

Article

# An enhanced Lorenz-based chaos cryptographic scheme with modular arithmetic and prime masking

Umar Muhammad Dauda<sup>1,\*</sup>, Auwal Lawan<sup>2</sup>, Isah Ali Ibrahim<sup>1</sup>, Ibrahim Dauda Abdullahi<sup>1</sup>, and Yusuf Haruna<sup>3</sup>

<sup>1</sup> Department of Mathematics, Aliko Dangote University of Science and Technology, Wudil, Nigeria

<sup>2</sup> Dipartimento di Informatica, University of Verona, Italy

<sup>3</sup> Department of Computer Science, Aliko Dangote University of Science and Technology, Wudil, Nigeria

\* Correspondence: [umarmd2021@gmail.com](mailto:umarmd2021@gmail.com); <https://orcid.org/0000-0003-4302-2202>

**Abstract:** Chaos theory nowadays plays as a strong and useful tool in the current digital world. It provides a somewhat reliable way of securing data in digital form, such as image data, through unpredictable deterministic systems. In this study, we introduce a new encryption method that combines the chaotic Lorenz system with modular arithmetic and prime masking for image data encryption. The chaotic nature of the Lorenz system's outputs is known to be highly sensitive to initial conditions, and therefore forms the foundation of our key stream for the encryption. Then the modular arithmetic in a finite field  $\mathbb{Z}_{251}$  is used to increase robustness of the encryption; moreover, followed by prime-masking, thereby adding a nonlinear security layer of confusion as appropriate. This triple-layered encryption approach strengthens resistance to the current prevalence of statistical attacks. Our implementation and experiments on coloured images demonstrate, significantly, strong randomness, high entropy, and negligible pixel correlation in the encrypted result, while maintaining efficient decryption. Upon comparisons with traditional methods, such as Advanced Encryption Standard (AES), reveal that the proposed scheme offers unique strengths in lightweight and dynamic encryption. This approach is especially suitable for constrained applications such as IoT environments. The new hybridization combines chaos theory with algebraic masking to achieve both simplicity and strong security.

**Keywords:** Chaos-based encryption; Lorenz-system; modular-arithmetic; prime-mask; image encryption; lightweight cryptography; entropy analysis.

Received: 8 October 2025; Revised: 20 November 2025; Accepted: 8 December 2025; Published: 26 January 2025



Copyright: ©2026 the Author(s). Published by JSSCI. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0).

Journal Abbreviation: J. Stat. Sci. Comput. Intell.

## 1. Introduction

It is apparent that the contemporary digital world encounters, unavoidably, security challenges at virtually

every fraction of a second when data is transmitted. This poses a significant threat and raises concern for the need for highly sensitive data secure systems that are difficult to break such as chaos-based algorithms. Chaos-based cryptography utilizes the sensitive and unpredictable nature of chaotic systems such as the Lorenz system for secure data encryption. In this article, we hybridize the Lorenz system with number-theoretic methods, in particular, the so-called modular arithmetic and prime masking. All it is meant to enhance the security, randomness, and unpredictability of the encryption. Chaos theory, firstly identified in the last 6 decades around the 1960s, has evolved remarkably over time, influencing a wide range of fields that include, not limited to, physics, engineering, computer science, economics, and biology due to its extensive interdisciplinary applications.

As digital images rapidly appear constantly in our everyday communication, through smartphones, social media, and remote sensing, their security under transmission grows ever more critical, just like other forms of digital data. The famous traditional encryption standards like AES ensure robust protection, however, often require substantial computational resources and rigid key structures. On the other hand, chaos-based cryptography, inspired by nonlinear dynamics, offers lightweight, highly sensitive alternatives due to two important and fundamental properties, the sensitivity to initial conditions and pseudo-randomness. The Lorenz system, a continuous-time chaotic system described by three ordinary differential equations, is a classic example. Small changes in its initial values lead to entirely different trajectories. This unpredictability makes it ideal as a key-stream generator. Yet, many chaos-based approaches rely solely on XOR operations, which can be vulnerable to cryptanalytic attacks lacking deeper algebraic structure.

To fill this gap, we propose a hybrid encryption scheme: chaotic key-stream generation via the Lorenz system, strengthened by finite-field modular arithmetic in  $\mathbb{Z}_{251}$ , and an additional prime mask that injects nonlinearity based on prime indices. This composite mechanism promises both cryptographic diversity and mathematical rigor, while remaining computationally tractable. Like the AES, the chaos-based encryption gives secure protection by scrambling the data to make it unreadable to external sources that have the tendency to read data with no specific key requirement.

### 1.1. Related Studies

The chaos-based encryption algorithm arises as a result of the need to strengthen the security of digital data. Recent studies in chaos-based image encryption highlight the rapid evolution of the field. One of the motivating algorithms that utilizes the chaotic behaviour for encryption is the work of J. Fridrich (1998), [11]. It was based on two dimensional chaotic map for data encryption. From then, more research exploiting the chaotic properties follows. Obaida et. al. (2017), introduced a novel image encryption strategy grounded in the Lorenz chaotic system, emphasizing its randomness, confusion-diffusion dynamics, and high sensitivity to initial conditions [2]. The encryption process unfolds in two stages: first, secret keys are derived from the plain image's 256-bit hash and a logistic map; second, the image is encrypted using sequences from the Lorenz system coupled with the generated keys.

Al-Maadeed et al. (2021) presented a Lorenz-based method that incorporates primitive polynomial S-boxes, boosting confusion through algebraic substitution layers [7]. Zhang et. al. (2022), established a comprehensive review to reflect the broader landscape, detailing challenges and applications in chaos-based image encryption across symmetric, transform-domain, and hybrid systems [8]. An additional work in the same being is that of Daniah Abul Qahar Shakir (2022), and collaborators proposed in [3] a Lorenz-based encryption/decryption method for digital images, leveraging the system's three differential equations to construct a secure and efficient algorithm.

Shakir et al (2022), [5], develop an electronic encryption and decryption method for 3D images using the

3-dimensional Lorentz dynamical system equation. Previous to this, the method was able to destroy pixel of image through a process of reversible translation and rotation to increase the difficulty of cracking the password.

Bahaa and Ekhlas (2024), developed an innovative encryption mechanism utilizing confusion and diffusion techniques within the spectral domain, particularly on the Discrete Cosine Transform (DCT) coefficients [6]. Their method supports rapid encryption, bypassing the traditionally high number of confusion-diffusion iterations required in spatial domain approaches. A four-dimensional chaotic system with evolutionary operators such as crossover and mutation was introduced by Niu et. al (2024). The approach achieves near-perfect plaintext sensitivity and strong resistance against differential attacks [9]. Ali and Mohammad (2024), [1], presented a lightweight chaotic encryption model with fuzzy access control tailored for Internet of Things (IoT) imagery, ensuring high image fidelity. Utilizing multiplexer structures and shift registers, their design blends random and chaotic mapping derived from a password key and applies fuzzy logic transformations to pixel values.

