



**GENERALIZATION AND CONTROL OF CHAOTIC
SYSTEMS USING EXTRA PARAMETERS AND
AFFINE TRANSFORMATIONS**

By

Wafaa Saber AbdelHalim Sayed

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
DOCTOR OF PHILOSOPHY
in
Engineering Mathematics

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2020

**GENERALIZATION AND CONTROL OF CHAOTIC
SYSTEMS USING EXTRA PARAMETERS AND
AFFINE TRANSFORMATIONS**

By

Wafaa Saber AbdelHalim Sayed

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
DOCTOR OF PHILOSOPHY
in
Engineering Mathematics

Under the Supervision of

Prof. Dr. AbdelLatif E. Hussien

Professor

Engineering Mathematics and Physics Department

Faculty of Engineering, Cairo University

Prof. Dr. Ahmed G. Radwan

Professor

Engineering Mathematics and Physics Department

Faculty of Engineering, Cairo University

on leave (Nile University)

Prof. Dr. Hossam A. H. Fahmy

Professor

Electronics and Communication Engineering Department

Faculty of Engineering, Cairo University

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT

2020

**GENERALIZATION AND CONTROL OF CHAOTIC
SYSTEMS USING EXTRA PARAMETERS AND
AFFINE TRANSFORMATIONS**

By

Wafaa Saber AbdelHalim Sayed

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
DOCTOR OF PHILOSOPHY
in
Engineering Mathematics

Approved by the Examining Committee:

Prof. Dr. AbdelLatif E. Hussien, Thesis Main Advisor

Prof. Dr. Ahmed G. Radwan, Advisor
Professor, Nile University

Prof. Dr. Mohammed A. El-Beltagy, Internal Examiner

Prof. Dr. Hassan I. Saleh, External Examiner
Professor, Radiation Engineering, Egyptian Atomic Energy Authority

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2020

Engineer's Name: Wafaa Saber AbdelHalim Sayed
Date of Birth: 20/3/1991
Nationality: Egyptian
E-mail: wafaa.s.sayed@eng.cu.edu.eg
Registration Date: 1/10/2015
Awarding Date: --/--/2020
Degree: Doctor of Philosophy
Department: Engineering Mathematics and Physics



Supervisors:

Prof. Dr. AbdelLatif E. Hussien
Prof. Dr. Ahmed G. Radwan
Professor, Nile University
Prof. Dr. Hossam A. H. Fahmy

Examiners:

Prof. Dr. Hassan I. Saleh, Professor, (External examiner)
Radiation Engineering, Egyptian Atomic Energy Authority
Prof. Dr. Mohammed A. El-Beltagy (Internal examiner)
Prof. Dr. AbdelLatif E. Hussien (Thesis main advisor)
Prof. Dr. Ahmed G. Radwan (Advisor)
Professor, Nile University

Title of Thesis:

Generalization and Control of Chaotic Systems Using Extra Parameters and Affine Transformations

Key Words:

Fractional dynamics; Hidden attractors; Image encryption; Non-autonomous control; Switched synchronization

Summary:

Generalized scaled, reflected, rotated, sheared and/or translated chaotic attractors are generated via extra parameters and affine transformations. Reproducibility rules are set and potential applications of the implementation sensitivity property are discussed. Distributed self-reproduced attractors on an arbitrary trajectory are generated through dynamic parameters. A nontraditional multi-character chaotic writer is introduced. The proposed generalized chaotic systems are verified experimentally and exploited successfully in simple and synchronization-dependent ciphers.

Disclaimer

I hereby declare that this thesis is my own original work and that no part of it has been submitted for a degree qualification at any other university or institute.

I further declare that I have appropriately acknowledged all sources used and have cited them in the references section.

Name: Wafaa Saber AbdelHalim Sayed

Date:

Signature:

Dedication

To my beloved mother, Taragy, for her invaluable support. I could not have accomplished any success without her continual efforts.

To my beloved younger brother, Ahmed, who is a source of inspiration and a motivation for success.

