.*, “A CML-ECA Chaotic Image Encryption System Based on Multi-Source Perturbation Mechanism and Dynamic DNA Encoding,” *Symmetry (Basel).*, vol. 17, no. 7, pp. 1–26, 2025, doi: 10.3390/sym17071042.

[17] C. Tang, S. Wang, Y. Shu, and F. Ren, “Encryption algorithm based on improved four-dimensional chaotic system and dynamic DNA encoding,” *AIP Adv.*, vol. 14, no. 9, pp. 1–16, Sep. 2024, doi: 10.1063/5.0207225.

[18] A. Shafique *et al.*, “A hybrid encryption framework leveraging quantum and classical cryptography for secure transmission of medical images in IoT-based telemedicine networks,” *Sci. Rep.*, vol. 14, no. 1, pp. 1–24, 2024, doi: 10.1038/s41598-024-82256-3.

[19] U. Shahid, S. Kanwal, M. Bano, S. Inam, M. E. M. Abdalla, and Z. A. Shaikh, “Blockchain driven medical image encryption employing chaotic tent map in cloud computing,” *Sci. Rep.*, vol. 15, no. 1, p. 6236, Feb. 2025, doi: 10.1038/s41598-025-90502-5.

[20] S. Inam, S. Kanwal, R. Firdous, and F. Hajjej, “Blockchain based medical image encryption using Arnold’s cat map in a cloud environment,” *Sci. Rep.*, vol. 14, no. 1, pp. 1–22, 2024, doi: 10.1038/s41598-024-56364-z.

[21] S. A. Jabber, A. Al-Adhami, R. K. Hasoun, R. S. Ali, and S. H. Hashem, “Proposal to strength image encryption using blockchain and hybrid chaotic-DNA techniques,” *Egypt. Informatics J.*, vol. 32, no. August, p. 100765, 2025, doi: 10.1016/j.eij.2025.100765.

[22] S. Huang, G. Deng, L. Liu, and X. Li, “Technique for Enhancing the Chaotic Characteristics of Chaotic Maps Using Delayed Coupling and Its Application in Image Encryption,” *Mathematics*, vol. 11, no. 15, p. 3295, Jul. 2023, doi: 10.3390/math11153295.

[23] E. Güvenoğlu, “An image encryption algorithm based on multi-layered chaotic maps and its security analysis,” *Conn. Sci.*, vol. 36, no. 1, pp. 1–31, Dec. 2024, doi: 10.1080/09540091.2024.2312108.

[24] A. Abba, J. Sen Teh, and M. Alawida, “Towards accurate keyspace analysis of chaos-based image ciphers,” *Multimed. Tools Appl.*, vol. 83, no. 33, pp. 79047–79066, 2024, doi: 10.1007/s11042-024-18628-8.

[25] I. Mursidah, S. Mt, and S. Madenda, “A new chaos function development through the combination of Circle map and MS map,” *ITM Web Conf.*, vol. 61, p. 01005, 2024, doi: 10.1051/itmconf/20246101005.

[26] H. Zhang, W. Sun, and L. Lu, “Chaotic encryption algorithm with scrambling diffusion based on the Josephus cycle,” *Front. Phys.*, vol. 11, no. May, pp. 1–16, 2023, doi: 10.3389/fphy.2023.1191793.

[27] M. Riaz *et al.*, “Secure and Fast Image Encryption Algorithm Based on Modified Logistic Map,” *Inf.*, vol. 15, no. 3, pp. 1–20, 2024, doi: 10.3390/info15030172.

[28] H. A. Hosham and T. N. Alharthi, “Bifurcation and chaos in simple discontinuous systems separated by a hypersurface,” *AIMS Math.*, vol. 9, no. 7, pp. 17025–17038, 2024, doi: 10.3934/math.2024826.

[29] N. Kumar and S. Saini, "Intelligent Systems And Applications In Engineering Image Encryption Model based on Chaotic Henon Map and Termite Alate Optimization Algorithm," vol. 12, pp. 428–436, 2024, doi: 10.1080/03772063.2024.2390667.