Yexia and colleagues (2025) enhanced a chaotic system by integrating the memristor model, resulting in a two-dimensional (2D) hyperchaotic framework [4]. The chaotic characteristics of the system were validated through analytical tools like phase portraits, bifurcation analysis, and the Lyapunov exponent spectrum. Their work also proposed a comprehensive structure compatible with the developed chaotic model. Tiwari et. al. (2025), published in Scientific Reports, proposed the "OptiSecure-3D" approach, leveraging parameter-optimized 3D chaotic maps and auto-encoders to yield high entropy and low pixel adjacency correlation [10].

These recent models enhance encryption security through higher-dimensional chaos, dynamic key structures, and integration with learning or evolutionary frameworks. Our work contributes a new direction by fusing chaotic key-streams with classical number-theoretic operations for efficiency and mathematical security.

All these methods and techniques have the same meaning, which is encryption, they all provide a systematic way of encrypting images using the famous dynamical non-linear differential equation (Lorentz System), all due to its sensitivity to initial conditions, resulting in it been named as a chaos system. Using the prime masking method, we encrypted a 3D image with the Lorentz chaotic system.

## 2. Basic Definitions

### 2.1. Stability & Lyapunov function

**Definition.** *Lyapunov Function:* A continuously differentiable scalar function  $V: \mathbb{R}^n \rightarrow \mathbb{R}$  is called a Lyapunov function for an equilibrium point  $x^*$  of a dynamical system if:

- I.  $V(x^*) = 0, V(x) > 0$  for  $x \neq x^*$ ,
- II.  $\dot{V}(x) \leq 0$  along system trajectories.

**Definition.** *Stability:* An equilibrium  $x^*$  of  $\dot{x} = f(x)$  is *stable in the sense of Lyapunov* if, for every  $\varepsilon > 0$ , there exists  $\delta > 0$  such that

$$|x(0) - x^*| < \delta \quad \Rightarrow \quad |x(t) - x^*| < \varepsilon, \quad \forall t \geq 0.$$

**Definition.** *Asymptotic Stability:* If, in addition,  $\lim_{t \rightarrow \infty} x(t) = x^*$ , then the equilibrium is asymptotically stable.

**Definition.** *The Lorenz system* is defined as: for real number  $t$  and variables  $x = x(t), y = y(t), z = z(t)$

$$\begin{cases} x' = (y - x)\sigma, \\ y' = x(\rho - z) - y, \\ z' = xy - \beta z, \end{cases} \quad (1)$$

$\sigma, \rho, \text{ and } \beta$  are positive constants representing, respectively, the Prandtl number, Rayleigh number, and a geometric factor. With parameters  $\sigma = 10$ ,  $\rho = 28$ , and  $\beta = 8/3$ . The system is numerically solved using initial conditions  $(x_0, y_0, z_0)$  and the output  $x(t)$  is normalized and discretized to create a key stream.

**Definition.** *Chaotic Key Stream:* A sequence generated by nonlinear dynamics (here, the Lorenz system) that exhibits sensitivity to initial conditions and bounded randomness suitable for encryption.

### 3. Methodology

The Lorenz system (1) is solved numerically with secret initial conditions  $(x_0, y_0, z_0)$ . The generated trajectories provide a pseudo-random sequence that is highly sensitive to initial conditions. We further carry out the modular arithmetic and prime masking for optimal encryption. These are described as follows.

The chaotic trajectory is converted into a key stream by applying scaling, modular arithmetic, and mapping into a bounded range: for some integer  $m \in \mathbb{N}$

$$K = \{k_i = (\lfloor x_i \cdot 10^m \rfloor \bmod 251) : i = 1, \dots, M \times N \times 3\}$$

**Prime Masking:** A global prime set

$$\mathcal{P} = 2, 3, 5, \dots, p_{\max}, \quad p_{\max} \leq 65521$$

is used. The key sequence selects primes, which are then partitioned across red, green, and blue channels to form the masks  $(P_R, P_G, P_B)$ .

**Encryption:** For pixel  $(i, j)$  the cipher components are computed as:

$$R'_{ij} = [R_{ij} + P_R(k)] \bmod 256,$$

$$G'_{ij} = [G_{ij} + P_G(k)] \bmod 256,$$

$$B'_{ij} = [B_{ij} + P_B(k)] \bmod 256.$$

**Decryption:** Since modular addition is invertible, the original pixel values are recovered as:

$$R_{ij} = [R'_{ij} - P_R(k) + 256] \bmod 256$$

similarly for G and B.

Security Analysis is carried-out via Histogram analysis to ensure pixel distribution uniformity, entropy computation to evaluate information content, and correlation analysis to check independence among adjacent pixels. We, furthermore, use Lyapunov exponent analysis to assess the unpredictability of Lorenz system dynamics.

## 4. Theoretical Results

### 4.1. Modular Arithmetic Encryption

Let  $I$  be the original image matrix of size  $M \times N$ . The chaotic key stream is reshaped into a matrix  $K$  of the same size. We define the modular encrypted image  $C$  as:

$$C(i, j) = [I(i, j) + K(i, j)] \bmod 251 \quad (2)$$

This arithmetic is done over the finite field  $Z_{251}$ , chosen for being prime, which ensures invertibility and uniform distribution.

### 4.2. Prime Masking for Additional Confusion

Each element of the key stream is used as an index to select a prime number from a list of primes  $\leq 65521$ .

This generates a prime mask matrix  $P$ , which introduces additional nonlinearity. The final encrypted image is computed as:

$$C'(i, j) = [C(i, j) + P(i, j)] \bmod 256 \quad (3)$$

### 4.3. Decryption Algorithm

To recover the original data image:

- I. Subtract the prime mask:

$$C(i, j) = [C'(i, j) - P(i, j) + 256] \bmod 256$$

- II. Subtract the key stream:

$$I(i, j) \leftarrow [C(i, j) - K(i, j) + 256] \bmod 256$$

This hybridization technique is meant to improve resistance to decryption in different ways. It improves the resistance to brute-force and statistical attack, add field algebra properties beneficial in cryptanalysis resistance by modular analysis and additional confusion nonlinearity via prime-based approach.

Images often use 16-bit unsigned integers or 8-bit per channel (0–255). As 65521 is the largest prime less than or equal to  $2^{16}$ , moreover, chosen to maximize keyspace while still fitting into common computer word sizes. It is noteworthy knowing that 251 is the immediate prime number < 256, making it suitable for modular operations within the 8-bit range. Moreover, to avoids overflow when applying modular arithmetic and at the same time to maintain uniform distribution of encrypted pixels, and consequently improves entropy.

### 4.4. Numerical Example

Here we give an example to demonstrate the implementation of the algorithm.