To my sister by heart, not blood, my best friend forever Shaimaa Samir.

Acknowledgements

First and foremost, I am thankful to Allah for His uncountable grants upon all of us.

I owe sincere gratitude to Prof. AbdelLatif E. Hussien, Prof. Ahmed G. Radwan, and Prof. Hossam A. H. Fahmy for their valuable guidance and support. It is my pleasure to have this distinguished group of professors as my MSc. and PhD. thesis advisors, and I hope I managed to be as trustworthy as they expected. They gave me so much of their precious time, in spite of their busy schedules, and helped me out of many problems with their knowledge and experience. They have always encouraged me to explore new areas of science. They provided me with invaluable guidance in my early experiences in international publication. They answered my questions patiently and paid attention to every fine detail.

I would also like to thank Prof. Ahmed G. Radwan for being confident in my capabilities, motivating me to exert relentless efforts in my work and recommending me to participate in several research projects and collaborations. Through his recommendation, I got the great chance of learning from Prof. Salwa Abd-El-Hafiz; her extraordinary knowledge, diligence, dedication and accuracy cannot be easily put in words. I would also like to thank Eng. Moheb Henein, Eng. Sherif AbdElHaleem, Eng. Merna Habib, and Eng. Mohammed Tolba for their cooperation, sharing their expertise and the positive impact of our collaboration on the development of my knowledge.

I would like to thank my dear superior colleagues; specifically those who are patiently always a source of support and kindness and those who have helped me since day one as a teaching assistant and postgraduate student, namely: Dr. Ahmed ElSheikh and Dr. Mahmoud Taha. Special thanks go to the most trustworthy superior colleague Dr. Mohammed Fouda, who has always helped me in many situations, patiently provided me with his special technical tips and tricks whenever I got stuck, and given me sincere advice; let alone that he recommended me as an MSc. student to Prof. Radwan.

Finally, I would like to thank my dear friends and companions during the teaching, postgraduate studies, MSc. and PhD. journey. For the ones who are still in connection, I hope that it is not just a phase that will come to an end and that we can keep in touch and maintain the friendship bonds. I am grateful to every colleague, teacher and professor who contributed to my knowledge and my decisions throughout the route towards my career. May Allah bless and reward all those who have supported me.

Table of Contents

Disclaimer	i
Dedication	ii
Acknowledgements	iii
Table of Contents	iv
List of Tables	vii
List of Figures	ix
List of Symbols and Abbreviations	xii
Abstract	xiii
1 INTRODUCTION	1
1.1 Background and Motivation	1
1.2 List of Main Contributions	2
1.3 Publications out of this Thesis	3
1.4 Thesis Organization	4
2 REVIEW OF LITERATURE	6
2.1 Evolution of Chaotic Generators	6
2.1.1 Discrete-Time Chaotic Maps	6
2.1.2 Continuous-Time Chaotic Systems	7
2.1.2.1 Multi-Stability and Co-existing Attractors	8
2.1.2.2 Multi-Scroll and Multi-Wing Chaotic Attractors	8
2.1.2.3 Hidden Attractors	9
2.1.2.4 Fractional Calculus and Chaotic Systems	9
2.2 Generalization and Control of Chaotic Systems: Motivation and Review	9
2.2.1 Amplitude Control	10
2.2.2 Offset Boosting	11
2.2.3 More Systems with a Variable/Infinite Number of Equilibrium Points	13
2.2.4 Polarity and Degree Modification, Functions and Transformations	14
2.2.5 Chaotic Systems in Spherical Coordinates	16
2.2.6 Classification of the Reviewed Papers	17
2.3 Chaotic Synchronization and Encryption Applications	18
2.4 Implementation of Chaotic Systems	18
2.4.1 Digitally Implemented Generalized Chaotic Systems	19
2.4.2 Hidden Potential of Implementation Sensitivity	19