[30] M. A. Alkhonaini, E. Gemeay, F. M. Zeki Mahmood, M. Ayari, F. A. Alenizi, and S. Lee, "A new encryption algorithm for image data based on two-way chaotic maps and iterative cellular automata," *Sci. Rep.*, vol. 14, no. 1, pp. 1–15, 2024, doi: 10.1038/s41598-024-64741-x.

[31] N. El Ghouate *et al.*, "A high-entropy image encryption scheme using optimized chaotic maps with Josephus permutation strategy," *Sci. Rep.*, vol. 15, no. 1, pp. 1–26, 2025, doi: 10.1038/s41598-025-14784-5.

[32] K. M. Hosny, Y. M. Elnabawy, R. A. Salama, and A. M. Elshewey, "Multiple image encryption algorithm using channel randomization and multiple chaotic maps," *Sci. Rep.*, vol. 14, no. 1, pp. 1–18, 2024, doi: 10.1038/s41598-024-79282-6.

[33] S. M. Mohamed, W. S. Sayed, A. H. Madian, A. G. Radwan, and L. A. Said, "An Encryption Application and FPGA Realization of a Fractional Memristive Chaotic System," *Electronics*, vol. 12, no. 5, p. 1219, Mar. 2023, doi: 10.3390/electronics12051219.

[34] A. Daoui, M. Yamni, S. A. Chelloug, M. A. Wani, and A. A. A. El-Latif, "Efficient Image Encryption Scheme Using Novel 1D Multiparametric Dynamical Tent Map and Parallel Computing," *Mathematics*, vol. 11, no. 7, p. 1589, Mar. 2023, doi: 10.3390/math11071589.

[35] W. Alexan *et al.*, "A new multiple image encryption algorithm using hyperchaotic systems, SVD, and modified RC5," *Sci. Rep.*, vol. 15, no. 1, pp. 1–33, 2025, doi: 10.1038/s41598-025-92065-x.

[36] S. Kumar and D. Sharma, "A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm," *Artif. Intell. Rev.*, vol. 57, no. 4, p. 87, Mar. 2024, doi: 10.1007/s10462-024-10719-0.

[37] Magfirawaty Magfirawaty, Ariska Allamanda, Malika Ayunasari, and Muhammad Nadhif Zulfikar, "Confusion and Diffusion Techniques for Image Encryption Process Based on Chaos System," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 13, no. 2, pp. 93–100, 2024, doi: 10.22146/jnteti.v13i2.9623.

[38] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "Image Encryption Scheme Based on Newly Designed Chaotic Map and Parallel DNA Coding," *Mathematics*, vol. 11, no. 1, p. 231, Jan. 2023, doi: 10.3390/math11010231.

[39] S. Kumari, M. Dua, S. Dua, and D. Dhingra, "A novel Cosine-Cosine chaotic map-based video encryption scheme," *J. Eng. Appl. Sci.*, vol. 71, no. 1, pp. 1–17, 2024, doi: 10.1186/s44147-024-00376-z.

[40] M. Turan, E. Gökçay, and H. Tora, "An unrestricted Arnold's cat map transformation," *Multimed. Tools Appl.*, vol. 83, no. 28, pp. 70921–70935, 2024, doi: 10.1007/s11042-024-18411-9.

[41] J. Tang, F. Zhang, and H. Ni, "A novel fast image encryption scheme based on a new one-dimensional compound sine chaotic system," *Vis. Comput.*, vol. 39, no. 10, pp. 4955–4983, 2023, doi: 10.1007/s00371-022-02640-w.

[42] S. Sun, W. Yang, Y. Yin, X. Tian, G. Li, and X. Deng, "A color image encryption scheme utilizing a logistic-sine chaotic map and cellular automata," *Sci. Rep.*, vol. 15, no. 1, pp. 1–21, 2025, doi: 10.1038/s41598-025-04968-4.