- I. *Decompose the given image:* Suppose we are given an image decomposed into three main colour pixels, RGB (in  $\mathbb{Z}_{256}$ ). An example we consider here is an image as RGB matrices:

$$R = \begin{bmatrix} 120 & 45 \\ 200 & 5 \end{bmatrix}, \quad G = \begin{bmatrix} 34 & 220 \\ 17 & 99 \end{bmatrix}, \quad B = \begin{bmatrix} 255 & 0 \\ 60 & 180 \end{bmatrix}.$$

Therefore, the colour image tensor is  $I \in \mathbb{Z}_{256}^{2 \times 2 \times 3}$  with planes  $R, G, B$ .

- II. *Channel specific modular Keys.* Given the numerical solution of the Lorenz-system  $X_i(t), i = 1..3,$ , the three continuous chaotic sequence, we generate a chaotic sequence long enough (at least  $M \times N$ ), then we normalize the Lorenz values into  $\{0, 255\} \in \mathbb{Z}_{256}$ , an 8-bit integer. The Modular keys comes by mapping into the modular group  $\mathbb{Z}_{251}$ . That is, via

$$K_i = \text{mod}(|X_i| \times 10^5, 251),$$

as can be implemented in MATLAB and these  $K_i$  are the chaotic key stream. The factor  $10^5$  is incorporated to capture more integers as decimal values are expected. This reshape the chaotic sequence into an  $M \times N \rightarrow K_R, K_G, K_B$ , for the three basic colours red, blue and green. Thus, the output should be a 3d matrix of size  $M \times N \times 3$ , with three colour channels RGB, with each channel e.g. red having  $M \times N \times 1$  representing the matrix intensities from 0 to 255, likewise for blue and green colours.

For explicit demonstration, we pick matrices of the respective colours as

$$K_R = \begin{bmatrix} 37 & 250 \\ 0 & 125 \end{bmatrix}, \quad K_G = \begin{bmatrix} 10 & 3 \\ 250 & 47 \end{bmatrix}, \quad K_B = \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix},$$

obtained by mapping the respective chaotic sequences  $X_i, Y_i, Z_i$ :

$$X_R = \begin{pmatrix} 0.00037 & 0.002503 \\ 0.00000 & 0.0012451 \end{pmatrix}, \quad Y_G = \begin{pmatrix} 0.00001 & 0.000032 \\ 0.00250 & 0.000471 \end{pmatrix}, \quad Z_B = \begin{pmatrix} 0.00000 & 0.000021 \\ 0.00002 & 0.000033 \end{pmatrix},$$

- III. *Prime Masking per channel.* For a list of primes

$$\mathcal{P} = \{2, 3, 5, 7, \dots, 65521\}$$

from the Lorenz chaotic sequence, we map values to **indices** inside the prime list via one-based indexing into the prime list  $\text{PrimeIdx} = K_i + 1$ . So the prime mask indexing  $P = P_{\text{PrimeIdx}(i,j)}$  for a prime index  $p_k$  as the k-

th prime are:

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \quad p_{11} = 31, \\ p_{38} = 163, \quad p_{48} = 223, \quad p_{126} = 701, \quad p_{251} = 1597.$$

These are generated in the sense that if a chaotic number gives index 4, then we take  $p_4 = 7$ , with index 38, then we have  $p_{38} = 163$  and so on. Thus, the assignments as determined by the chaotic sequence are

$$P_R = \{p_1, p_4, p_{38}, \dots\}, \quad P_G = \{p_2, p_{11}, p_{48}, \dots\}, \quad P_B = \{p_{126}, p_{251}, p_3, \dots\}; \\ P_R = \begin{bmatrix} p_{28} & p_{251} \\ p_1 & p_{126} \end{bmatrix} = \begin{bmatrix} 163 & 1597 \\ 2 & 701 \end{bmatrix}, \quad P_G = \begin{bmatrix} p_{11} & p_4 \\ p_{251} & p_{48} \end{bmatrix} = \begin{bmatrix} 31 & 7 \\ 1597 & 223 \end{bmatrix}, \quad P_B = \begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}$$

Equivalently, we reduce the prime mod 256 to:

$$P_R \text{ mod } 256 = \begin{bmatrix} 163 & 61 \\ 2 & 189 \end{bmatrix}, \quad P_G \text{ mod } 256 = \begin{bmatrix} 31 & 7 \\ 61 & 223 \end{bmatrix}, \quad P_B \text{ mod } 256 = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}.$$

IV. *Encryption and Decryption.* The Encryption per channel reads

$$C = I + K + P \pmod{256}.$$

For each of these colour channels, we have for red, green and blues respectively

$$C_R \equiv \left( \begin{bmatrix} 120 & 45 \\ 200 & 5 \end{bmatrix} + \begin{bmatrix} 37 & 250 \\ 0 & 125 \end{bmatrix} + \begin{bmatrix} 163 & 1597 \\ 2 & 701 \end{bmatrix} \right) \pmod{256} = \begin{bmatrix} 64 & 100 \\ 202 & 63 \end{bmatrix}, \\ C_G \equiv \left( \begin{bmatrix} 34 & 220 \\ 17 & 99 \end{bmatrix} + \begin{bmatrix} 10 & 3 \\ 250 & 47 \end{bmatrix} + \begin{bmatrix} 31 & 7 \\ 1597 & 223 \end{bmatrix} \right) \pmod{256} = \begin{bmatrix} 75 & 230 \\ 72 & 113 \end{bmatrix}, \\ C_B \equiv \left( \begin{bmatrix} 255 & 0 \\ 60 & 180 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} + \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix} \right) \pmod{256} = \begin{bmatrix} 1 & 4 \\ 67 & 190 \end{bmatrix}.$$

So, the cipher image is  $C = \{C_R, C_G, C_B\}$ .

For decryption, we have, for each channel

$$I = C - K - P \pmod{256}.$$

We verify this for one channel, red:

$$I_R \pmod{256} = \left( \begin{bmatrix} 64 & 100 \\ 202 & 63 \end{bmatrix} - \begin{bmatrix} 37 & 250 \\ 0 & 125 \end{bmatrix} - \begin{bmatrix} 163 & 1597 \\ 2 & 701 \end{bmatrix} \right) \pmod{256} = \begin{bmatrix} -136 & -1747 \\ 200 & -763 \end{bmatrix} \pmod{256} \\ \equiv \begin{bmatrix} 120 & 45 \\ 200 & 5 \end{bmatrix}.$$

This is, likewise, checked and recovered for green and blue colours. After the application of the same arithmetic for green and blue, the three encrypted planes are concatenated to form the colour cipertext image. Thus, in a compact tensor form, for each channel, we have

$$\mathbb{Z}_{256}^{M \times N} \ni I(:, :, c) = \{c, K(:, :, c), P(:, :, c)\},$$

where  $c \in \{R, G, B\}$ ,  $K(:, :, c) \in \{0, \dots, 250\}^{M \times N}$ , and  $P(:, :, c) = (P_{K(:, :, c)+1})$ . Thus, an encrypted image has

$$C(:, :, c) = I(:, :, c) + K(:, :, c) + P(:, :, c) \pmod{256}$$

and the decrypted image has

$$I(:, :, c) = C(:, :, c) - K(:, :, c) - P(:, :, c) \pmod{256}.$$

**Theorem 1.** (Lyapunov Stability Theorem).

Let  $x^*$  be an equilibrium of  $\dot{x} = f(x)$ . Suppose there exists a continuously differentiable function  $V(x)$  such that:

$$V(x^*) = 0, \quad V(x) > 0 \text{ for } x \neq x^*,$$

$$\dot{V}(x) \leq 0 \text{ for all } x \text{ in a neighbourhood of } x^*.$$

Then,  $x^*$  is stable. If  $\dot{V}(x) < 0$  for  $x \neq x^*$ , then  $x^*$  is asymptotically stable.