3	CONTROLLABLE JERK-BASED ATTRACTORS AND REPRODUCIBILITY	21
3.1	Two Modified Non-Linearities	21
3.1.1	Piece-Wise Nonlinearity: Scaled Tent Map	21
3.1.2	Quadratic Nonlinearity: Scaled Logistic Map	22
3.2	Generalized Controllable Jerk-Based Systems Using Extra Parameters	22
3.2.1	Sensitivity to Main System Parameters	27
3.2.2	Sensitivity to Scaling Parameters	30
3.2.3	Self-Reproducing and Multi-Scroll Attractors	34
3.2.4	Fractional-Order Extension and Sensitivity to Fractional Orders	35
3.3	Reproducibility Rules and Implementation Sensitivity	36
3.3.1	Sensitivity to Order of Additions	36
3.3.1.1	Software Floating-Point Implementation	38
3.3.1.2	Hardware Fixed-Point Implementation	41
3.3.2	Sensitivity to Order of Multiplications	42
3.3.2.1	Software Floating-Point Implementation	42
3.3.2.2	Hardware Fixed-Point Implementation	43
3.4	Sensitivity Effect on Image Encryption	46
3.4.1	Encryption and Decryption Schemes	46
3.4.2	Wrong Decryption Results	47
3.5	Encryption Application of the Mismatch Signal	48
4	2D AND 3D AFFINE TRANSFORMATIONS-BASED CONTROL	52
4.1	Two-Dimensional Affine Transformations	52
4.2	Validation Examples	53
4.2.1	Validation Example 1: Generalized Simplest System	53
4.2.2	Validation Example 2: Generalized Lorenz System	56
4.3	Trajectory Control by Dynamic Translation	56
4.4	PRNG and Image Encryption Application	59
4.4.1	Encryption and Decryption Schemes	61
4.4.2	Performance Evaluation	62
4.4.2.1	PRNG Properties	62
4.4.2.2	Perceptual and Statistical Tests	62
4.4.2.3	Key Space and Key Sensitivity	65
4.4.2.4	Resistance to Differential Attacks	65
4.4.2.5	Resistance to Other Cryptanalysis Attacks	65
4.4.2.6	Robustness Against Noise	67
4.4.2.7	Time Analysis	67
4.4.3	Discussion and Comparison Against Other Works	68
4.5	Extension to 3D and Fractional Systems with Hidden Attractors	70
4.5.1	Hidden Chaotic Attractors in Fractional-Order Systems	71
4.5.2	3D Affine Transformations in Fractional Systems	72
4.5.3	Autonomous Parameters	73
4.5.3.1	Time Series Complexity Estimation	75
4.5.3.2	Generic Parameters and Bifurcation Diagrams	76
4.5.4	Non-Autonomous Parameters	77
4.5.4.1	Multiple Wings Generated by Multi-Level Pulse Signals	77

4.5.4.2	Multiple Wings Distributed on a Predefined or Arbitrary Line, Curve or Surface	77
4.5.5	Impact on Potential Encryption Applications	79
5	PLANAR AND SPATIAL ROTATION WITH A SYNCHRONIZATION-DEPENDENT ENCRYPTION APPLICATION	82
5.1	Rotation with Offset Boosting and Amplitude Control	82
5.1.1	Multi-Character Chaotic Attractor	82
5.1.1.1	V-like Characters	83
5.1.1.2	Straight Characters	84
5.1.1.3	Curved Characters	84
5.1.2	Planarly Rotating Translational Fractional-Order Multi-Scroll Grid Chaotic System	86
5.1.2.1	Encryption Applications	87
5.1.2.2	Experimental FPGA Realization	90
5.2	Synchronization-Dependent Image Encryption Application	92
5.2.1	Dynamic Rotation of Three Fractional-Order Chaotic Systems	92
5.2.2	Generalized Switched Synchronization Scheme	95
5.2.3	Simulation Results for the Synchronization Scheme	96
5.2.4	Proposed Encryption/Decryption Scheme	97
5.2.5	Simulation Results and Performance Evaluation	100
5.2.6	Discussion and Comparison	103
5.3	Three-Dimensional Rotating Chaotic Systems	105
5.3.1	Implementation I: Matrix-Based Rotation	105
5.3.1.1	Mathematical Analysis	105
5.3.1.2	Matrix-Based Rotating Chaotic System	105
5.3.2	Implementation II: Quaternions-Based Rotation	106
5.3.2.1	Mathematical Analysis	106
5.3.2.2	Quaternion-Based Rotating Chaotic System	107
5.3.3	Implementation III: Shearing-Based Rotation	107
5.3.3.1	Mathematical Analysis of 2D Skewing	107
5.3.3.2	Shearing-Based Rotating Chaotic System	109
5.3.4	Spatially Rotating Fractional-Order System Realization	109
5.4	Preliminary Insights on Jerk-Analogues in Other Coordinates	112
6	CONCLUSIONS AND FUTURE WORK	113
	References	116

