Vedant Pansare

Final Thesis_compressed

Assignment2

Document Details

Submission ID

trn:oid:::27535:139867574

Submission Date

May 21, 2026, 3:28 PM GMT+5:30

Download Date

May 21, 2026, 3:30 PM GMT+5:30

File Name

Final Thesis_compressed.pdf

File Size

3.4 MB

51 Pages

10,852 Words

59,759 Characters

9% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Small Matches (less than 10 words)

Match Groups

51 Not Cited or Quoted 8%
Matches with neither in-text citation nor quotation marks

5 Missing Quotations 1%
Matches that are still very similar to source material

1 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

6% Internet sources
4% Publications
7% Submitted works (Student Papers)

Match Groups

- **51** Not Cited or Quoted 8%
  Matches with neither in-text citation nor quotation marks
- **5** Missing Quotations 1%
  Matches that are still very similar to source material
- **1** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

6% Internet sources
4% Publications
7% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Student papers	Rajiv Gandhi National University of Law on 2026-05-20	<1%
2	Internet	www.dspace.dtu.ac.in:8080	<1%
3	Student papers	Global Banking Training on 2026-05-15	<1%
4	Student papers	Delhi Technological University on 2026-04-29	<1%
5	Publication	Sen Zhang, Yi Cheng Zeng, Zhi Jun Li. "A Novel 4D No-equilibrium Hyper-chaotic S...	<1%
6	Student papers	The University of Manchester on 2025-09-05	<1%
7	Internet	ia601409.us.archive.org	<1%
8	Internet	www.mdpi.com	<1%
9	Publication	Qi Xie, Yicheng Zeng. "Generating different types of multi-double-scroll and multi...	<1%
10	Student papers	University of College Cork on 2026-03-27	<1%

11 Internet

www.aimspress.com <1%

12 Internet

pdfs.semanticscholar.org <1%

13 Student papers

University of Sulaimani on 2026-04-10 <1%

14 Student papers

Indian Institute of Technology, Madras on 2017-01-13 <1%

15 Publication

Khaled Aldwoah, E. I. Hassan, Mohammed Alsharafi, Amal F. Alharbi. "Hyperchaot... <1%

16 Student papers

National University of Singapore on 2007-08-06 <1%

17 Student papers

University of Sunderland on 2024-05-26 <1%

18 Internet

era.library.ualberta.ca <1%

19 Internet

jurnal.stkippgritulungagung.ac.id <1%

20 Student papers

Delhi Technological University on 2026-05-07 <1%

21 Student papers

Indian Institute of Technology, Madras on 2026-05-08 <1%

22 Internet

www.numberanalytics.com <1%

23 Publication

Pengfei Ding, Jingge Zhu, Juan Zhang. "A four-dimensional no-equilibrium chaotic... <1%

24 Internet

fds.duke.edu <1%

25 Publication

Cars H. Hommes, Helena E. Nusse, András Simonovits. "Cycles and chaos in a soci... <1%

26 Publication

Yuming Sun, Xiangpeng Wang, Qiong Wu, Nariman Sepehri. "On stability analysis... <1%

27 Internet

coek.info <1%

28 Internet

pubs.asahq.org <1%

29 Student papers

Pranveer Singh Institute Of Technology, Kanpur (PSIT) on 2026-05-05 <1%

30 Student papers

University of Bristol on 2008-11-04 <1%

31 Student papers

University of Newcastle upon Tyne on 2012-08-30 <1%

32 Internet

discovery-pp.ucl.ac.uk <1%

33 Publication

"Bio-Inspired Computing -- Theories and Applications", Springer Nature, 2015 <1%

34 Student papers

Delhi Technological University on 2026-05-13 <1%

35 Publication

Fei Yu, Xuqi Wang, Rongyao Guo, Zhijie Ying, Shuo Cai, Jie Jin. "Dynamical analysis... <1%

36 Publication

Mishra, D.C., R.K. Sharma, Rakesh Ranjan, and M. Hanmandlu. "Security of RGB i... <1%

37 Internet

di.univ-blida.dz <1%

38 Internet

www.jestr.org <1%

39 Student papers

Indian Institute of Technology, Madras on 2016-05-02 <1%

40 Student papers

Odisha University of Technology and Research on 2026-05-01 <1%

41 Student papers

SASTRA University on 2014-02-17 <1%

42 Student papers

University of Sussex on 2025-04-28 <1%

43 Internet

d197for5662m48.cloudfront.net <1%

44 Internet

springerplus.springeropen.com <1%

45 Internet

tudr.thapar.edu:8080 <1%

A Novel 4D No-Equilibrium Hyperchaotic System with Applications in Synchronization and Image Encryption

2

A DISSERTATION

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE OF

MASTER OF SCIENCE

IN

APPLIED MATHEMATICS

submitted by

Garvit Lodha
(24/MSCMAT/50)

2

Under the Supervision of
Dr. Dhirendra Kumar

DEPARTMENT OF APPLIED MATHEMATICS
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi–110042

MAY 2026

Delhi Technological University

(Formerly Delhi College of Engineering)

Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, **Garvit Lodha**, hereby certify that the work which is being presented in the dissertation entitled **"A Novel 4D No-Equilibrium Hyperchaotic System with Applications in Synchronization and Image Encryption"** in partial fulfillment of the requirements for the award of the Degree of Master of Science submitted in the Department of Applied Mathematics, Delhi Technological University, Delhi is an authentic record of my own work carried out during the period from August 2025 to May 2026 under the supervision of Dr. Dhirendra Kumar.

The matter presented in the dissertation has not been submitted by me for the award of any other degree of this or any other Institute.

Garvit Lodha
Roll no. 24/MSCMAT/50

20

Delhi Technological University

(Formerly Delhi College of Engineering)

Bawana Road, Delhi-110042

CERTIFICATE BY SUPERVISOR

1

1

Certified that **Mr. Garvit Lodha** (Roll no. 24/MSCMAT/50) has carried out his research work presented in this dissertation entitled **"A Novel 4D No-Equilibrium Hyperchaotic System with Applications in Synchronization and Image Encryption"** for the award of **Master of Science** from Department of Applied Mathematics, Delhi Technological University, Delhi, under my supervision. The dissertation embodies results of original work, and studies are carried out by the student himself and the contents of the dissertation do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

Dr. Dhirendra Kumar
Supervisor
Department of Applied Mathematics
Delhi Technological University
Delhi.

Delhi Technological University

(Formerly Delhi College of Engineering)

Bawana Road, Delhi-110042

PLAGIARISM VERIFICATION

Title of the Thesis: **"A Novel 4D No-Equilibrium Hyperchaotic System with Applications in Synchronization and Image Encryption"**. Total Pages: **65**. Name of the Student: **Garvit Lodha (24/MSCMAT/50)** for the award of Master of Science from Department of Applied Mathematics, Delhi Technological University, Delhi, under my supervision.

This is to report that the above thesis was scanned for similarity detection. Process and outcome is given below:

Software used: **Turnitin**.
Similarity Index: **–%**
Total Word Count: **—**

Place: Delhi **Dr. Dhirendra Kumar**

Date: 23/05/2026 **SUPERVISOR**

ACKNOWLEDGEMENT

31 I express my sincere gratitude to my supervisor **Dr. Dhirendra Kumar**, for his motivation and unconditional support during my dissertation work. It has been a great pleasure to work under his guidance, and I am deeply thankful for his invaluable assistance in making this work possible.

34 I am thankful to the Head of the Department, **Prof. R. Srivastava**, and all the faculty members of the Department of Applied Mathematics for their support and for providing me the necessary help during my M.Sc. coursework.

Finally, I am deeply grateful to **Ms. Devleena Kashyap**, Ph.D. Scholar, Department of Applied Mathematics, for her guidance and constant help throughout my dissertation work. Her insights and suggestions have been truly valuable.

Date: 23 May 2026 **Garvit Lodha**
Place: Delhi, India.

ABSTRACT

Four-dimensional chaotic models, such as the no-equilibrium system proposed by Zhang et al. [1], offer significant cryptographic advantages by generating hidden attractors. However, they often fall short of true hyperchaos by producing only a single positive Lyapunov exponent. This research addresses this limitation to significantly expand the available cryptographic key space. We transform a standard 4D chaotic framework into a robust 4D hyperchaotic system. This is achieved by replacing simple polynomial nonlinearities with a custom hybrid activation function. By blending signum and sigmoid traits with layered shifting functions, the proposed system sustains deep hyperchaotic behavior.

A comprehensive dynamical analysis confirms the complete absence of fixed points. Crucially, the system exhibits two independent positive Lyapunov exponents. This guarantees the generation of highly complex, unpredictable hidden attractors. The system's complexity is further validated by a Kaplan–Yorke dimension of approximately 3.174 and severe structural randomness, indicated by a Shannon entropy of 4.6715.

The practical viability of the system is demonstrated across two secure communication scenarios. First, an active control synchronization strategy is implemented. This successfully drives synchronization errors to machine precision (10^{-14}) at an exponential rate. Second, the system serves as a keystream generator for a rigorous image encryption algorithm. This algorithm utilizes argsort-based spatial permutation alongside chained XOR diffusion.

The resulting ciphertexts achieve a near-ideal information entropy of 7.997 bits, perfectly flat intensity histograms, and essentially zero adjacent pixel correlation. Furthermore, the algorithm achieves an NPCR of 99.4787% against sub-microscopic key perturbations. These results demonstrate that the engineered 4D no-equilibrium hyperchaotic system provides superior resistance to statistical and differential cryptanalysis when compared to standard chaotic maps.

Keywords: Hyperchaotic system; Hidden attractors; No-equilibrium; Lyapunov exponents; Kaplan–Yorke dimension; Adaptive synchronization; Image encryption; Secure communication.

Contents

1 Introduction **2**

1.1 Background 2

16 1.2 Motivation 2

1.3 Objectives 3

1.4 Organization of the Thesis 4

2 Preliminaries **5**

2.1 Literature Review 5

2.1.1 Hyperchaotic Systems 5

2.1.2 Chaos-based Image Encryption 6

2.2 Performance Measures of Chaotic Systems 6

2.2.1 Lyapunov Exponents 7

2.2.2 Phase Portraits 7

2.2.3 Bifurcation Diagrams 8

2.2.4 Kaplan–Yorke Dimension 8

2.2.5 Poincaré Map 8

2.3 Performance Measures of Image Encryption 8

2.3.1 Information Entropy 9

2.3.2 Pixel Correlation 9

2.3.3 Histogram Analysis 9

2.3.4 Key Sensitivity Analysis 9

2.3.5 MSE and PSNR 10

2.4 Data-set Description 10

3 Proposed Hyperchaotic System and Its Applications **12**

3.1 Background 12

3.1.1 Equilibrium Points 12

3.1.2 Lyapunov Spectrum and Kaplan–Yorke Dimension 13

3.1.3 Phase Portraits 13

3.2 Proposed System 15

3.3 Analysis of Proposed System 16
3.3.1 Lyapunov Spectrum and Kaplan–Yorke Dimension 16
3.3.2 Phase Portraits 18
3.3.3 Bifurcation Analysis 21
3.3.4 Lyapunov Convergence 22
3.3.5 Lyapunov Spectrum vs Parameter b 23
3.3.6 Time Series Analysis 24
3.3.7 Entropy Analysis 24
3.3.8 Poincaré Map 25
3.3.9 Lyapunov Convergence Comparison Across All N, M 26
3.4 Applications 26
3.4.1 Synchronization 26
3.4.2 Image Encryption 30

30

4 Conclusions and Future Scope 37
4.1 Conclusions 37
4.2 Future Scope 38

List of Figures

2.1 Left: Exponential divergence of nearby trajectories demonstrating sensitive dependence on initial conditions ($\lambda_1 > 0$). Right: Lyapunov exponent spectrum of a 4D hyperchaotic system, characterized by two positive exponents ($\lambda_1 > 0, \lambda_2 > 0$). 7

3.1 Phase portraits of the base system [1] showing the double-wing attractor structure in the x–y and z–y planes. Parameters: $a = 15$, $b = 4$, $c = 1$, $d = 0.1$; IC $= (1,1,1,1)$. 14

3.2 Lyapunov spectrum of the base system vs parameter b (top: all four exponents; bottom: largest exponent $\lambda_{\max}$ with chaotic and stable regions shaded). λ_2 never crosses into positive territory in a sustained way, confirming the system remains chaotic only throughout the parameter range studied. 14

3.3 2D phase portraits of the proposed system at $N = 2$, $M = 2$ showing (left) x–y projection with double-wing topology, (centre) x–z projection with S-shaped twisted loop, and (right) y–z projection with layered double-ring structure. 18

3.4 3D strange attractor of the proposed system at $N = 2$, $M = 2$ projected onto the x–y–z subspace and coloured by normalised time. The diffuse elongated band fills a substantially larger volume than the thin looping structure of the base system, consistent with the higher Kaplan–Yorke dimension of $D_{KY} = 3.17446$. 19

3.5 Phase portrait comparisons for $N = 1, M = 1$ and $N = 2, M = 1$. 20

3.6 Phase portrait comparisons for $N = 2, M = 2$ and $N = 2, M = 3$. 21

3.7 Bifurcation diagrams of the state variables x, y, z, and w as parameter b varies from 0 to 6. The dense, continuous bands across the parameter space indicate robust hyperchaotic behavior without significant periodic windows. 22