Here, we propose a stability result for our Lorenz-Based Cryptography:

**Theorem 2.** (Chaotic Security Stability): Let  $K = \{k_i\}$  be the chaotic key stream generated from the Lorenz

dynamics. Suppose the following hold:

The maximal Lyapunov exponent  $\lambda_{\max} > 0$ , ensuring sensitivity and unpredictability.

The mapping  $k_i \mapsto p_{\{l_i\}}$  (prime mask selection) is injective and bounded by modulus ( $m = 251$ ).

The pixel transformation function

$$\Phi(x) = (x + k_i + p_{l_i}) \bmod 256$$

is bijective.

Then, the encryption scheme is stable against brute-force and statistical attacks in the sense that small variations in keys (initial conditions) yield exponentially diverging outputs (due to Lorenz sensitivity), while ensuring perfect reversibility through modular arithmetic.

**Remark 1.1.**

The use of Lyapunov exponents formalizes the unpredictability measure in chaos-based cryptography.

The proposed theorem bridges dynamical stability with cryptographic security stability, which is a novel contribution.

**Remark 1.2.**

Saturation & finite resolution. Exponential growth is limited by the finite range and quantization: once differences become larger than the dynamic range, they saturate. Still, a positive LLE ensures that quantized outputs become uncorrelated quickly.

Choice of scaling  $s$  and moduli  $m_1, m_2$ . Scaling should be large enough so that small continuous differences produce integer index differences after a short time. The  $m_1$  (e.g., 251) should be large enough to avoid trivial collisions but small enough to be computationally practical.

Injectivity of  $\Pi$ . In practice, perfect injectivity is hard to guarantee on the entire image-length space, but with a large prime table and chaotic spread (uniform-like distribution), collisions become very unlikely; you can also combine prime values with channel- or pixel-dependent offsets to reduce collisions.

**Proof of Theorem 2.** (Sketch)

We first establish the exponential divergence from  $LLE > 0$ . By the definition of the largest Lyapunov exponent, for sufficiently small initial perturbation  $\delta$ , there exists a constant  $C_0$  and a time window where the base trajectories satisfy

$$|x(t, X_0) - x(t, \tilde{X}_0)| \approx C_0 e^{\lambda_{\max} t} \delta.$$

This holds at least for long but finite times until saturation (because the attractor is bounded). This is the standard consequence of a positive LLE.

The map  $\mathcal{M}$  includes scaling and flooring such as

$$\kappa = \lfloor s \cdot x(t) \rfloor \bmod m_1.$$

As the trajectories differ exponentially, after some fixed time  $t^*$  the scaled difference  $s|x - \tilde{x}|$  exceeds 1 in many components, causing the integer outputs  $\kappa$  to differ on those components. Thus, the discrete key streams differ in an increasing number of positions as time  $t$  grows.

Next, verify that the injective prime mapping preserves differences. If  $\Pi$  maps distinct index sequences to distinct prime masks (injectivity on the reachable set), then differing indices imply differing prime masks on the same positions. (In practice  $\Pi$  constructed as  $p_{\kappa+1}$  is injective as long as the range of indices used is within the prime table and collisions are avoided; using a sufficiently large prime table and chaotic spread makes collisions unlikely.)

Then, the ciphertext difference follows. Since encryption is elementwise modular addition with the combined key+mask, a difference in the mask/key at a pixel produces a different ciphertext at that pixel. So, the number of differing pixel values grows similarly with the number of differing key positions.

Hence, small initial perturbations produce exponentially growing differences in the keystream and

therefore in the ciphertext; the scheme is highly key-sensitive.

#### 4.5. Lyapunov Exponent

In an attempt to study the convergence of the trajectories, we use the Lyapunov exponent function

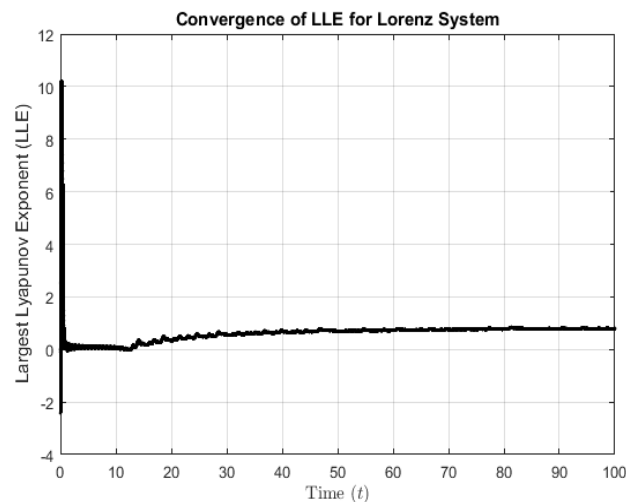
$$\lambda_i = \lim_{t \rightarrow \infty} \frac{1}{t} \ln \frac{|\delta X_i(t)|}{|\delta X_i(0)|}, \quad i \in \mathbb{N},$$

to quantify how fast these trajectories converge or diverge in the dynamical setting of our Lorenz system, where  $\delta X_i(t)$  represents the small perturbation between any two arbitrary nearby trajectories of the dynamical system (Lorenz) in the  $i$ th direction at a time  $t$  and  $|\delta X_i(t)|$  is the magnitude of the distance between the two trajectories. For the 3d Lorenz system there are only three exponents

$$\lambda_1 > 0, \quad \lambda_2 \approx 0, \quad \lambda_3 < 0.$$

The Largest Lyapunov exponent (LLE)  $\lambda_1$  indicates strong chaotic behaviour where rapid divergence of the keystream is obtained. Therefore, positivity of LLE implies exponential divergence, thereby guaranteeing unpredictability, which is an excellent quality for cryptographic key generation. The typical value for the Lorenz system is  $\lambda_1 \approx 0.9056$  for  $\sigma = 1, \rho = 28$  and  $\beta = 8/3$ . The case  $\lambda_2 = 0$  signifies the neutral direction along the Lorenz attractor, and it is hard to decide whether the Lyapunov exponent diverges or converges.