List of Tables

2.1	Examples of chaotic generators	7
3.1	Proposed systems and their properties	25
3.2	Responses against the parameter r at $a = b = \mu = 1$	27
3.3	Responses against the parameter μ at $a = b = 1$ and $r = 0.6$	27
3.4	Summary of the sensitivity to the system parameter μ and the similarities with the discrete scaled tent and logistic maps	29
3.5	Piece-wise nonlinearity system attractor diagrams and time series for different combinations of the parameters b and μ at $a = 1$ and $r = 0.6$. . .	30
3.6	Summary of the sensitivity of the piece-wise nonlinearity system to the scaling parameters a and b and the similarities with the discrete scaled tent map	31
3.7	Summary of the sensitivity of the quadratic nonlinearity system to the scaling parameters a and b and the similarities with the discrete scaled logistic map	32
3.8	Piece-wise nonlinearity system responses versus the fractional-order α at parameter values $a = b = \mu = 1$ and $r = 0.6$	37
3.9	Quadratic nonlinearity system responses versus the fractional-order α at parameter values $a = b = \mu = 1$ and $r = 0.5$	37
3.10	Different implementations of three chaotic systems corresponding to different orders of addition	38
3.11	Time series and three-dimensional plots of the error between cases I and III of system 1 for different time steps and precisions in a floating-point implementation	40
3.12	Time series and three-dimensional plots of the error between cases I and III of systems 2 and 3 for different time steps and precisions in a software floating-point implementation	41
3.13	Time series and three-dimensional plots of the error between cases I and V of system 3 for different time steps and precisions in a floating-point implementation on Matlab	44
3.14	Time series and three-dimensional plots of the error between cases I and V of system 3 for different time steps and precisions in a fixed-point implementation	45
3.15	Hardware resources utilization and efficiency of mismatch signals production	46
3.16	Performance metrics of image encryption systems	48
3.17	Decryption results for each of cases I, IV and V using case V in encryption	49
3.18	Performance evaluation of the image encryption scheme based on the mismatch signal	50
3.19	NIST results for the PRNG based on the mismatch signal and encrypted images	51
4.1	Example transformations of the simplest chaotic system	54
4.2	Transformations of the simplest chaotic system: results and discussion . .	55

4.3	Attractor diagrams and time series of (4.8)	57
4.4	Trajectory control of (4.9) for $a = e = 0.1$ and different dynamic c and f parameters	60
4.5	NIST results for the PRNG and encrypted images	64
4.6	Performance metrics of the scheme for three encrypted images	66
4.7	Chosen plaintext attack/known plaintext attack analysis	67
4.8	Comparison of the ideas and evaluation of different image encryption schemes	69
4.9	Summary of Hidden Chaotic Attractors in Fractional-Order Systems	72
4.10	Transformed Systems Special Cases Using Autonomous Parameters	74
4.11	Multi-level pulse signals used in Fig. 4.14	78
5.1	Single character generation	85
5.2	x - y projections and bifurcation diagrams of the solution of (5.8)	88
5.3	The proposed image encryption scheme and its performance analysis	89
5.4	The proposed speech encryption scheme and its performance analysis	90
5.5	FPGA summary and experimental results for rotating fractional-order multi-scroll attractor	91
5.6	Systems equations and attractor diagrams at $(\alpha, \beta, \gamma) = (0.99, 0.96, 0.95)$	93
5.7	Dynamic rotation examples for the three systems and four dynamic signals, where $A = 5$ and $T = 50$	94
5.8	Successful synchronization simulation results	98
5.9	NIST results for the PRNG from the three chaotic systems	101
5.10	Performance evaluation of the image encryption scheme for three synchronization scenarios	102
5.11	3D rotation FPGA summary and experimental results for the fractional-order multi-scroll grid attractor	111
5.12	Proposed chaotic equations in other coordinate systems	112