3.8 Convergence of the Lyapunov spectrum for the proposed system at $N = 2, M = 2$. Both λ_1 and λ_2 settle above zero, confirming hyperchaotic behaviour. All four exponents converge by approximately $t = 400$. . . . 23
3.9 Lyapunov spectrum vs parameter b for the proposed system at $N = 2$, $M = 2$. Both λ_1 and λ_2 remain positive across the entire range of b studied, confirming that hyperchaos is a robust and persistent property of the system. 24
3.10 Time series analysis of the proposed hyperchaotic system for state variables x, y, and z over time $t \in [40, 400]$, demonstrating bounded, non-periodic chaotic oscillations. 24
3.11 Extended time series of the state variable x utilized for the Shannon and Permutation entropy calculations. 25
3.12 Poincaré map of the proposed hyperchaotic system on the $z = 0$ cross-section at parameter $b = 3.0$. The dense, scattered distribution of points confirms the presence of a highly complex strange attractor. 26
3.13 Lyapunov convergence comparison. Transition from single to dual positive exponents as N and M increase. 27
3.14 Active control synchronization results for the proposed hyperchaotic system ($N = 2$, $M = 2$). Top four panels: time evolution of drive and response state pairs (x, x_r), (y, y_r), (z, z_r), (w, w_r) — convergence is achieved within approximately 10 time units. Bottom left: synchronization error norm on a logarithmic scale, reaching machine precision ($\approx 10^{-14}$) by $t \approx 12$. Bottom right: drive vs response phase plot collapsing onto the diagonal, confirming complete synchronization. Drive IC: $(1, 1, 1, 1)$; Response IC: $(0.5, -1.0, 3.0, -2.5)$; control gains $k_i = 3$. . . 30
3.15 Original image (left), encrypted image (centre), and decrypted image (right). The encrypted image is visually indistinguishable from random noise. Decryption with the correct key recovers the original exactly: MSE(Dec↔Orig)= 0, PSNR(Dec↔Orig)= ∞ dB. 32
3.16 Pixel intensity histograms for R, G, B channels before (top row) and after (bottom row) encryption. The highly non-uniform original distributions become essentially flat after encryption, indicating effective concealment of pixel value statistics. 33
3.17 Information entropy for each colour channel before and after encryption. All encrypted channels exceed the 7.99-bit threshold and approach the theoretical maximum of 8.0 bits, confirming near-ideal randomness in the ciphertext. 33

3.18 Pixel correlation scatter plots for the Red channel. Top row: original image showing tight diagonal clusters in all three directions (H, V, D), confirming high spatial correlation. Bottom row: encrypted image showing uniformly scattered point clouds with correlation values near zero, confirming complete decorrelation. 34
3.19 MSE (left) and PSNR (right) for encrypted vs original and decrypted vs original comparisons. The high encryption MSE (12059.83) and low PSNR (7.32 dB) confirm strong pixel-level confusion. Perfect lossless decryption is confirmed by MSE = 0 and PSNR = ∞ dB. 35
3.20 Key Sensitivity analysis. Left: original image. Centre: decrypted image with correct key — perfect recovery confirmed (MSE = 0, PSNR = ∞ dB). Right: decrypted image with key perturbed by $\Delta = 1 \times 10^{-14}$ — output is completely random noise with pixel change rate 99.4787%, demonstrating full avalanche under key perturbation. 35

List of Tables

3.1 Lyapunov spectrum of the base system [1]. Parameters: $a = 15$, $b = 4$, $c = 1$, $d = 0.1$; IC $= (1,1,1,1)$. 13
3.2 Lyapunov spectrum and Kaplan–Yorke dimension for different N and M values. Parameters: $a = 8$, $b = 4$, $c = 1$, $d = 0.01$, $e = 0.1$, $A = 0.4$, $\alpha = 0.3$, $k = 6$; IC $= (1,1,1,1)$. 17
3.3 Largest Lyapunov exponent λ_1 and Kaplan–Yorke dimension D_{KY} across all tested N, M combinations. 17
3.4 Pixel correlation coefficients for the Red channel before and after encryption in horizontal (H), vertical (V), and diagonal (D) directions. . . 34
3.5 Complete security metrics summary for the proposed image encryption scheme tested on `4.1.01.tiff`. 36

Chapter 1

Introduction

1.1 Background

The study of nonlinear dynamical systems has given rise to one of the most fascinating phenomena in modern science — chaos. What makes chaotic systems particularly striking is that although they follow completely deterministic mathematical rules, their long-term behavior becomes practically impossible to predict. This happens not because of any randomness in the system, but because even the tiniest difference in starting conditions grows exponentially over time, causing two nearly identical initial states to evolve into completely different trajectories. Together with topological mixing and dense periodic orbits, this sensitivity forms the core mathematical character of chaos. These same properties make chaotic systems naturally attractive for cryptographic use. Their complex, pseudo-random outputs break down the correlation between neighboring pixels in an image and hold up well against statistical and differential attacks. Going a step further, hyperchaos extends classical chaos by exhibiting more than one positive Lyapunov exponent, which means the system expands in multiple phase-space directions at once. This results in richer dynamics, a significantly larger key space, and stronger unpredictability. Making hyperchaotic systems particularly well suited for demanding encryption tasks. Among the known chaotic systems, the Sprott B system stands out for its algebraic simplicity and well-established chaotic behavior, making it a natural starting point for constructing a more complex hyperchaotic system.

1.2 Motivation

The evolution of chaos-based image encryption has rendered traditional methods increasingly inadequate. Earlier approaches relied on conventional chaotic mechanisms, which are often characterized by limited sensitivity ranges and insufficient dynamical

complexity. These inherent weaknesses make such systems susceptible to advanced security threats, including system-identification and phase space reconstruction attacks.

Consequently, the overall security of any cryptographic framework is intrinsically linked to the richness and unpredictability of its underlying dynamical system. When the governing dynamics are constrained by these limitations, the integrity of the entire cryptographic architecture is compromised.

Hyperchaotic systems, characterized by multiple positive Lyapunov exponents, offer a promising approach to enhancing system complexity by increasing the number of phase-space dimensions. However, there remains a dearth of research on the design of novel hyperchaotic systems grounded in simple, comprehensible chaotic bases in the existing literature.

The modified Sprott B system, derived from the original Sprott B chaotic flow, provides a compelling foundation for this type of expansion due to its compact algebraic structure and robust chaotic behavior. Nonetheless, the hyperchaotic generalization of this system has received limited scholarly attention. Consequently, this research is predicated on the concept of developing a new hyperchaotic system by incorporating nonlinear terms into the enhanced Sprott B system. This approach aims to broaden the sensitivity range and elevate the dynamical complexity, thereby leveraging these advancements for secure image encryption. The anticipated outcome is a larger key space, which would enhance resilience against cryptanalytic attacks compared to traditional chaotic schemes.

29

1.3 Objectives

The primary objectives of this research are as follows:

(a) To develop a new four-dimensional hyperchaotic system by introducing nonlinear terms into a modified Sprott B chaotic system, with the aim of broadening its sensitivity range and enhancing its dynamical complexity.

(b) To analyze the dynamical properties of the proposed system, covering equilibrium points, stability analysis, Lyapunov exponents, bifurcation diagrams, phase portraits, and Kaplan–Yorke dimension.

(c) To implement a chaos-based image encryption scheme using the proposed hyperchaotic system, employing confusion and diffusion operations to disrupt pixel correlation and destroy plaintext structure.

(d) To evaluate the performance of the encryption scheme through standard security metrics including information entropy, pixel correlation, histogram analysis, and key sensitivity analysis.

39

(e) To demonstrate the effectiveness of the proposed system through numerical simulations and compare key results with relevant existing work in the literature.

18

1.4 Organization of the Thesis

The remainder of this thesis is organized as follows:

- **Chapter 2** reviews the relevant literature on hyperchaotic systems and chaos-based image encryption, and covers the performance measures used to assess both — including Lyapunov exponents, phase portraits, and bifurcation diagrams for the chaotic system, and information entropy, pixel correlation, histogram analysis, and key sensitivity for the encryption scheme.
- **Chapter 3** presents a four-dimensional hyperchaotic system developed from a modified form of the Sprott B chaotic flow. A thorough dynamical analysis of the system is conducted, followed by an investigation of its synchronization using active control techniques, which confirms the system's suitability for secure communication applications. The chapter further describes an image encryption scheme constructed on the basis of this system, accompanied by an extensive evaluation of its security performance
- **Chapter 4** concludes the thesis by summarizing the main findings and contributions of this work and outlining directions for future research.

Chapter 2

Preliminaries

2.1 Literature Review

2.1.1 Hyperchaotic Systems

The concept of hyperchaos was formally established by Rössler [2] in 1979. By utilizing a four-dimensional autonomous system, he demonstrated that a dynamical system could possess multiple positive Lyapunov exponents. This discovery revealed behavior significantly more complex than that observed in traditional three-dimensional chaotic systems. Consequently, this established a new class of dynamical systems that expand in multiple phase-space directions, rendering their trajectories substantially more difficult to predict or reconstruct.

Following this development, the construction of hyperchaotic systems from established chaotic bases became a prominent research focus. Sprott [3] provided a foundational contribution in 1994 by conducting a systematic computational search. This identified nineteen algebraically simple three-dimensional chaotic flows, including the Sprott B system, which serves as the foundation for the system proposed in this work.

Building upon these foundations, Zhang et al. [1] introduced a novel four-dimensional hyperchaotic system. This system is capable of generating grid multi-wing hidden attractors in the absence of equilibrium points. Because the system lacks equilibrium points, conventional stability analysis techniques are not applicable; by definition, these attractors are hidden, providing enhanced resistance against reconstruction-based attacks. The system was validated through its Lyapunov exponent spectrum, bifurcation diagrams, and phase portraits, confirming robust hyperchaotic behavior across a broad parameter range.

23

Similarly, Ding et al. [4] presented a four-dimensional no-equilibrium chaotic system that generates multi-scroll hidden attractors with direct applications in image encryption.

Their research demonstrated that the absence of equilibrium points results in richer dynamical behavior. This complexity translates into measurable improvements in encryption security, establishing no-equilibrium hyperchaotic systems as a compelling framework for cryptographic applications.

2.1.2 Chaos-based Image Encryption

Parallel to advancements in hyperchaotic system design, chaos-based image encryption has emerged as a robust field of study.

Shoreh et al. [5] investigated the synchronization of complex hyperchaotic systems with unknown parameters. Utilizing an adaptive algorithm grounded in Lyapunov stability theory, they demonstrated that these systems can be reliably synchronized despite parameter uncertainty. This property is particularly relevant for secure communication protocols and cryptographic key agreement, underscoring the practical utility of hyperchaotic systems beyond theoretical exploration.

In the domain of image encryption, Pal and Kumar [6] proposed a two-dimensional hyperchaotic map derived from the Zirili optimization function. They utilized this map to develop an encryption algorithm featuring cascading confusion transformations and a modified cyclic diffusion process. Their scheme achieved superior performance across various security metrics and demonstrated notable robustness against data occlusion and noise-based attacks.

In a related study, Pal and Kumar [7] introduced the coupled Kaplan–Yorke–Logistic map. This approach integrates two established chaotic maps to extend chaotic orbit lengths and enhance output distribution. Their encryption algorithm employs simultaneous confusion and diffusion processes to reduce computational overhead without compromising security, rendering it suitable for real-time applications.

Furthermore, Pal and Kumar [8] introduced a novel chaotic map with enhanced dynamics tailored for image encryption. This contribution further validates the efficacy of designing purpose-built chaotic systems specifically for cryptographic applications.

2.2 Performance Measures of Chaotic Systems

A rigorous analysis of any proposed chaotic or hyperchaotic system requires a set of well-established dynamical tools. The following measures are used in this work to characterize the proposed system.

2.2.1 Lyapunov Exponents

Lyapunov exponents measure the average divergence or convergence rate of nearby trajectories. The maximal exponent, λ, is defined as:

$$\lambda = \lim_{t\to\infty} \frac{1}{t} \ln \frac{\|\delta\mathbf{x}(t)\|}{\|\delta\mathbf{x}(0)\|} \tag{2.1}$$

Here, $\delta\mathbf{x}(0)$ and $\delta\mathbf{x}(t)$ represent the separation vectors at time zero and time t.

An n-dimensional system has n exponents, ordered as $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. The signs of the largest exponents dictate the system's dynamic behavior:

- **Stable Fixed Point:** $\lambda_1 < 0$. Trajectories converge.
- **Periodic Cycle:** $\lambda_1 = 0$. The system oscillates predictably.
- **Chaotic:** $\lambda_1 > 0$. Trajectories diverge exponentially.
- **Hyperchaotic:** $\lambda_1 > 0$ and $\lambda_2 > 0$. Trajectories diverge in multiple directions simultaneously.

Computationally, this spectrum is evaluated by applying QR decomposition [9] to the system's variational equations.

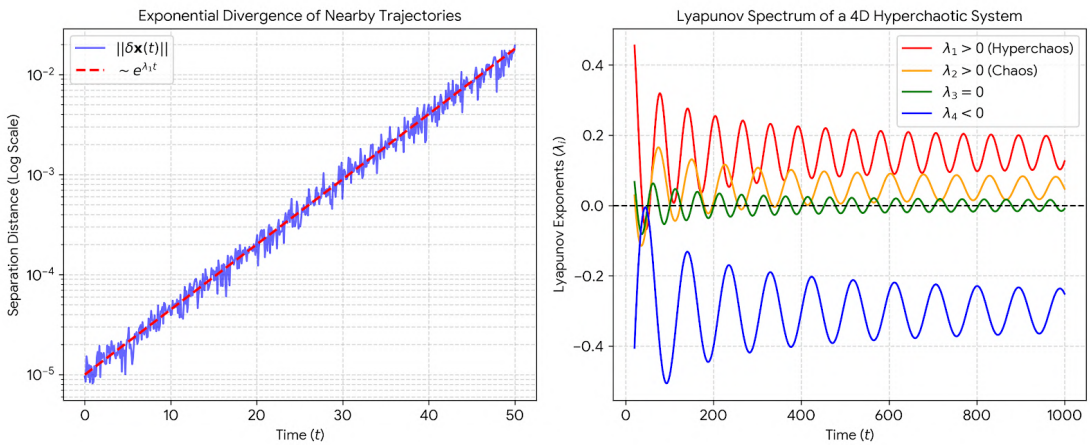


Figure 2.1: Left: Exponential divergence of nearby trajectories demonstrating sensitive dependence on initial conditions ($\lambda_1 > 0$). Right: Lyapunov exponent spectrum of a 4D hyperchaotic system, characterized by two positive exponents ($\lambda_1 > 0, \lambda_2 > 0$).