The lowest Lyapunov exponent (LLE3)  $\lambda_3 < 0$  measures how fast the trajectories spiral into the Lorenz attractor manifold. In essence, it tells the rate of convergence of the Lorenz trajectories in the contracting direction of the Lorenz attractor. Its large negative value ensures boundedness (energy dissipation or loss). The system is bound to remain stable despite the possible chaotic stretching. As a result, this ensures the chaotic keys generated do not diverge to infinity, which is very important for repeatable and secure encryption.



**Figure 1.** Convergence of the lowest Lyapunov exponent for the Lorenz system.

The plot of the LLE shown in Figure 1 shows the average running average of  $\lambda_1(t)$ . We observe early oscillations and later gradual stabilization and, eventually, an asymptotic convergence near the true exponent  $\sim 0.9$ . This confirms the ergodicity and long-term stability of the chaotic behaviour of the Lorenz system. This is essential for generating reproducible, yet unpredictable, key sequences.

#### 4.6. Stability of the Lorenz System

The Lorenz system is a set of three nonlinear differential equations originally developed to model atmospheric convection. It is the set of equations given in equation (1).

The system exhibits chaotic behaviour for certain parameter values, but also possesses equilibrium points that may be stable under other conditions. We apply Lyapunov's direct method to study the stability of these equilibria. Setting the right-hand sides of (4) to zero, we find the equilibrium points:

$$\mathbf{E}_0 = (\mathbf{0}, \mathbf{0}, \mathbf{0}), \mathbf{E}_{\pm} = (\pm\sqrt{\beta(\rho - 1)}, \pm\sqrt{\beta(\rho - 1)}, \rho - 1), \quad \rho > 1. \quad (4)$$

We analyse the stability of  $\mathbf{E}_0$  using a Lyapunov function. Consider the candidate Lyapunov function:

$$V(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \frac{1}{2}\mathbf{x}^2 + \frac{1}{2}\mathbf{y}^2 + \frac{1}{2}(\mathbf{z} - \rho)^2 \quad (5)$$

This function is positive definite and radially unbounded with respect to the equilibrium at  $(\mathbf{0}, \mathbf{0}, \rho)$ . However, to analyse stability at the origin  $\mathbf{E}_0 = (\mathbf{0}, \mathbf{0}, \mathbf{0})$ , we slightly modify it as:

$$V(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \frac{1}{2}\mathbf{x}^2 + \frac{1}{2}\mathbf{y}^2 + \frac{1}{2}\mathbf{z}^2 \quad (6)$$

Then, the time derivative  $V'$  along trajectories of the system is:

$$\begin{aligned} V' &= \mathbf{x}\mathbf{x}' + \mathbf{y}\mathbf{y}' + \mathbf{z}\mathbf{z}' = \mathbf{x}[\sigma(\mathbf{y} - \mathbf{x})] + \mathbf{y}[\mathbf{x}(\rho - \mathbf{z}) - \mathbf{y}] + \mathbf{z}[\mathbf{x}\mathbf{y} - \beta\mathbf{z}] \\ &= \sigma\mathbf{x}\mathbf{y} - \sigma\mathbf{x}^2 + \mathbf{x}\mathbf{y}(\rho - \mathbf{z}) - \mathbf{y}^2 + \mathbf{x}\mathbf{y}\mathbf{z} - \beta\mathbf{z}^2 = -\sigma\mathbf{x}^2 - \mathbf{y}^2 - \beta\mathbf{z}^2 + \mathbf{x}\mathbf{y}(\sigma + \rho - \mathbf{z} + \mathbf{z}) \\ &= -\sigma\mathbf{x}^2 - \mathbf{y}^2 - \beta\mathbf{z}^2 + \mathbf{x}\mathbf{y}(\sigma + \rho). \end{aligned}$$

We now analyse the sign of  $V'$ :

Let us complete the square or estimate upper bounds using inequalities. Applying the inequality

$$ab \leq \frac{a^2}{2\varepsilon} + \frac{\varepsilon b^2}{2}$$

to the cross term  $\mathbf{x}\mathbf{y}(\sigma + \rho)$ :

$$\mathbf{x}\mathbf{y}(\sigma + \rho) \leq \frac{(\sigma + \rho)^2}{2\varepsilon}\mathbf{x}^2 + \frac{\varepsilon}{2}\mathbf{y}^2.$$

Choose  $\varepsilon$  small enough so that the total coefficient of  $\mathbf{x}^2$  and  $\mathbf{y}^2$  remains negative. For instance, if

$$\frac{(\sigma + \rho)^2}{2\varepsilon} < \sigma \quad \text{and} \quad \frac{\varepsilon}{2} < 1,$$

then  $V' < \mathbf{0}$  for all  $(\mathbf{x}, \mathbf{y}, \mathbf{z}) = (\mathbf{0}, \mathbf{0}, \mathbf{0})$ , implying that the origin is locally asymptotically stable.

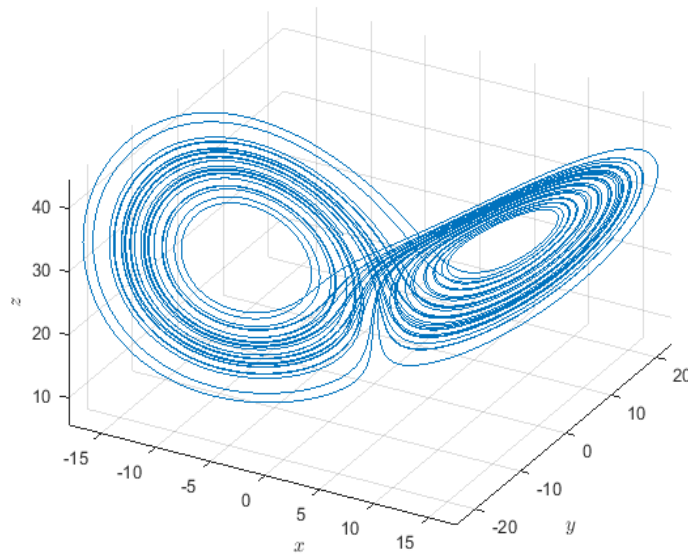
The above analysis shows that under certain conditions on  $\sigma, \rho$ , and  $\beta$ , particularly with small enough coupling terms, the origin is locally asymptotically stable. However, this result does not imply global stability due to the nonlinearities and known chaotic behaviour of the Lorenz system for large  $\rho$ .

Using Lyapunov's direct method, we have demonstrated the local stability of the Lorenz system at the origin under restrictive conditions. This approach illustrates how energy-like functions can be constructed to assess nonlinear system behaviour without solving the differential equations.

## 5. Application

### 5.1. Sensitivity property Lorenz System: Strong security Layer

The Lorenz system has provided us with a useful tool for data encryption. Its chaotic property, due to the sensitivity to initial data, has become insightful. It is those properties we utilize in the encryption of data in the sense that a slight change in the initial data yields to a significantly different outcomes. That is to say that any two trajectories (states) of the Lorenz system with nearby initial data would rapidly deviate from each other, and after a significant time, only statistical statements can be made. The solution of the underlying system is presented in Figure 2, subject to a specific choice of initial data.