List of Figures

2.1	Classification of the reviewed paper and their publication years.	17
3.1	Scaled (a) positive and (b) mostly positive tent maps, where $\mu_{min} = -\left(1 + \frac{1}{b}\right)$.	23
3.2	Generic bifurcations of the scaled tent map in both sides of μ (a) $b < 1$, (b) $b > 1$	23
3.3	Bifurcations of the scaled tent map at (a) $b = 1$ and $a = \{0.5, 1, 2\}$ and (b) $a = 1$ and $b = \{1, 2, 4\}$	23
3.4	Scaled (a) positive and (b) mostly positive logistic maps.	24
3.5	(a) Generic bifurcations of the scaled logistic map and numerical examples at (b) $b = 1$ and $a = \{0.5, 1, 2\}$ and (c) $a = 1$ and $b = \{0.5, 1, 2\}$	24
3.6	Time series sampling to decide the type of system response.	26
3.7	Bifurcation diagram and MLE against the parameter r for (a) the piece-wise nonlinearity system at $\mu = a = b = 1$ and (b) the quadratic non-linearity system at $\mu = a = b = 1$	28
3.8	Scaled chaotic responses of the piece-wise nonlinearity system for different values of the parameter a at $b = \mu = 1$, $r = 0.6$	33
3.9	Scaled chaotic responses of the quadratic nonlinearity system for different values of the parameter b at $a = \mu = 1$ and $r = 0.5$	33
3.10	Bifurcation diagrams versus μ of (a) the piece-wise nonlinearity system at $b = \{0.5, 1\}$ and (b) the quadratic nonlinearity system at $a = \{0.5, 1\}$	34
3.11	Differently allocated attractor diagrams at $b > 0$ (darker) and $b < 0$ (lighter) for (a) the piece-wise nonlinearity system and (b) the quadratic nonlinearity system.	34
3.12	(a) Four-scroll attractor using the piece-wise nonlinearity system and (b) Double-scroll attractor using the quadratic nonlinearity system.	35
3.13	The studied chaotic systems and map, their implementation cases and sensitivity factors.	38
3.14	(a) Attractor diagrams and (b) mismatches in x time series of the three cases of system 1 in software double-precision floating-point implementation.	39
3.15	Bifurcation diagrams of (a) system 1, (b) system 3, (c) LEs of system 3 at $b = 0.6$ and (d) MLE versus b	42
3.16	(a) Exact implementation, f_1 versus f_1 . (b) Double-precision and (c) single-precision floating-point different implementations, f_2 versus f_1 , of the logistic map.	43
3.17	Fixed-point computations sensitivity of the logistic map (a) $p_f = 24$, (b) $p_f = 32$ and (c) $p_f = 48$	44
3.18	Chaotic properties of f_1 in double, single floating-point and fixed point ($p_f = 32$) computations (a) time series and (b) MLE.	45
3.19	Oscilloscope experimental mismatch signal result between two different cases of system 3.	46
3.20	(a) Encryption and decryption block diagrams of the stream cipher system with feedback, (b) multiplexing table and (c) the utilized PRNG.	47