2.2.2 Phase Portraits

A phase portrait is a graphical representation of the trajectories of a dynamical system in its state space. By plotting the state variables against each other. for example x versus y, or y versus z the geometric structure of the attractor can be visualized. A strange attractor with a fractal, non-repeating structure in the phase portrait confirms chaotic or

hyperchaotic behavior. For a four-dimensional system, multiple two-dimensional and three-dimensional projections are typically examined.

2.2.3 Bifurcation Diagrams

A bifurcation diagram shows how the long-term behavior of a system changes as one of its parameters is varied. By plotting the local maxima of a state variable against a varying parameter, the transition from periodic to chaotic to hyperchaotic behavior can be clearly observed. Regions of dense, continuous values indicate chaos, while discrete bands indicate periodic behavior. Bifurcation diagrams are essential for identifying the parameter ranges over which the proposed system exhibits hyperchaotic behavior.

2.2.4 Kaplan–Yorke Dimension

The Kaplan–Yorke dimension provides an estimate of the fractal dimension of the attractor and is computed directly from the Lyapunov spectrum as:

$$D_{KY} = j + \frac{\sum_{i=1}^{j} \lambda_i}{|\lambda_{j+1}|} \tag{2.2}$$

where j is the largest integer for which $\sum_{i=1}^{j} \lambda_i \geq 0$. A non-integer value of D_{KY} confirms the fractal nature of the attractor, and a higher value indicates greater dynamical complexity.

2.2.5 Poincaré Map

A Poincaré map is constructed by recording the points at which a trajectory crosses a chosen hyperplane in phase space. For a chaotic system, the resulting points form a complex, structured cloud rather than a finite set of discrete points as would be seen for periodic behavior. The Poincaré map provides a lower-dimensional view of the attractor's structure and serves as a useful visual confirmation of chaotic dynamics.

2.3 Performance Measures of Image Encryption

The security and effectiveness of the proposed image encryption scheme are evaluated using the following standard metrics.

2.3.1 Information Entropy

Information entropy measures the randomness of the pixel intensity distribution in an image and is defined as:

$$H(m) = -\sum_{i=0}^{255} P(m_i) \log_2 P(m_i) \tag{2.3}$$

where $P(m_i)$ is the probability of pixel intensity value m_i. For a perfectly random image, all 256 intensity values are equally probable, giving an ideal entropy of 8.0 bits. A value close to 8.0 in the encrypted image indicates that the encryption has effectively destroyed all statistical structure in the original image.

2.3.2 Pixel Correlation

In a natural image, adjacent pixels — whether horizontal, vertical, or diagonal neighbors — tend to be highly correlated, with correlation coefficients close to 1. A secure encryption scheme must reduce this correlation to near zero. The correlation coefficient r_{xy} between two sets of adjacent pixels x and y is computed as:

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2.4}$$

Values of r_{xy} close to zero in the encrypted image confirm that inter-pixel correlation has been effectively eliminated.

2.3.3 Histogram Analysis

The pixel intensity histogram of a plaintext image typically shows a non-uniform distribution reflecting the image content. After encryption, the histogram should be as flat and uniform as possible, indicating that pixel intensities are evenly distributed across all 256 values. A uniform histogram confirms that no statistical information about the original image can be inferred from the cipher image.

2.3.4 Key Sensitivity Analysis

A secure encryption scheme must be highly sensitive to its key — a tiny change in the key should produce a completely different cipher image, and decryption with even a slightly incorrect key should fail entirely. Key sensitivity is tested by encrypting an image with the correct key and attempting decryption with a key perturbed by as little as 10^{-14}. The resulting image should be visually indistinguishable from random noise, confirming that the key space is effectively continuous.

2.3.5 MSE and PSNR

19 Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) measure the difference between two images. Between the original and encrypted image, a high MSE and low PSNR are desirable, confirming strong visual difference. Between the original and correctly decrypted image, MSE should be exactly zero and PSNR infinite, confirming perfect recovery. They are defined as:

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left[P(i,j) - C(i,j) \right]^2 \tag{2.5}$$

$$\text{PSNR} = 10 \log_{10} \left(\frac{255^2}{\text{MSE}} \right) \tag{2.6}$$

8 where $P(i,j)$ and $C(i,j)$ are the pixel values of the plaintext and ciphertext images, respectively, and $M \times N$ is the image size.

2.4 Data-set Description

44 The images used in this work are taken from the USC-SIPI Image Database[1], a widely
24 referenced repository maintained by the Signal and Image Processing Institute at the University of Southern California. The database provides a collection of digitized images spanning multiple categories, including textures, aerial photographs, and miscellaneous scenes, at varying resolutions. Images from this database have been extensively used in the image processing and encryption literature, making them a reliable and standard benchmark for comparative evaluation.

For the purpose of this work, color images of different sizes are selected to test the proposed encryption scheme across a range of visual content types — from smooth, uniform textures to structurally complex patterns. Unlike gray-scale images, color images carry information across three independent channels, namely the red, green, and blue components, which makes the encryption task more demanding and the evaluation more comprehensive. This diversity in content ensures that the evaluation is not biased toward any particular image characteristic and reflects the practical applicability of the scheme.

37 To assess the security and computational performance of the proposed algorithm, a series of experiments is carried out on these images. The results are further compared with those reported in recent related works using standard security metrics. All numerical simulations were carried out using Python 3.10 on Google Colaboratory, which provides

[1] https://sipi.usc.edu/database/database.php

17

a cloud-based execution environment well suited for scientific computing tasks. The local system used for development and testing ran a 64-bit Windows 11 operating system, powered by an AMD Ryzen 5 5500U processor with Radeon Graphics at 2.10 GHz and 8.00 GB of installed RAM.

Chapter 3

Proposed Hyperchaotic System and Its Applications

3.1 Background

The work in this thesis builds on a four-dimensional chaotic system introduced by Zhang et al. [1], which itself grew out of the structure of the well-known Sprott B chaotic flow. By applying a state feedback control technique to that simpler three-dimensional base, Zhang et al. arrived at the following autonomous system:

$$\dot{x} = -yz - dw \tag{3.1}$$

$$\dot{y} = z^2 - 1 \tag{3.2}$$

$$\dot{z} = ax - byz - z \tag{3.3}$$

$$\dot{w} = cz \tag{3.4}$$

Here x, y, z, and w are the four state variables, while a, b, c, and d are positive real parameters. At $a = 15$, $b = 4$, $c = 1$, $d = 0.1$, starting from $(1, 1, 1, 1)$, the system settles into a chaotic regime.

3.1.1 Equilibrium Points

To find equilibrium, all four derivatives are set to zero simultaneously. The fourth equation $\dot{w} = cz = 0$ immediately gives $z = 0$. Plugging this back into the second equation gives $\dot{y} = 0^2 - 1 = -1$, which can never be zero regardless of the other variables. So the system simply has no equilibrium points at all. This puts it in the category of hidden attractor systems — systems whose attractors cannot be found by the usual approach of

starting near an equilibrium, because no equilibrium exists to start from.

3.1.2 Lyapunov Spectrum and Kaplan–Yorke Dimension

Numerical computation of the Lyapunov spectrum yields:

$$\lambda_1 = 0.0190, \quad \lambda_2 = -0.0055, \quad \lambda_3 = -0.0350, \quad \lambda_4 = -1.3749 \tag{3.5}$$

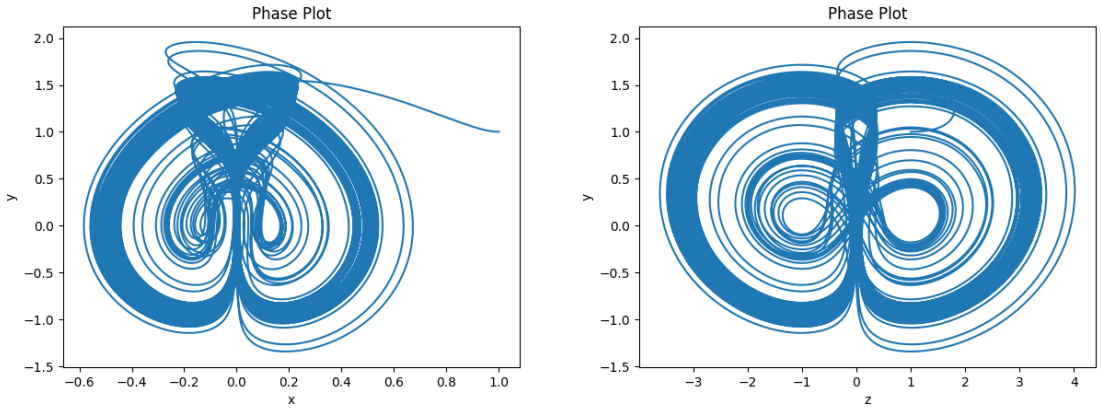
The full spectrum is summarised in Table 3.1. Only λ_1 is positive, which means the system is chaotic but falls short of hyperchaos — hyperchaos requires at least two positive exponents. The Kaplan–Yorke dimension comes out to $D_{KY} = 2.3849$, a relatively modest value reflecting the limited complexity of the attractor. The negative total $\sum \lambda_i$ confirms the system is dissipative. Looking at the Lyapunov spectrum across different values of b in Figure 3.2, λ_2 consistently stays near zero or dips negative, never crossing into positive territory in a sustained way. So across the parameter range studied, the system remains chaotic rather than hyperchaotic.

Table 3.1: Lyapunov spectrum of the base system [1]. Parameters: $a = 15$, $b = 4$, $c = 1$, $d = 0.1$; IC $= (1, 1, 1, 1)$.

Exponent	Value	Type
λ_1	$+0.0190$	Positive (chaos)
λ_2	-0.0055	Negative
λ_3	-0.0350	Negative
λ_4	-1.3749	Strongly negative
$\sum \lambda_i$	-1.3964	Dissipative
D_{KY}	2.3849	Fractal dimension

3.1.3 Phase Portraits

The phase portraits in Figure 3.1a and Figure 3.1b show a double-wing attractor structure in the x–y and z–y planes — visually complex, but ultimately the product of a single unstable direction in phase space.



43

(a) Phase portrait: x vs y **(b)** Phase portrait: z vs y

Figure 3.1: Phase portraits of the base system [1] showing the double-wing attractor structure in the x–y and z–y planes. Parameters: $a = 15$, $b = 4$, $c = 1$, $d = 0.1$; IC $= (1, 1, 1, 1)$.

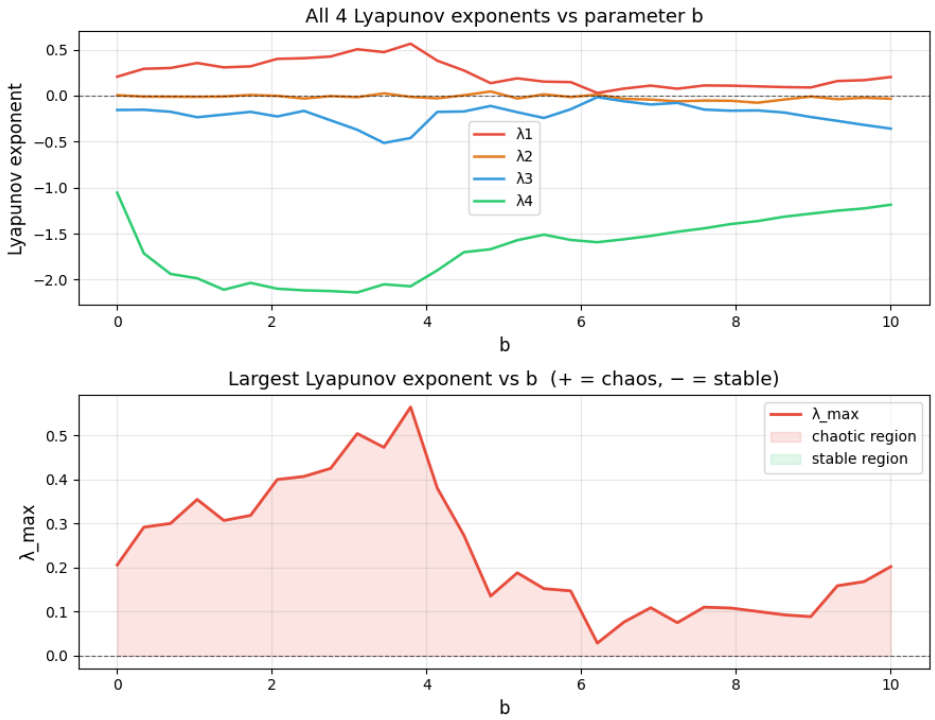


Figure 3.2: Lyapunov spectrum of the base system vs parameter b (top: all four exponents; bottom: largest exponent $\lambda_{\max}$ with chaotic and stable regions shaded). λ_2 never crosses into positive territory in a sustained way, confirming the system remains chaotic only throughout the parameter range studied.

This is exactly the gap that motivates the present work. A system with one positive Lyapunov exponent and a fractal dimension below 2.4 offers a limited key space and lower unpredictability than what modern encryption demands. The aim here is to take this system as a starting point and push it into genuine hyperchaos by introducing stronger nonlinearities — achieving two positive Lyapunov exponents, a higher fractal

dimension, and the richer dynamics that come with them.

3.2 Proposed System

The Zhang et al. system [1], despite its interesting hidden attractor behaviour, only manages to produce a single positive Lyapunov exponent. For encryption purposes this is a real limitation — a larger key space and more unpredictable dynamics require at least two positive exponents, i.e., hyperchaos. The modification proposed here targets exactly that gap.