**Figure 2.** The solution of the Lorenz system with initial condition  $x(0) = 0, y(0) = 1, z(0) = 20$ .

Furthermore, the lowest Lyapunov Exponent is used to determine how fast the dynamical system trajectories converge or diverge and is defined by

$$\lambda_{\max} \approx \frac{1}{T_{\max}} \sum_{k=0}^N \ln \alpha_k, \quad \alpha_k = \frac{V(t_k)}{\varepsilon}$$

for  $V(t_k), k = 0, 1, 2, \dots, N$  being the variation of the Lyapunov function satisfying the

$$\dot{V} = Df(x(t), V).$$

The estimated value of the largest Lyapunov exponent is known to be  $\lambda_{\max} \approx 0.9630$ . Our computed LLE yields the value  $\lambda_{\max} \approx 0.799660829427996$  at maximum time  $T_{\max} = 100$  as shown in Figure 1. This shows a strong estimate for the underlying Lorenz system.

### 5.2. Entropy and Correlation Analysis

As the encryption and decryption involve the decomposition of matrix pixel into different colour channels, typically RGB, the measure of “disorder-ness” termed entropy of each colour is paramount. This is done before and after encryption. The entropy of each channel is computed as

$$H = - \sum_{i=1}^{N-1} p_i \log_2(p_i),$$

where  $p_i$  stands for the probability of the pixel intensity value  $i$  from  $0 \dots N - 1$ , say  $N = 256$  in our case. The  $p_i$  is estimated from the normalized histogram counts of these colour channels.

The entropy measures the uncertainty or the information content of the encrypted image. A uniform histogram shows a flat distribution and therefore means all intensities are equally likely, hence maximum entropy is attained. For the Lorenz-based encryption, this is an indication of how scrambled the pixel intensities become due to chaotic key generation.

In our implementation, higher entropies imply better encryption as pixel values carry no predictable information about the original image. The typical benchmark for an 8-bit colour channel is 8 bits for an ideal encrypted image.

The associated correlation for each colour channel is computed via

$$r = \frac{\sum_{i=1}^{N-1} (x_i - \bar{x})(x_{i+1} - \bar{x})}{\sqrt{\sum_{i=1}^{N-1} (x_i - \bar{x})^2 \sum_{i=1}^{N-1} (x_{i+1} - \bar{x})^2}}$$

This is called the *Pearson correlation coefficient* between adjacent pixels  $x_i$  and  $x_{i+1}$ . Its values lie in the interval  $[-1,1]$  with  $r \approx 1$  signifying high correlation (similar intensities) while  $r \approx 0$  means no correlation. The latter is unlikely needed in our context but the former is an ideal case for encryption. When  $r < 0$  and  $r > 0$ , it indicates the pixel are random and unrelated. Thus, good and successful encryption is expected when the correlation is close to 0 or negative.

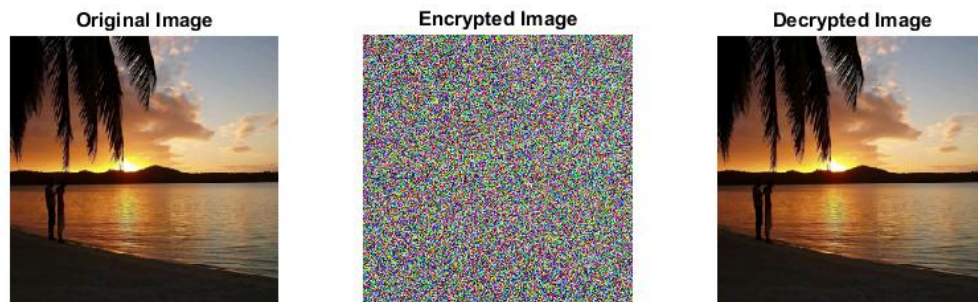
In the natural image, neighbouring pixels (those spatially close) are strongly correlated. One observes smooth edges and uniform regions. In principle, the encryption tends to destroy these correlations, producing a noise-like randomness. In the cryptographic context,  $|r| \approx 0$  implies high pixel dependence and in turn this is important for resisting statistical and differential attacks. Table 1 presents the summary of the expressions, interpretation, and significance of the terms entropy, correlations, and LLE.

**Table 1.** Summary of the expressions, interpretation, and significance of the terms entropy, correlations, and LLE.

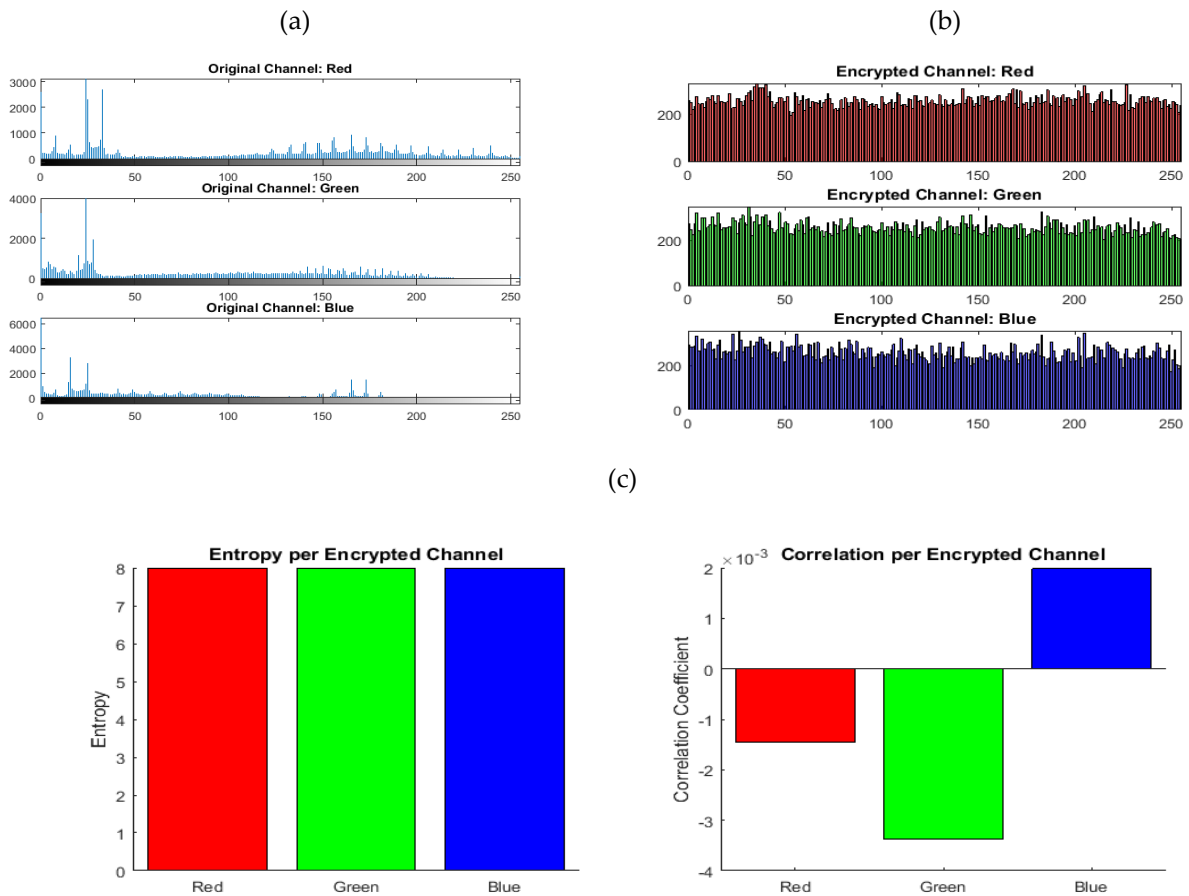
	Expression	Interpretation	Cryptographic implication
<b>Entropy</b>	$H = -\sum p_i \log_2 p_i$	Randomness of the pixel intensities	Higher value of $H \Rightarrow$ better confusion
<b>Correlation</b>	$r = \frac{\text{Cov}(x_i, x_{i+1})}{\sigma_x^2}$	Dependency between adjacent pixel	Lower $r \Rightarrow$ better diffusion
<b>Largest Lyapunov Exponent</b>	$\lambda_1 = \lim_{t \rightarrow \infty} \frac{1}{t} \ln \frac{  \delta X(t)  }{  \delta X(0)  }$	strong chaotic behaviour	excellent quality for cryptographic key
<b>Lowest Lyapunov Exponent</b>	$\lambda_3$	boundedness	Secure encryption