3.21	(a) Time series, (b) frequency distribution of the outputs, (c) histogram and (d) auto-correlation function of the PRNG based on the mismatch signal.	50
4.1	Attractor diagram and time series of system (4.3).	53
4.2	EVI against θ at the (a) first and (b) second equilibrium points.	56
4.3	MLE of (4.8) against the parameters in (a) Scaling, (b) Translation and (c) Shearing cases.	58
4.4	Trajectory control of transformed Lorenz chaotic system by scaling and translation for (a) line $f = c$, (b) parabola $f = c^2$, (c) a square and (d) a circle of radius 4 ($c^2 + f^2 = 16$) at $a = e = \frac{1}{8}$.	58
4.5	Bifurcation diagrams of transformed Lorenz chaotic system against the translation parameter c for the parabolic trajectory $f = c^2$ and different values of the scaling parameters (a) $a = e = 0.1$ and (b) $a = e = 0.7$.	59
4.6	(a) Encryption/decryption block diagrams, encryption/decryption key for (b) Lorenz and (c) transformed Lorenz chaotic generators and (d) multiplexing table.	61
4.7	Time series of Lorenz, light colored, and transformed Lorenz, dark colored, at $a = 2, b = 0.25, c = 3, d = -0.5, e = -2, f = -4, x_0 = y_0 = z_0 = w_0 = 0.1, u_0 = 3.225$ and $v_0 = -0.425$.	62
4.8	Time series, frequency distribution of the outputs and histogram of the PRNG using (a) Lorenz and (b) transformed Lorenz chaotic generators.	63
4.9	Original and encrypted (a) mandril and (b) peppers images.	64
4.10	Histograms of the red channel of (a) Lena image and the corresponding encrypted images using (b) Lorenz and (c) transformed Lorenz systems.	64
4.11	Decrypted images and correlation coefficients corresponding to Lena for (a) AWGN of mean 0 and different variances and (b) S & P of different densities when $P_{sum} = 0$ and MUX is removed.	68
4.12	Generic case of transformed (a) system 1 and (b) system 2.	76
4.13	Bifurcation diagrams and SE plots of transformed system 2 against affine transformation parameters.	77
4.14	Multi-wing attractors by transformed system 1 and multi-level pulse signals as (a) scaling (b) skewing parameters and (c) rotation angle.	78
4.15	Self-reproduced attractors by transformed system 1 along (a) a line, (b) a circle and (c) a sphere.	79
4.16	Simple example substitution cipher based on the proposed transformed system(s) and encryption key design.	80
4.17	(a) u , (b) v and (c) w bifurcation diagrams and (d) MLE against the rotation angle θ of rotating Lorenz system.	81
5.1	Rotating multi-scroll system at (a) $\theta = 0$ and (b) $\theta = \pi/2$.	84
5.2	Rotating V-shape for dynamic values of θ and different number of scrolls.	84
5.3	Multi-character attractors writing (a) "WELCOME", (b) "WORLD", "WELCOME WORLD" on (c) a single line and (d) two lines.	86
5.4	Two-dimensional (a) static translation, (b) dynamic translation and (c) dynamic rotation.	88
5.5	Experimental results for rotating integer-order V-shape multi-scroll attractor	91
5.6	Static rotation of the three fractional-order chaotic systems.	93

5.7	Multi-scroll attractors generated by dynamic rotation of system 2 using (a) $\theta = 5 \text{ square}\left(\frac{2\pi t}{50}\right)$ and (b) $\theta = 5 + \lfloor \frac{t}{50} \rfloor$	94
5.8	Generalized dynamic switched synchronization scheme of rotating fractional-order chaotic systems.	96
5.9	Generalized dynamic switched synchronization applications on rotating chaotic systems.	97
5.10	Synchronization-Dependent Image Encryption/Decryption Scheme.	99
5.11	Histograms of the encrypted red channel for (a) scenario 1 (b) scenario 2 and (c) scenario 3.	101
5.12	Failed attack of image green channel restoration from the proposed rotating chaotic time series.	103
5.13	Projections of the attractor diagrams of (5.22) at (a) $\theta_1 = \theta_2 = 0$ and $\theta_3 = \pi/4$, (b) $\theta_1 = \theta_3 = 0$ and $\theta_2 = \pi/4$ and (c) $\theta_2 = \theta_3 = 0$ and $\theta_1 = \pi/4$	106
5.14	Attractor diagram and time series from the rotation-matrix and quaternion-based implementations.	108
5.15	Rotation by -20° using three successive shears for the simplest chaotic system.	110
5.16	Attractor diagram and time series from the rotation-matrix and shearing-based implementations.	110
5.17	Spatially rotating fractional-order multi-scroll grid attractor at $(\theta_1, \theta_2, \theta_3) = (90^\circ, 90^\circ, 45^\circ)$	111