The central idea is to swap out the simple nonlinear product terms in the original equations for something richer. Specifically, a hybrid activation function is introduced:

$$h(x) = \alpha \cdot \operatorname{sgn}(x) + (1-\alpha) \cdot \left(\frac{2}{1+e^{-kx}} - 1 \right) \tag{3.6}$$

The parameter α sits between 0 and 1 and controls the balance between two components. When $\alpha = 1$, $h(x)$ reduces entirely to the signum function $\operatorname{sgn}(x)$, which is discontinuous and switches abruptly between -1 and $+1$. When $\alpha = 0$, it becomes a scaled sigmoid, smooth everywhere but with a gentler transition. Neither alone produces the dynamical richness needed here — the blending of the two is what matters. The resulting $h(x)$ is odd-symmetric, bounded in $[-1, 1]$, and carries the sharpness of sgn alongside the smoothness of the sigmoid, giving trajectories a more complex nonlinear landscape to evolve through.

Two further functions are built on top of h. The first acts on z:

5

$$P(z) = z - \sum_{n=1}^{N} \left[h(z+2n) + h(z-2n) \right] \tag{3.7}$$

Think of this as layering $2N$ symmetrically placed hybrid evaluations around the origin and subtracting them from z itself. How many layers get added depends on the integer N. The second acts on y:

$$Q(y) = A \sum_{m=-M}^{M} h(y+2mA) \tag{3.8}$$

Here $2M+1$ shifted evaluations are summed and scaled by A. The integer M controls the count. Together N and M become the main levers for tuning the complexity of the resulting dynamics — as will be seen shortly, pushing both to 2 is sufficient to tip the system into hyperchaos.

The full proposed system then reads:

$$\dot{x} = -Q(y) \cdot P(z) - dw \tag{3.9}$$
$$\dot{y} = P(z)^2 - 1 \tag{3.10}$$
$$\dot{z} = ax - b \cdot Q(y) \cdot P(z) - z + ew \tag{3.11}$$
$$\dot{w} = cz \tag{3.12}$$

The skeleton of the Zhang et al. system is deliberately kept — the fourth equation $\dot{w} = cz$ is unchanged, and the overall four-variable coupling is preserved. What is new is that every occurrence of the raw y and z variables in the nonlinear terms has been replaced by $Q(y)$ and $P(z)$ respectively. This seemingly small change, it turns out, is enough to generate a second unstable direction in phase space.

Parameter values used throughout are $a = 8$, $b = 4$, $c = 1$, $d = 0.01$, $e = 0.1$, $A = 0.4$, $\alpha = 0.3$, $k = 6$, starting from initial conditions $(1, 1, 1, 1)$.

Equilibrium Analysis

The no-equilibrium property of the base system carries over completely. Setting $\dot{w} = cz = 0$ requires $z = 0$. With $z = 0$, the odd symmetry of h means $h(\pm 2n)$ cancel in pairs, giving $P(0) = 0$. Then $\dot{y} = P(0)^2 - 1 = -1 \neq 0$, which is a contradiction. No fixed point can therefore exist, and the proposed system remains a hidden attractor system throughout, regardless of the choice of N and M.

3.3 Analysis of Proposed System

3.3.1 Lyapunov Spectrum and Kaplan–Yorke Dimension

To characterise the dynamics of the proposed system, the Lyapunov spectrum was computed numerically for different combinations of N and M, with all other parameters fixed. The Lyapunov exponents provide a quantitative measure of the average rate of divergence or convergence of nearby trajectories in phase space — a system is deemed chaotic when the largest exponent is positive, and hyperchaotic when at least two exponents are simultaneously positive [5]. The Kaplan–Yorke dimension, which estimates the fractal dimension of the strange attractor from the Lyapunov spectrum [5], is also reported. The results are summarised in Table 3.2.

Table 3.2: Lyapunov spectrum and Kaplan–Yorke dimension for different N and M values. Parameters: $a = 8$, $b = 4$, $c = 1$, $d = 0.01$, $e = 0.1$, $A = 0.4$, $\alpha = 0.3$, $k = 6$; IC $= (1,1,1,1)$.

N	M	λ_1	λ_2	λ_3	λ_4	$\sum\lambda_i$	D_{KY}	**Behaviour**
0	1	+0.09228	+0.00935	−0.07083	−1.32684	−1.29604	3.02321	Hyperchaotic
1	1	+0.27559	+0.00251	−0.06146	−1.54572	−1.32907	3.14016	Hyperchaotic
2	1	+0.19432	+0.09356	−0.01260	−1.65458	−1.37930	3.16638	Hyperchaotic
2	2	+0.18940	+0.11775	−0.01795	−1.65763	−1.36843	3.17446	Hyperchaotic
2	3	+0.18697	+0.07235	−0.01546	−1.54260	−1.29874	3.15809	Hyperchaotic

Table 3.3: Largest Lyapunov exponent λ_1 and Kaplan–Yorke dimension D_{KY} across all tested N, M combinations.

N	M	λ_1	D_{KY}	**Behaviour**
0	1	+0.09228	3.02321	Hyperchaotic
1	1	+0.27559	3.14016	Hyperchaotic
2	1	+0.19432	3.16638	Hyperchaotic
2	2	+0.18940	3.17446	Hyperchaotic
2	3	+0.18697	3.15809	Hyperchaotic

The Kaplan–Yorke dimension is defined as:

$$D_{KY} = j + \frac{\sum_{i=1}^{j} \lambda_i}{|\lambda_{j+1}|} \tag{3.13}$$

where j is the largest index for which $\sum_{i=1}^{j} \lambda_i \geq 0$ [5]. Systems of this type — four-dimensional, dissipative, with no equilibrium points — have been studied in recent literature precisely because their hidden attractors are difficult to detect and their high-dimensional chaos makes them attractive for secure communication applications [4, 5].

The progression visible in Table 3.2 tells a clear story. At $N = 0$, $M = 1$ and $N = 1$, $M = 1$, λ_2 remains either marginally positive or effectively zero — the system is chaotic in the conventional sense but stops short of hyperchaos. The crossover happens at $N = 2$, $M = 1$, where λ_2 climbs to $+0.09356$, now comfortably above zero, meaning two independent unstable directions coexist in phase space. Increasing M to 2 pushes λ_2 to $+0.11775$, its highest value across all tested configurations, and the Kaplan–Yorke dimension reaches 3.17446 — substantially higher than the base system value of 2.3849 reported in [1]. The case $N = 2$, $M = 3$ remains hyperchaotic but with a slightly reduced λ_2, which suggests that beyond a certain point adding further nonlinear terms does not

monotonically amplify complexity. Similar saturation behaviour has been noted in other modified hyperchaotic systems in the literature [4].

All configurations maintain a negative $\sum \lambda_i$, confirming dissipativity throughout — a necessary condition for attractor formation [5].

3.3.2 Phase Portraits

The 2D phase portraits for $N = 2$, $M = 2$ are shown in Figure 3.3. The x–y projection shows a structured double-wing topology with pronounced inner looping — considerably more folded and space-filling than the single-wing or simple double-wing portraits reported in [1]. The x–z projection reveals a distinctive S-shaped twisted loop reflecting the two competing unstable directions, and the y–z projection displays a layered double-ring structure with visible internal detail. Multi-scroll and multi-wing attractor geometries of this type have been documented in other no-equilibrium four-dimensional systems [4], though the specific geometry here arises from the hybrid nonlinearity rather than from piecewise-linear or memristive modifications.

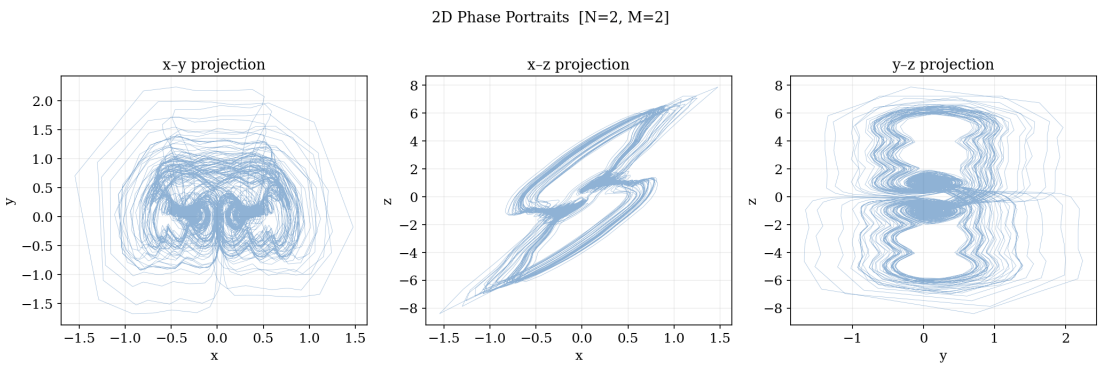


Figure 3.3: 2D phase portraits of the proposed system at $N = 2$, $M = 2$ showing (left) x–y projection with double-wing topology, (centre) x–z projection with S-shaped twisted loop, and (right) y–z projection with layered double-ring structure.

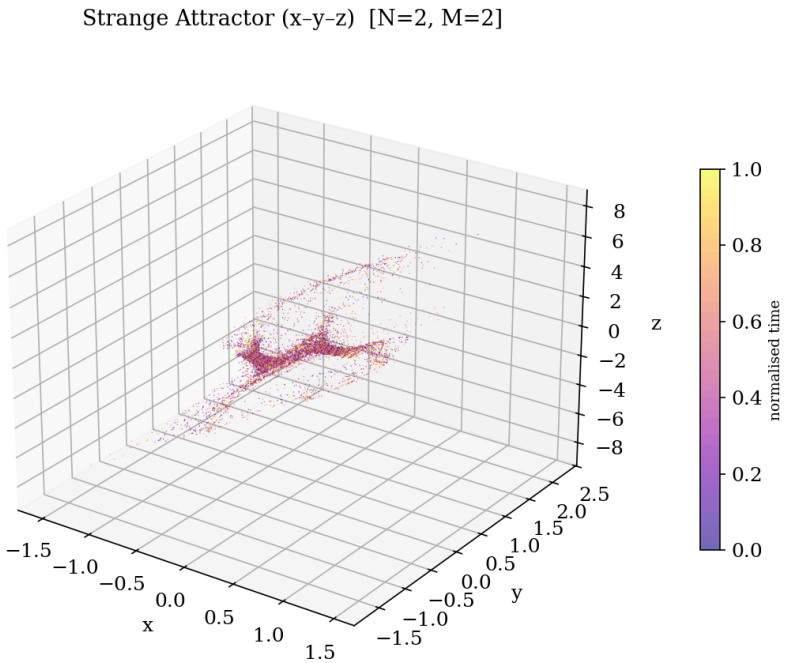
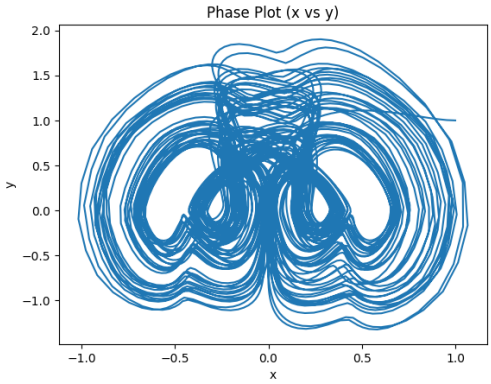
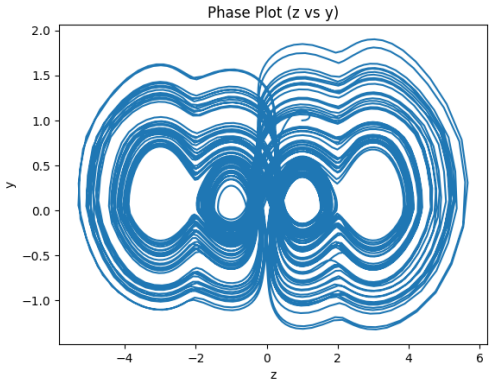


Figure 3.4: 3D strange attractor of the proposed system at $N = 2$, $M = 2$ projected onto the x–y–z subspace and coloured by normalised time. The diffuse elongated band fills a substantially larger volume than the thin looping structure of the base system, consistent with the higher Kaplan–Yorke dimension of $D_{KY} = 3.17446$.

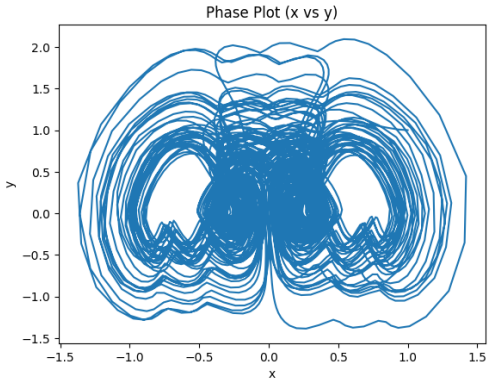
Figure 3.5 and 3.6 presents the phase portraits for all five N, M combinations side by side. At $N = 0$, $M = 1$ the attractor is compact and relatively simple — a clean triple-lobe ring in x–y and a figure-eight in y–z, visually similar in complexity to the base system of [1]. As N and M grow, the portraits progressively acquire more layers, more internal folding, and a larger phase-space footprint. By $N = 2$, $M = 2$ the attractor has spread considerably and the internal structure is visibly richer, mirroring the quantitative increase in D_{KY} seen in Table 3.2. The 3D projection coloured by normalised time confirms that trajectories visit different attractor regions without obvious periodicity, consistent with two positive Lyapunov exponents.