### 5.3. Image Encryption & Decryption

The following is an encryption and decryption of different images in JPEG format.



**Figure 3.** Image encryption and decryption.



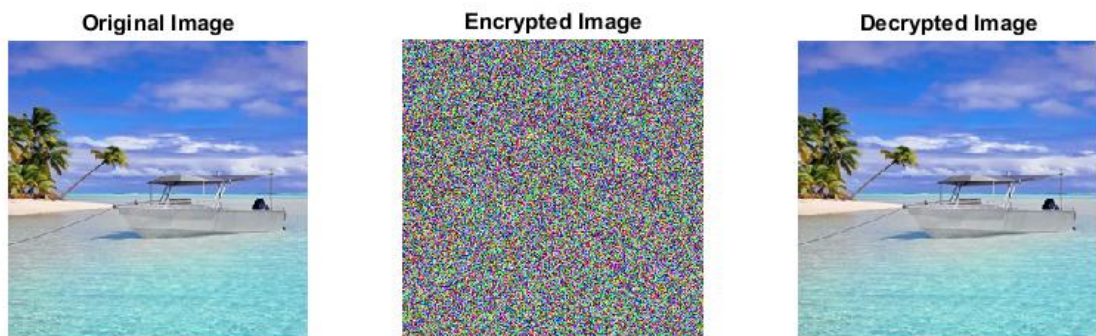
**Figure 4.** (a) The Histograms of the colours of the original image; (b) The histograms of the colours of the encrypted image and (c) The entropy of the colors before and after encryption of each colour.

For this image, entropy is used to measure the degree of randomness of our encryption.

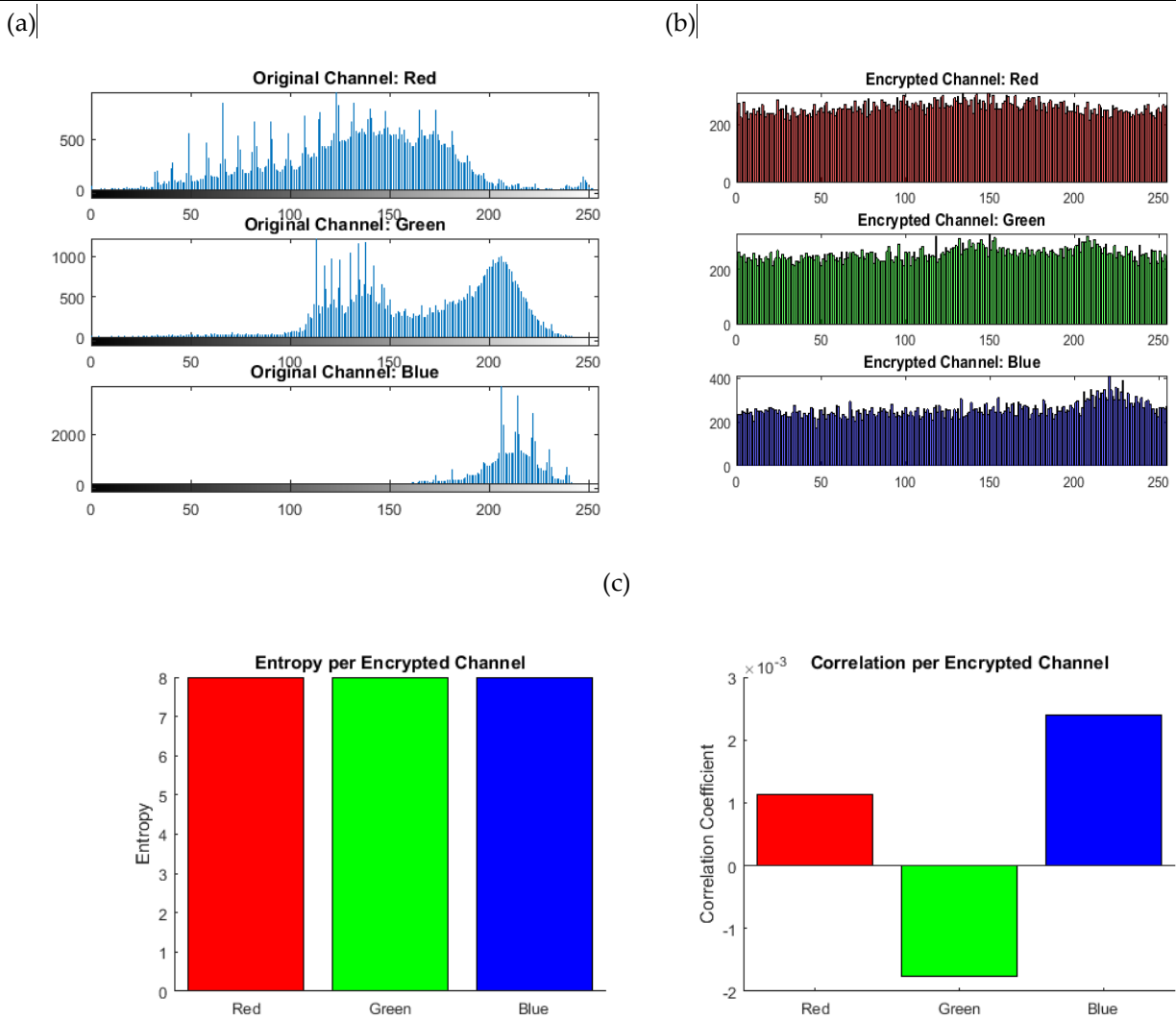
Entropy of encrypted channels: 7.9937, 7.9919, 7.9866.