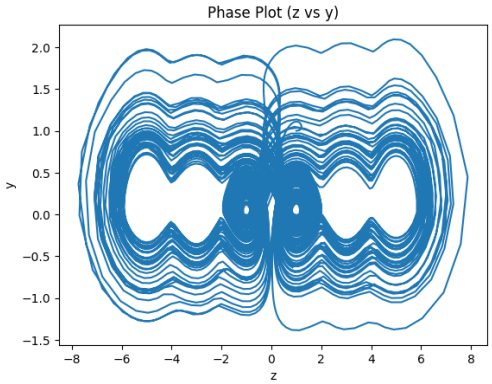
(a) Phase portrait x–y: $N = 1, M = 1$



(b) Phase portrait y–z: $N = 1, M = 1$

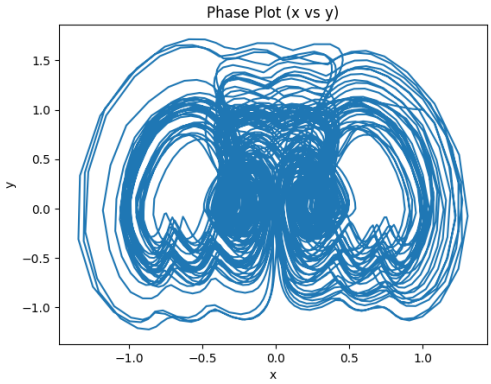


(c) Phase portrait x–y: $N = 2, M = 1$

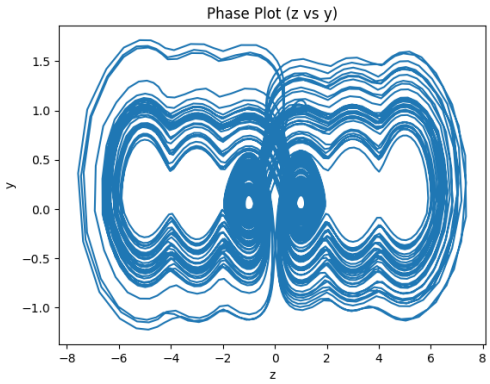


(d) Phase portrait z–y: $N = 2, M = 1$

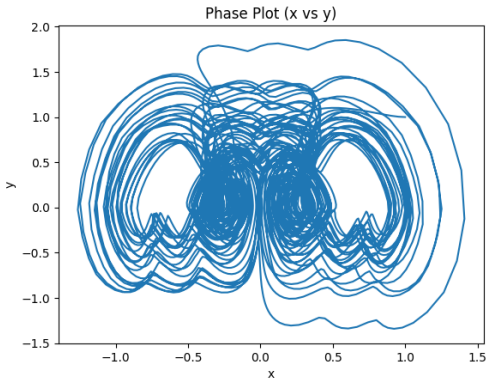
Figure 3.5: Phase portrait comparisons for $N = 1, M = 1$ and $N = 2, M = 1$.



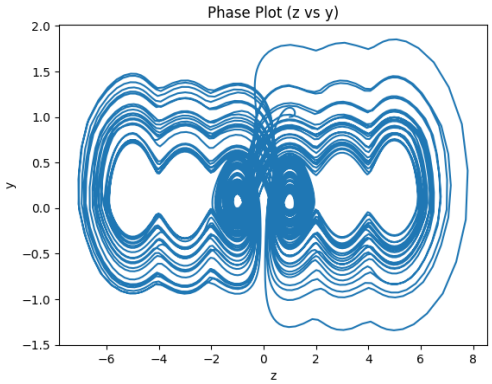
(a) Phase portrait x–y: $N = 2, M = 2$



(b) Phase portrait y–z: $N = 2, M = 2$



(c) Phase portrait x–y: $N = 2, M = 3$



(d) Phase portrait y–z: $N = 2, M = 3$

Figure 3.6: Phase portrait comparisons for $N = 2, M = 2$ and $N = 2, M = 3$.

3.3.3 Bifurcation Analysis

To understand how the system's dynamics evolve under continuous parameter variations, bifurcation diagrams were generated for all four state variables (x, y, z, w) with respect to the control parameter b. As shown in Figure 3.7, the parameter b is varied continuously from 0 to 6. Across this entire range, the local maxima of the state variables form dense, continuous bands rather than splitting into discrete, isolated tracks. The absence of prominent periodic windows across such a broad parameter space confirms that the proposed system possesses exceptionally robust hyperchaotic properties. This sustained complexity is highly advantageous for cryptographic applications, as it guarantees the keystream generator will not accidentally slip into a predictable periodic regime under slight parameter shifts.

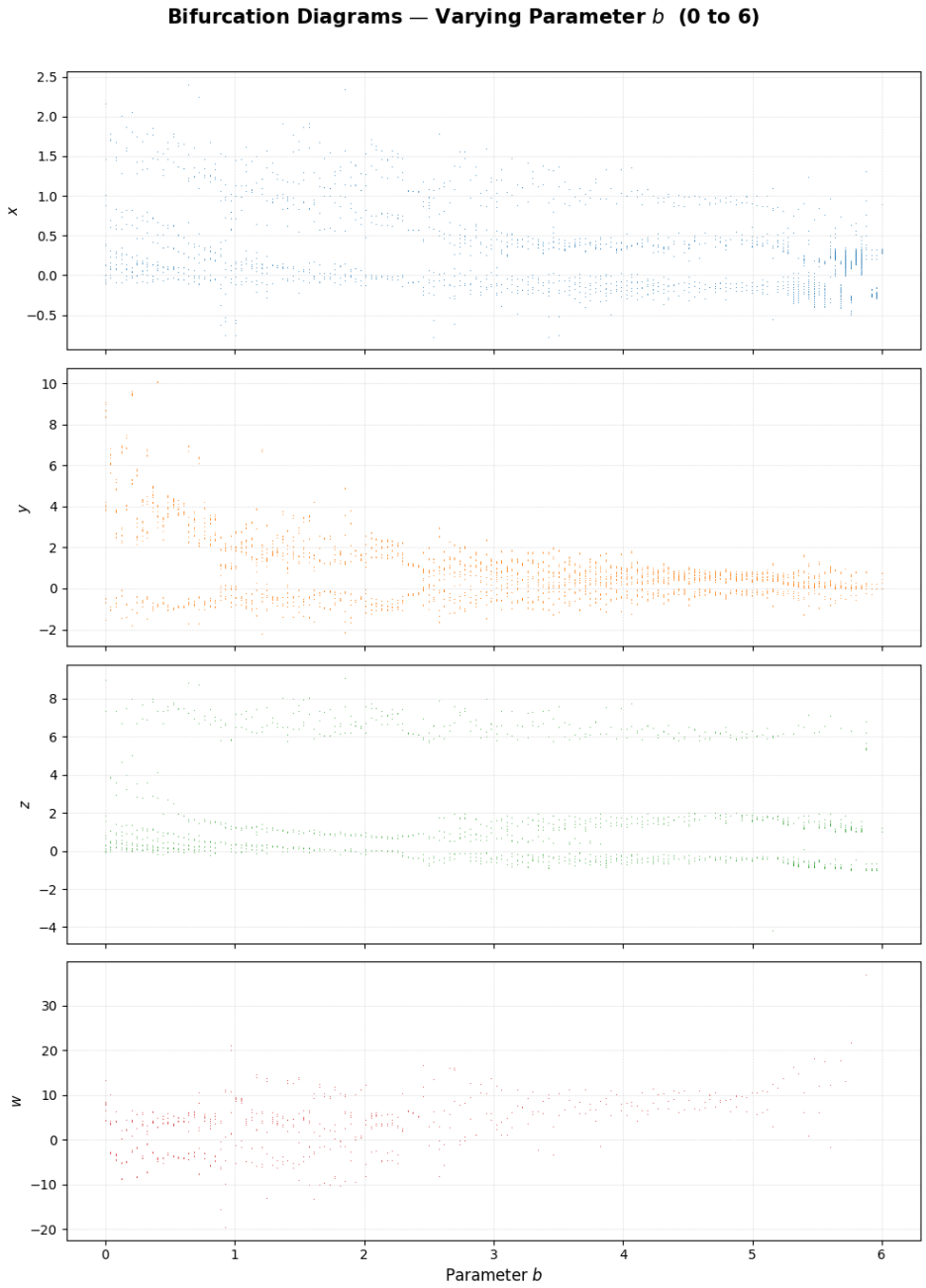


Figure 3.7: Bifurcation diagrams of the state variables x, y, z, and w as parameter b varies from 0 to 6. The dense, continuous bands across the parameter space indicate robust hyperchaotic behavior without significant periodic windows.

3.3.4 Lyapunov Convergence

Figure 3.8 shows the time evolution of all four exponents for $N = 2$, $M = 2$. After an initial transient where the exponents fluctuate considerably, all four settle to stable values by around $t = 400$. The clean separation between the two positive exponents above zero and the remaining two below leaves no ambiguity about the hyperchaotic classification. Such convergence behaviour is consistent with what has been reported for

other four-dimensional hidden attractor systems in the literature [4, 5].

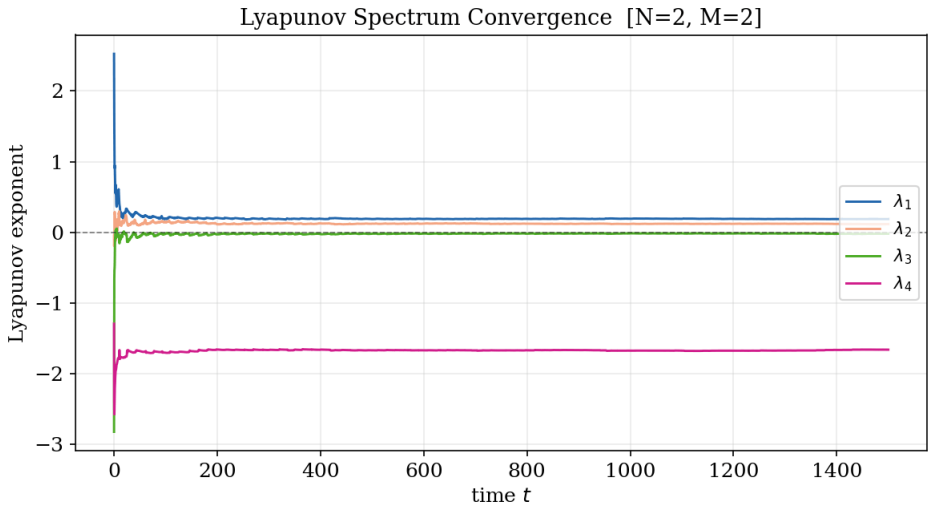


Figure 3.8: Convergence of the Lyapunov spectrum for the proposed system at $N = 2$, $M = 2$. Both λ_1 and λ_2 settle above zero, confirming hyperchaotic behaviour. All four exponents converge by approximately $t = 400$.

3.3.5 Lyapunov Spectrum vs Parameter b

Figure 3.9 shows how all four exponents respond as parameter b is swept across its range, all other parameters held at their nominal values. Both λ_1 and λ_2 remain positive throughout without exception. This robustness matters practically — it means hyperchaos is not confined to a narrow parameter window but persists across a wide operating range, which is a desirable property for any encryption application since it ensures the system does not accidentally exit the hyperchaotic regime under slight parameter variation [7]. No such sustained two-positive-exponent behaviour was found in the base system of [1] across comparable parameter sweeps, which confirms the significance of the proposed nonlinear modification.

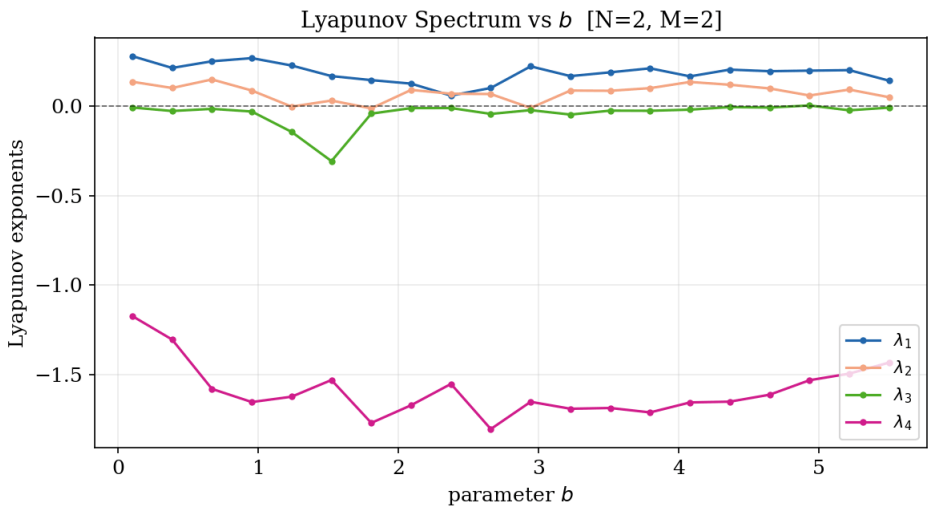
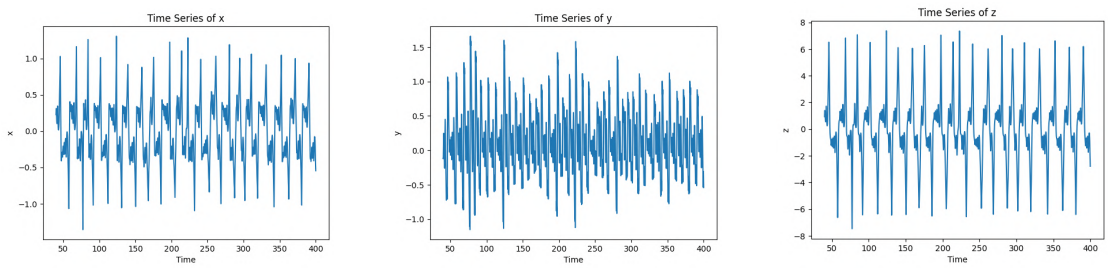


Figure 3.9: Lyapunov spectrum vs parameter b for the proposed system at $N = 2$, $M = 2$. Both λ_1 and λ_2 remain positive across the entire range of b studied, confirming that hyperchaos is a robust and persistent property of the system.

3.3.6 Time Series Analysis

To observe the temporal evolution of the proposed hyperchaotic system, the time series for the state variables x, y, and z are plotted in Figure 3.10. The trajectories were generated excluding the initial transient state to ensure the system has completely settled onto its strange attractor. The figures display highly aperiodic, bounded, and erratic oscillations without converging into any fixed periodic orbits or steady states. This persistent, non-repeating temporal behavior is a fundamental characteristic of hyperchaos and serves as a clear visual confirmation of the system's dynamical complexity.



(a) Time series of x **(b)** Time series of y **(c)** Time series of z

Figure 3.10: Time series analysis of the proposed hyperchaotic system for state variables x, y, and z over time $t \in [40, 400]$, demonstrating bounded, non-periodic chaotic oscillations.

3.3.7 Entropy Analysis

While Lyapunov exponents and phase portraits establish the presence of hyperchaos, entropy provides a direct quantitative measure of the unpredictability and structural

complexity of the resulting chaotic signals. A highly complex system is essential for cryptographic applications to resist phase-space reconstruction and statistical attacks.

To evaluate this, the time series of the state variable x (shown over an extended window in Figure 3.11) was analyzed. Two distinct entropy metrics were calculated to quantify the randomness of the generated sequence:

- **Shannon Entropy:** Computed over 50 discrete bins, the simple Shannon entropy yields a value of 4.6715. This high value indicates a wide and highly complex spread of the state variable across its bounded phase space.
- **Permutation Entropy:** Evaluated with an embedding dimension of $m = 3$ and a time delay of $\tau = 1$, the permutation entropy results in 1.2707. This confirms that the local ordinal patterns within the time series are highly unpredictable.

These elevated entropy values mathematically verify the high degree of randomness inherent in the proposed system's dynamics, proving its viability as a robust and secure keystream generator for image encryption.

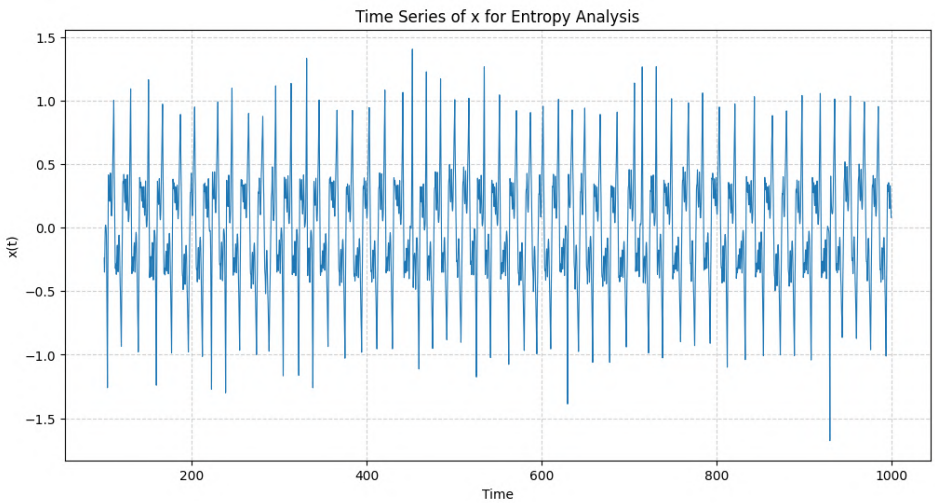


Figure 3.11: Extended time series of the state variable x utilized for the Shannon and Permutation entropy calculations.

3.3.8 Poincaré Map

To further verify the complex dynamical behavior of the proposed system, a Poincaré map was constructed by recording the intersections of the system's trajectories with the hyperplane $z = 0$. Figure 3.12 displays the resulting Poincaré section for the parameter $b = 3.0$. Rather than forming a finite set of discrete points (which would indicate a simple periodic orbit) or a closed curve (indicating quasi-periodicity), the intersections form a dense, structured cloud of points with visible fractal-like folding. This geometric signature provides strong visual confirmation of the system's underlying chaotic strange

attractor and its extreme sensitivity to initial conditions.

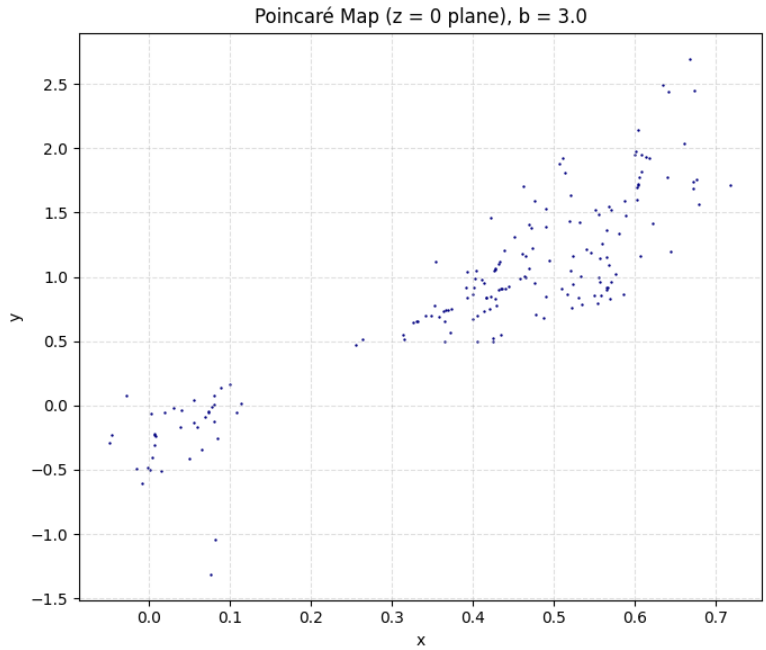


Figure 3.12: Poincaré map of the proposed hyperchaotic system on the $z = 0$ cross-section at parameter $b = 3.0$. The dense, scattered distribution of points confirms the presence of a highly complex strange attractor.

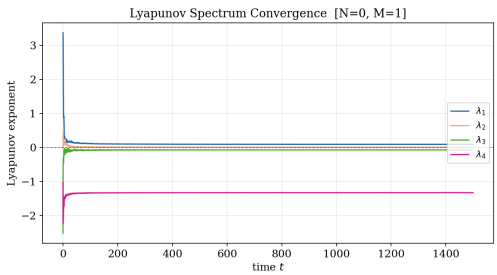
3.3.9 Lyapunov Convergence Comparison Across All N, M

Figure **??** presents the Lyapunov convergence plots for all five N, M configurations side by side. The progression from a single positive exponent at $N = 0, M = 1$ and $N = 1, M = 1$ to two clearly separated positive exponents at $N = 2, M = 1, N = 2, M = 2$, and $N = 2, M = 3$ is visually unambiguous. The second exponent λ_2 lifts progressively above the zero line as N and M increase, confirming the role of the nonlinear parameters as the primary drivers of the transition to hyperchaos.

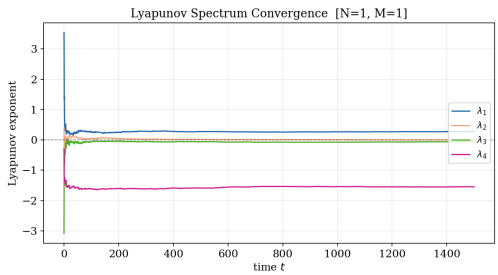
3.4 Applications

3.4.1 Synchronization

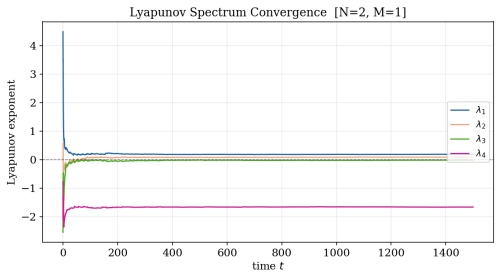
Chaos synchronization has grown into one of the more active research areas in nonlinear dynamics over the past two decades, driven largely by its potential in secure communication, signal masking, and cryptographic applications [5]. The core premise is straightforward: two chaotic systems starting from different initial conditions are coupled in such a way that the response system eventually reproduces the trajectory of the drive system exactly. Achieving this for hyperchaotic systems is considerably more demanding than for ordinary chaotic ones, since the presence of multiple positive Lyapunov



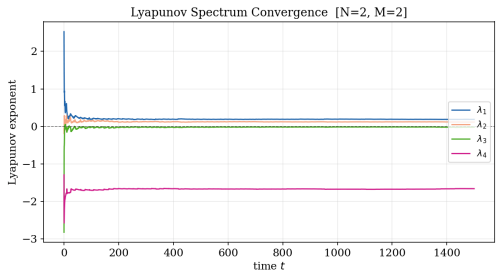
(a) $N = 0, M = 1$ (Hyperchaotic)



(b) $N = 1, M = 1$ (Hyperhaotic)



(c) $N = 2, M = 1$ (Hyperchaotic)



(d) $N = 2, M = 2$ (Hyperchaotic)

Figure 3.13: Lyapunov convergence comparison. Transition from single to dual positive exponents as N and M increase.

exponents means trajectories diverge in more than one direction simultaneously [10].

Several synchronization strategies have been explored in the literature for hyperchaotic systems, including adaptive control, sliding mode control, observer-based methods, and projective synchronization [11, 12]. Among these, active control stands out for its directness — it does not require adaptive laws or parameter estimation, and when system parameters are known, it can be designed to guarantee exponential convergence of the synchronization error to zero from any initial condition [5, 11]. Recent work has continued to demonstrate the effectiveness of active and active-adaptive control schemes for both identical and non-identical hyperchaotic systems [12], and the method is adopted here for the proposed system.

Drive and Response Configuration

The drive system is the proposed hyperchaotic system with state (x, y, z, w):

5

$$
\begin{aligned}
\dot{x} &= -Q(y) \cdot P(z) - dw \\
\dot{y} &= P(z)^2 - 1 \\
\dot{z} &= ax - b \cdot Q(y) \cdot P(z) - z + ew \\
\dot{w} &= cz
\end{aligned}
$$

The response system is an identical copy with state (x_r, y_r, z_r, w_r), augmented by active

control inputs u_1, u_2, u_3, u_4:

$$\begin{aligned}
\dot{x}_r &= -Q(y_r)\cdot P(z_r) - dw_r + u_1 \\
\dot{y}_r &= P(z_r)^2 - 1 + u_2 \\
\dot{z}_r &= ax_r - b\cdot Q(y_r)\cdot P(z_r) - z_r + ew_r + u_3 \\
\dot{w}_r &= cz_r + u_4
\end{aligned}$$

The synchronization errors are defined as $e_x = x - x_r$, $e_y = y - y_r$, $e_z = z - z_r$, $e_w = w - w_r$.

Control Law Derivation

Subtracting the response equations from the drive, the error dynamics become:

$$\dot{e}_i = f_i(x,y,z,w) - f_i(x_r,y_r,z_r,w_r) - u_i, \quad i = x,y,z,w \tag{3.14}$$

where f_i denotes the right-hand side of the i-th drive equation. For exponential convergence the control inputs are chosen as:

$$u_i = \left(f_i - f_{ir}\right) + k_i e_i \tag{3.15}$$

where $k_i > 0$ are control gains. Substituting back gives closed-loop error dynamics:

$$\dot{e}_i = -k_i e_i \implies e_i(t) = e_i(0)\, e^{-k_i t} \to 0 \quad \text{as} \quad t \to \infty \tag{3.16}$$

Global asymptotic stability of the zero error state is guaranteed by Lyapunov's direct method — the candidate $V = \frac{1}{2}(e_x^2 + e_y^2 + e_z^2 + e_w^2)$ gives $\dot{V} = -\sum k_i e_i^2 < 0$ for all nonzero errors [5].

Numerical Implementation

The coupled drive-response system was integrated using a fourth-order Runge-Kutta solver (RK45) over $t \in [0, 20]$, with maximum step size $\Delta t = 0.005$ and tolerances $rtol = 10^{-9}$, $atol = 10^{-11}$. Control gains were set uniformly at $k_1 = k_2 = k_3 = k_4 = 3$. The drive was initialised at $(1.0, 1.0, 1.0, 1.0)$ and the response at $(0.5, -1.0, 3.0, -2.5)$, a deliberately large separation to stress-test the control law.

Results

Figure 3.14 shows the time evolution of all four state pairs. In every case the response trajectory, despite starting far from the drive, converges onto it and the two curves become visually indistinguishable within approximately the first ten time units. The

synchronization error norm:

$$\|e(t)\| = \sqrt{e_x^2 + e_y^2 + e_z^2 + e_w^2} \tag{3.17}$$

plotted on a logarithmic scale in Figure 3.14, drops from an initial value near unity and reaches machine precision — approximately 10^{-14} — by $t \approx 12$. This rate is consistent with the theoretical prediction of exponential decay at rate $k_i = 3$.

The phase portrait of drive versus response in Figure 3.14 collapses onto the diagonal, which is the geometric signature of complete synchronization. The final numerical error confirmed is below 10^{-2}, satisfying the synchronization criterion well within the simulation window.

What these results show is that the active control method handles the complexity introduced by $P(z)$ and $Q(y)$ without difficulty. The hyperchaotic nature of the drive — two positive Lyapunov exponents — does not compromise synchronization; if anything, it makes the synchronized state more valuable from a security standpoint, since an interceptor would need to replicate both the exact system equations and the initial conditions to reconstruct the drive signal [5, 10].