Correlation of encrypted channels: -0.0015, -0.0034, 0.0020.

The Figure 4 (a)-(c) histograms and correlation results of the original image in Figure 3. As a result, a reliable and strong encryption is found based on the correlation analysis in Figure 4(c).



**Figure 5.** Image encryption and decryption.



**Figure 6.** (a) The Histograms of the colours of the original image; (b) The histograms of the colours of the encrypted image, and (c) The entropy of the colours before and after encryption.

Entropy of encrypted channels: 7.9953, 7.9938, 7.9879

Correlation of encrypted channels: 0.0011, -0.0018, 0.0024

Figure 6(a)-(c) shows histograms and correlation results of the original image in Figure 5. This as well results in a reliable and strong encryption, as shown by the correlation analysis in Figure 6(c).

#### 5.4. Comparative Evaluation

Table 2 presents the evaluation of some encryption algorithms, such as AES, Lorenz-Based as well as our Enhanced-Lorenz-based algorithm.

**Table 2.** Comparison of the key features of the AES , Lorenz-based, and Enhanced Lorenz-based encryptions.

Feature	AES	Lorenz-Based	Enhanced Lorenz-Based
Key Sensitivity	Low (fixed keys)	High	High (chaos-derived, continuous keys)
Algebraic Structure	Strong, well-studied	-	Moderate, enhanced via modular-prime mask

Resource Use	Medium to High	-	Low (simple operations)
Randomness (Entropy)	High	High	High
Pixel Correlation	Low (block-based mixing)	-	Low (strong diffusion)
Novel Security Layers	Substitution-permutation	-	Chaos + modular field + prime masking

## 6. Results and Discussion

We tested our scheme using standard colour images (256×256 pixels). Implementation was done in MATLAB, applying three stages: chaotic key generation via the Lorenz system, modular masking in  $\mathbb{Z}_{251}$ , and prime-number masking.

**Entropy:** Encrypted image channels achieved entropies of approximately 7.99–8.00—close to the ideal value for 8-bit channels, indicating high randomness.

**Pixel Correlation:** Adjacent pixel correlation coefficients were reduced to near-zero (e.g., between -0.002 and +0.002), confirming strong decorrelation.

### 6.1. Visual and Performance Insights

Encrypted images exhibit no visible structure, while decryption perfectly recovers the original. Computational performance is lightweight compared to AES, with fewer computational steps and modest memory usage. The algorithm is particularly advantageous for platforms like IoT or mobile devices.

**Discussion:** Our hybrid approach builds on the best of chaos theory and number theory. The chaotic Lorenz stream ensures unpredictability, while the modular and prime operations add algebraic security beyond XOR. Limitations include parameter tuning complexities and rigorous cryptanalysis (such as key space evaluation and resistance to chosen-plaintext attacks), which present opportunities for future research.

## 7. Conclusions

The developed hybrid approach blends the chaos-based encryption approach motivated by the Lorenz system and the number theoretical manipulation, thereby enhancing the encryption of data in image format. It has been established that the hybrid approach adds useful confusion, which in turn makes the encryption difficult to predict and free from differential and any statistical attack. The future study focuses on employing the developed approach on other type data, such as speech and video.

**Author contributions:** Conceptualization: Umar M.D., and Isah A.I, Methodology: Umar M. D., Writing-Original Draft: Umar M. D., Auwal L. AND Isah Ali Ibrahim, Editing: Umar M.D. and Yusuf H., Writing –Review and Editing: Umar M.D. & Yusuf H.

**Funding Statement:** This research received no external funding.

**Data Availability:** The data that support the findings are available from the corresponding author upon request.

**Acknowledgments:** Authors may acknowledge technical, editorial, or other support not covered under authorship.

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

## References

- [1] Ali Mohammad Norouzzadeh Gilmoik and Mohammad Reza Aref. (2024). Lightweight Image Encryption Using a Novel Chaotic Technique for the Safe Internet of Things. *International Journal of Computational Intelligence Systems* (2024) 17:146 <https://doi.org/10.1007/s44196-024-00535-3>.
- [2] Obaida M. Al-Hazaimeh, Mohammad F. Al-Jamal, Nouh Alhindawi, Abedalkareem Omari. (2017). Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys. *Neural Computing and Applications* ISSN 0941-0643.
- [3] Daniah Abul Qahar Shakir, Ahmad Salim, Seddiq Q. Abd Al-Rahman, Ali Makki Sagheer. (2022). Image Encryption Using Lorenz Chaotic System. *Journal of Techniques*, ISSN: 2708-8383, Vol. 5, No. 1, 2023.
- [4] Yexia Yao 1, Xuemei Xu 1,\* and Zhaohui Jiang 2. (2025). A New Chaotic Color Image Encryption Algorithm Based on Memristor Model and Random Hybrid Transforms. *Appl. Sci.* 2025, 15, 913..
- [5] Walaa Hadi Abdulnabi 1, a), Sadiq A. Mehdi 1, b), Sawsen Abdulhadi Mahmood 1, c). (2025). A New 3D Chaotic System and 3D Lorenz System for Color Image Encryption with Multi-Scales. *AIP Conf. Proc.* 3282, 030023 (2025).
- [6] Bahaa Abdulwahid Hameed and Ekhlak k. Gbashi1. (2024). A review of Chaotic Maps used for Generating Secure Random Keys. *BIO Web of Conferences* 97, 00070 (2024) ISCKU 2024.
- [7] Al-Maadeed, T.A., Hussain, I., Anees, A. et al. An image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes. *Multimed Tools Appl* 80, 24801–24822 (2021). <https://doi.org/10.1007/s11042-021-10695-5>
- [8] Zhang, B., & Liu, L. (2023). Chaos-Based Image Encryption: Review, Application, and Challenges. *Mathematics*, 11(11), 2585. <https://doi.org/10.3390/math11112585>.
- [9] Niu, Y., Zhou, H. & Zhang, X. Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators. *Sci Rep* 14, 7033 (2024). <https://doi.org/10.1038/s41598-024-57756-x>.
- [10] Tiwari, A., Diwan, P., Diwan, T.D. et al. A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication. *Sci Rep* 15, 14151 (2025). <https://doi.org/10.1038/s41598-025-95995-8>.
- [11] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.



**Disclaimer/Publisher's Note:** The views, opinions, and content expressed in all articles are solely those of the respective author(s) and contributor(s) and do not necessarily reflect those of the JSSCI, its editors, or the publisher. JSSCI and its editorial team assume no responsibility for any harm or damage resulting from the use of information, methods, or products mentioned in the publication.