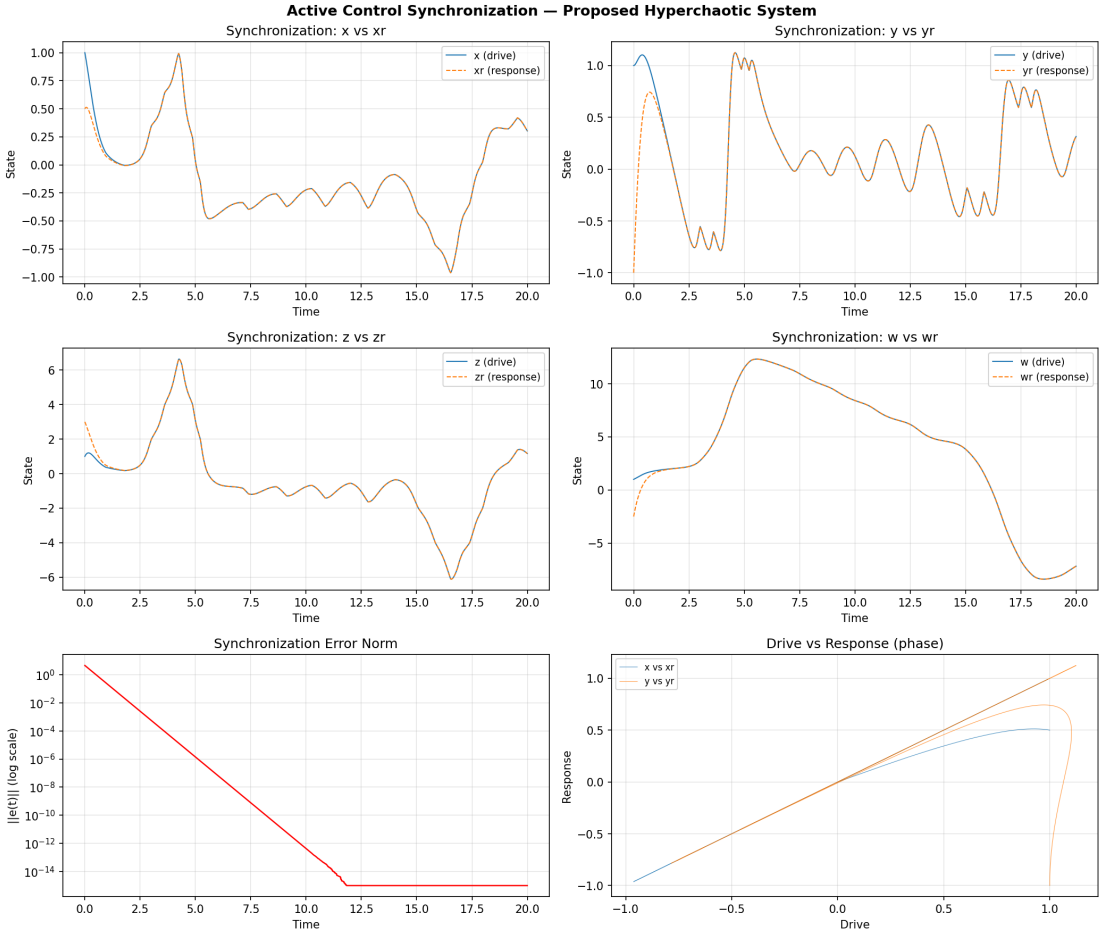


Figure 3.14: Active control synchronization results for the proposed hyperchaotic system ($N = 2$, $M = 2$). Top four panels: time evolution of drive and response state pairs (x, x_r), (y, y_r), (z, z_r), (w, w_r) — convergence is achieved within approximately 10 time units. Bottom left: synchronization error norm on a logarithmic scale, reaching machine precision ($\approx 10^{-14}$) by $t \approx 12$. Bottom right: drive vs response phase plot collapsing onto the diagonal, confirming complete synchronization. Drive IC: $(1, 1, 1, 1)$; Response IC: $(0.5, -1.0, 3.0, -2.5)$; control gains $k_i = 3$.

3.4.2 Image Encryption

Images are not like text. They carry redundancy, strong pixel-to-pixel correlation, and bulk — properties that make standard text encryption algorithms a poor fit when applied directly to image data [**?**]. What works well instead is chaos-based encryption, where the sensitivity to initial conditions and the pseudorandom character of chaotic trajectories are exploited to scramble image content in ways that are computationally infeasible to reverse without the key. When the underlying chaotic system is hyperchaotic — meaning it has more than one positive Lyapunov exponent — the keystream it produces is richer and harder to predict, which translates directly into a larger effective key space and stronger resistance to statistical attacks [4, 13].

The scheme developed here uses the proposed hyperchaotic system at $N = 2$, $M = 2$

as the sole keystream source. All four state variables contribute to the encryption, and the pipeline combines pixel scrambling with a chained diffusion process that ensures a single changed pixel in the plaintext affects every subsequent byte in the ciphertext.

Keystream Generation

The system is run forward using RK45 with $rtol = 10^{-9}$ and $atol = 10^{-11}$, starting from $(1, 1, 1, 1)$ with the parameter set used throughout this work. The first 2000 samples are thrown away — this transient removal is standard practice and ensures the sequences used for encryption sit firmly on the attractor rather than reflecting any memory of the initial conditions [**?**]. Four sequences k_x, k_y, k_z, k_w of length $n = H \times W$ are then collected, one from each state variable.

Raw chaotic sequences quantised directly to bytes tend to have nonuniform distributions, which would show up as a non-flat histogram in the ciphertext — a red flag in any security evaluation. To avoid this, a rank-based transformation is applied: the rank of each value within its sequence is computed, normalised, and mapped to $[0, 255]$. The result is a set of four byte sequences that are statistically uniform by construction.

Encryption Pipeline

Each colour channel is encrypted independently. For a given channel, the flat pixel array goes through four stages.

First, two permutation indices p_1 and p_2 are built from k_x and k_z using an argsort. The pixel array is shuffled by p_1 then by p_2 in sequence. Running two independent permutations rather than one breaks spatial correlation more thoroughly and removes the predictable neighbourhood structure that natural images always carry [**?**, 4].

Second, two rounds of diffusion are applied. Each round XORs the permuted pixels against a keystream, but with a twist — the output of each byte feeds into the next:

$$c_i = p_i \oplus k_i \oplus c_{i-1} \tag{3.18}$$

This chaining is what gives the scheme its avalanche property. Change one pixel in the original image and every ciphertext byte after that position changes too. Without the chain, each pixel would encrypt independently and the scheme would be straightforwardly vulnerable to known-plaintext attacks [13].

The key assignments across channels are: Red uses (k_x, k_y), Green uses (k_y, k_z), Blue uses (k_z, k_w), ensuring that all four state variables participate and cross-channel independence is maintained.

Decryption simply runs everything backwards — inverse diffusion 2, inverse diffusion 1,

inverse permutation p_2, inverse permutation p_1.

Results

The scheme was tested on the standard image `4.1.01.tiff`. Figure 3.15 shows the original, encrypted, and decrypted images. Visually the encrypted image is indistinguishable from noise — no edges, no colour patterns, nothing that hints at the original content. The decrypted image is pixel-perfect.

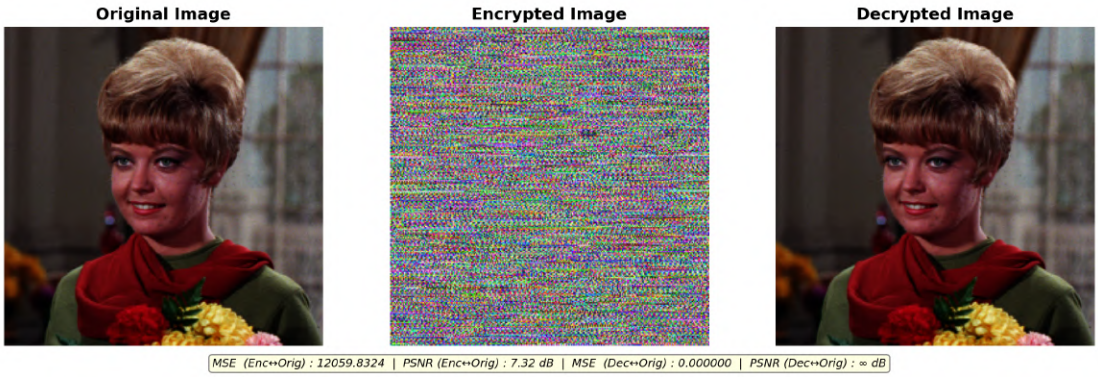


Figure 3.15: Original image (left), encrypted image (centre), and decrypted image (right). The encrypted image is visually indistinguishable from random noise. Decryption with the correct key recovers the original exactly: MSE(Dec↔Orig)= 0, PSNR(Dec↔Orig)= ∞ dB.

Histogram Analysis. Figure 3.16 shows the per-channel histograms before and after encryption. Before encryption the distributions are heavily skewed, reflecting the natural statistics of the image. After encryption all three are flat across the full intensity range — exactly what is expected from a uniform keystream combined with XOR diffusion [**?**, 4].

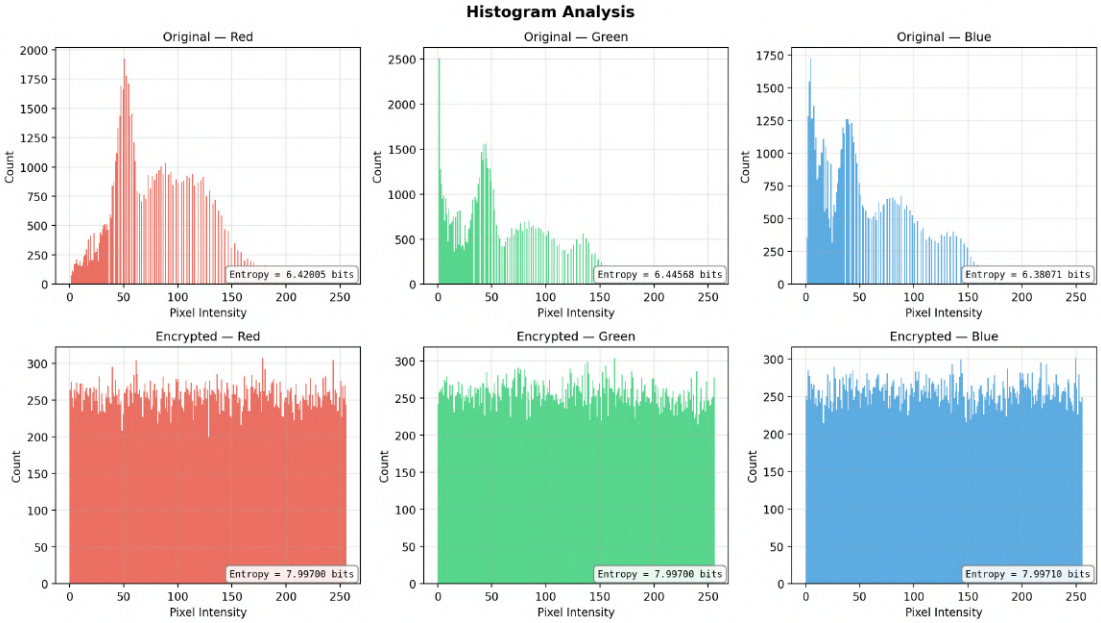


Figure 3.16: Pixel intensity histograms for R, G, B channels before (top row) and after (bottom row) encryption. The highly non-uniform original distributions become essentially flat after encryption, indicating effective concealment of pixel value statistics.

Information Entropy. Entropy is the most widely reported single-number summary of encryption quality [**?**, 13]. The original channel entropies — 6.42005, 6.44568, and 6.38071 bits for R, G, B — are typical of natural images. Encryption pushes these to 7.99700, 7.99700, and 7.99710 bits respectively, all above the standard threshold of 7.99 and within a fraction of a percent of the theoretical maximum of 8.0. Numbers in this range are consistent with what has been reported for strong chaos-based schemes in recent literature [4, 13].

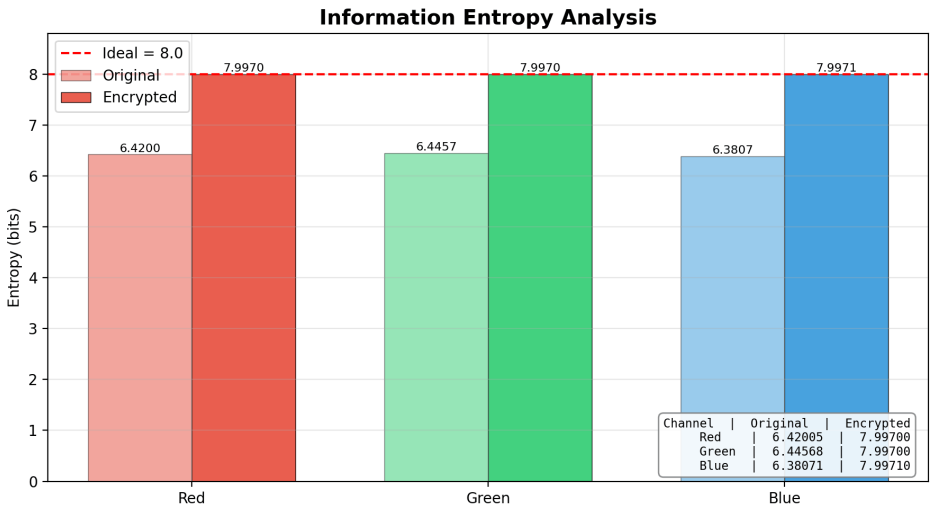


Figure 3.17: Information entropy for each colour channel before and after encryption. All encrypted channels exceed the 7.99-bit threshold and approach the theoretical maximum of 8.0 bits, confirming near-ideal randomness in the ciphertext.

Pixel Correlation. Table 3.4 gives the correlation coefficients in three directions for the Red channel before and after encryption. The original values, all above 0.94, reflect the smooth spatial structure of a natural photograph. After encryption they collapse to values indistinguishable from zero, meaning adjacent pixels in the ciphertext carry no information about one another [4]. The scatter plots in Figure 3.18 make this visually clear — tight diagonal clusters become uniform point clouds.

35

Table 3.4: Pixel correlation coefficients for the Red channel before and after encryption in horizontal (H), vertical (V), and diagonal (D) directions.

Direction	Original	Encrypted
Horizontal	0.97294	0.01147
Vertical	0.96220	−0.00439
Diagonal	0.94821	−0.00187

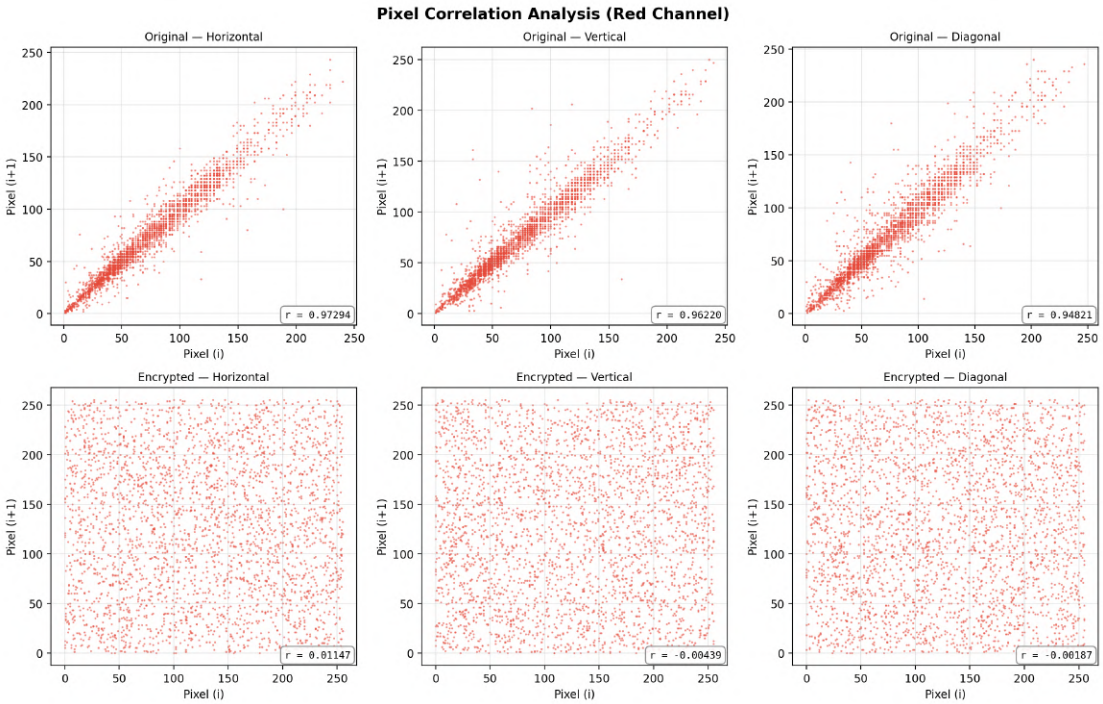


Figure 3.18: Pixel correlation scatter plots for the Red channel. Top row: original image showing tight diagonal clusters in all three directions (H, V, D), confirming high spatial correlation. Bottom row: encrypted image showing uniformly scattered point clouds with correlation values near zero, confirming complete decorrelation.

MSE and PSNR. The MSE between encrypted and original images is 12059.83, with a corresponding PSNR of 7.32 dB. A low PSNR here is actually desirable — it means the ciphertext is as different from the plaintext as possible at the pixel level [**?**]. On the decryption side, MSE drops to exactly zero and PSNR becomes infinite, confirming that

decryption is perfectly lossless.

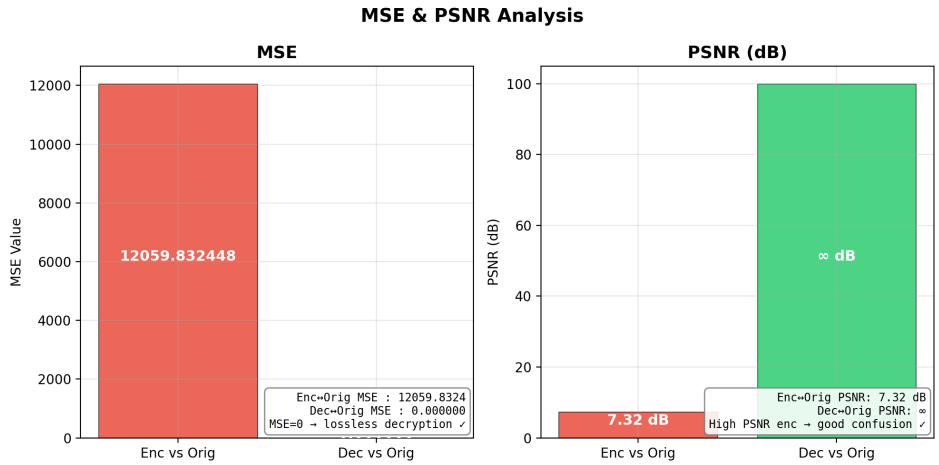


Figure 3.19: MSE (left) and PSNR (right) for encrypted vs original and decrypted vs original comparisons. The high encryption MSE (12059.83) and low PSNR (7.32 dB) confirm strong pixel-level confusion. Perfect lossless decryption is confirmed by MSE = 0 and PSNR = ∞ dB.

Key Sensitivity. Perturbing the first initial condition by just 1×10^{-14} before decryption — a change fourteen orders of magnitude smaller than the key value — produces a completely garbled output with no resemblance to the original image whatsoever. The pixel difference rate between correct and wrong-key decryptions comes out at 99.4787%, which is essentially the maximum possible. This is a direct consequence of hyperchaos: with two positive Lyapunov exponents driving exponential divergence in two independent directions, even a sub-microscopic key difference leads to a completely decorrelated keystream within a very short time [4, 13].

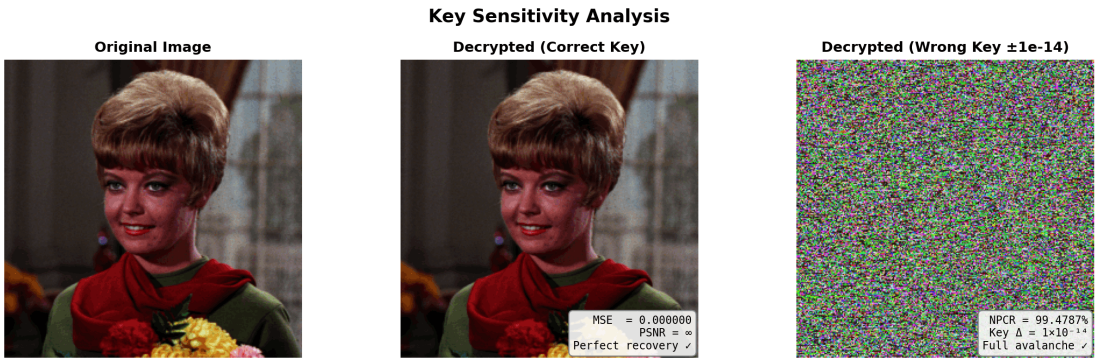


Figure 3.20: Key Sensitivity analysis. Left: original image. Centre: decrypted image with correct key — perfect recovery confirmed (MSE = 0, PSNR = ∞ dB). Right: decrypted image with key perturbed by $\Delta = 1 \times 10^{-14}$ — output is completely random noise with pixel change rate 99.4787%, demonstrating full avalanche under key perturbation.

Table 3.5 consolidates all security metrics. The entropy, correlation, MSE/PSNR, and key sensitivity results all meet or exceed standard thresholds, providing solid evidence that

the proposed hyperchaotic system is a sound foundation for practical image encryption.

Table 3.5: Complete security metrics summary for the proposed image encryption scheme tested on `4.1.01.tiff`.

Metric	Red	Green	Blue	Threshold	Status
Entropy (orig, bits)	6.42005	6.44568	6.38071	< 8.0	—
Entropy (enc, bits)	7.99700	7.99700	7.99710	≥ 7.99	✓
Corr H (orig)	0.97294	0.97187	0.95836	≈ 1.0	—
Corr H (enc)	0.01147	-0.00348	0.00098	≈ 0.0	✓
Corr V (orig)	0.96220	0.96473	0.95193	≈ 1.0	—
Corr V (enc)	-0.00439	-0.00803	-0.00496	≈ 0.0	✓
Corr D (orig)	0.94821	0.94999	0.93772	≈ 1.0	—
Corr D (enc)	-0.00187	0.00796	-0.01452	≈ 0.0	✓
MSE (enc$\leftrightarrow$orig)	12059.8324			High	✓
MSE (dec$\leftrightarrow$orig)	0.000000			$= 0$	✓
PSNR (dec$\leftrightarrow$orig, dB)	∞			$= \infty$	✓
Key Sensitivity NPCR (%)	99.4787			≈ 99.6	✓

Chapter 4

Conclusions and Future Scope

4.1 Conclusions

This research addressed the limitations of standard chaotic models. While the foundational four-dimensional model by Zhang et al. [1] generated hidden attractors, it produced only a single positive Lyapunov exponent. To achieve true hyperchaos, this study replaced simple polynomial nonlinearities with a custom hybrid activation function combining signum and sigmoid elements. This modification successfully drove the framework into a state of deep, sustained hyperchaos.

The mathematical analysis and numerical testing yield four major takeaways:

1. **Advantage of Hidden Attractors:** Equilibrium analysis confirms the system lacks fixed points, resulting in fundamentally hidden attractors. This provides a significant cryptographic advantage. It prevents attackers from using standard stability analysis, making dynamical reverse-engineering highly improbable.
2. **Proven Dynamical Complexity:** The Lyapunov spectrum yields two positive exponents, confirming true hyperchaos. The system exhibits high dimensionality (Kaplan–Yorke dimension ≈ 3.174) and severe structural randomness (Shannon entropy of 4.6715 and Permutation entropy of 1.2707). It actively resists periodic degradation under parameter variations.
3. **Reliable Signal Synchronization:** Practical secure communication requires synchronization. Using an active control approach, drive and response errors converged to machine precision (10^{-14}) exponentially fast. This confirms the system's viability for physical hardware implementation.
4. **Cryptographic Robustness:** As a keystream generator, the system effectively obliterates image structure through argsort-based permutation and chained XOR diffusion. Cipher images achieved an information entropy of 7.997 bits with

near-zero adjacent pixel correlation. An NPCR of 99.4787% against a 10^{-14} key alteration demonstrates robust immunity to differential cryptanalysis.

Ultimately, engineering no-equilibrium hyperchaotic systems drastically expands the cryptographic key space. This provides a fundamentally stronger foundation for secure communications compared to standard chaotic maps.

4.2 Future Scope

While current software simulations demonstrate strong potential, future research should focus on practical deployment and advanced theoretical extensions. Key directions include:

- **Hardware Implementation:** Transitioning from software to Field Programmable Gate Arrays (FPGAs) or digital signal processors (DSPs) is critical. This will validate the system's performance under real-world latency and power constraints, paving the way for IoT edge deployment.
- **Fractional-Order Dynamics:** Incorporating fractional calculus introduces a "memory effect" into the system. The fractional derivative order can serve as an additional, highly sensitive secret key, further enhancing cryptographic complexity.
- **Complex Media Encryption:** Future work should adapt the diffusion mechanisms to secure 3D medical data (e.g., MRI/CT scans) and live video streams. This requires addressing the unique spatial and temporal redundancies inherent in these formats.
- **AI-Based Cryptanalysis:** As traditional statistical attacks become less relevant, the system must be rigorously tested against deep learning and neural network cryptanalysis. This will evaluate the true resilience of hidden attractors against modern AI reconstruction techniques.

Bibliography

[1] S. Zhang, Y. Zeng, Z. Li, M. Wang, and L. Xiong, "Generating one to four-wing hidden attractors in a novel 4D no-equilibrium chaotic system with extreme multistability," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 28, no. 1, 2018.

[2] O. E. Rossler, "An equation for hyperchaos," *Physics Letters A*, vol. 71, no. 2, pp. 155–157, 1979.

[3] F. Verhulst and T. Bakri, "The Sprott B system," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 34, no. 10, p. 103116, 2024.

[4] P. Ding, J. Zhu, and J. Zhang, "A four-dimensional no-equilibrium chaotic system with multi-scroll chaotic hidden attractors and its application in image encryption," *Physica Scripta*, vol. 99, no. 10, p. 105211, 2024.

[5] A. A.-H. Shoreh, N. V. Kuznetsov, and T. N. Mokaev, "New adaptive synchronization algorithm for a general class of complex hyperchaotic systems with unknown parameters and its application to secure communication," *Physica A: Statistical Mechanics and its Applications*, vol. 586, p. 126466, 2022.

[6] P. K. Pal and D. Kumar, "Zirili map-based image encryption method for healthcare, military, and personal data security," *Physica Scripta*, vol. 99, no. 12, p. 125228, 2024.

[7] P. K. Pal and D. Kumar, "The coupled Kaplan–Yorke-Logistic map for the image encryption applications," *Computers and Electrical Engineering*, vol. 120, p. 109850, 2024.

[8] P. K. Pal, D. Kumar, and V. Agarwal, "Efficient image encryption using the Tinkerbell map in conjunction with linear feedback shift registers," *Multimedia Tools and Applications*, vol. 83, no. 15, pp. 44903–44932, 2024.

[9] T. Janaki and G. Rangarajan, "Lyapunov exponents for continuous-time dynamical systems," *Journal of the Indian Institute of Science*, vol. 78, no. 4, p. 267, 1998.

[10] Various, "Synchronization and application of a novel hyperchaotic system based

on adaptive observers," *Applied Sciences*, vol. 14, no. 3, p. 1311, 2024.

[11] D. Khattar, M. Sirohi, and R. Bansal, "Comparative analysis of two novel chaotic systems, and validation of hybrid function projective and complete synchronization using active-adaptive control," *Physica Scripta*, vol. 99, no. 12, p. 125244, 2024.

[12] N. Yadav, Pallav, and H. Handa, "Projective synchronization for a new class of chaotic/hyperchaotic systems with and without parametric uncertainty," *Transactions of the Institute of Measurement and Control*, vol. 45, no. 5, pp. 950–965, 2023.

[13] P. K. Pal and D. Kumar, "A novel chaotic map with high chaotic dynamics for image encryption applications," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–6, 2024.