List of Symbols and Abbreviations

AES	Advanced Encryption Standard
AWGN	Additive White Gaussian Noise
CORDIC	Coordinate Rotation Digital Computer
EVI (ϕ_E)	Eigenvectors Inclination
FPGA	Field Programmable Gate Array
GL	Grünwald-Letnikov
LE	Lyapunov Exponents
LSB	Least Significant Bit
MLE	Maximum Lyapunov Exponent
MSE	Mean Squared Error
NIST	National Institute of Standards & Technology
NPCR	Number of Pixel Change Rate
NSCR	Number of Sample Change Rate
PP	Proportion of Passing Sequences
PRNG	Pseudo-Random Number Generator
PSNR	Peak Signal-to-Noise Ratio
PV	P-Value Distribution
S & P	Salt and Pepper Noise
SE	Spectral Entropy
UACI	Unified Average Changing Intensity
$sgn(\cdot)$	Signum function
$\Gamma(\cdot)$	Gamma function
$H(\cdot)$	Heaviside function
ρ	Correlation coefficient

Abstract

Generalized and controllable chaotic systems are highly required for various engineering applications such as: Pseudo-Random Number Generation (PRNG) for chaos-based communication, motion planning and natural phenomena and behavior modeling. In this thesis, various chaos generalization and control approaches are presented highlighting their advantages and discussing their limitations.

The first approach controls jerk-based attractors by employing generalized discrete maps with extra parameters as their nonlinear terms. The effect of different implementation factors on traditional chaotic ciphers is uncovered and reproducibility rules are recommended. The mismatch signals between slightly different implementations are consciously utilized in PRNG and encryption applications. The second approach is suitable for any chaotic system, where two-dimensional affine transformations provide scaling, reflection, rotation, shearing, translation and multi-scroll generation from the traditional systems with single or limited attractors. An encryption application is presented to validate the good cryptographic properties of and the role of the proposed generalization in enhancing the key space and, hence, the robustness against brute force attacks. This approach is further extended to cover three-dimensional transformations and control fractional-order systems with hidden attractors with challenging properties. Using affine transformations, non-autonomous trajectory control and distributed self-reproduced attractors generation along an arbitrary line, curve or surface are achieved through dynamic parameters.

A slightly modified approach focuses on planar rotation followed by translation and scaling and is applied to multi-scroll systems with already wide basin of attraction to be capable of covering the whole space. A multi-character chaotic writer is designed by a planarly rotating V-shape system with amplitude control and offset boosting. A rotating translational fractional-order multi-scroll grid attractor is also presented, utilized successfully in speech and image encryption applications and verified experimentally on Field Programmable Gate Arrays (FPGAs). A novel generalized switched synchronization-dependent secure communication setup is proposed accordingly, which is suitable for one-to-one, one-to-many, mutual interconnection and role switching. An image encryption scheme is proposed, which modulates the rotation angle of a fractional-order chaotic system using the plain image and uses this system as a PRNG in data substitution. The scheme successfully passes the standard performance tests. The rotation transformation is extended to three-dimensions presenting spatially rotating chaotic attractors. Three different implementations of three-dimensional rotation are presented: matrix-based, quaternions-based and shearing-based. The matrix-based implementation is verified experimentally as well. Preliminary results on chaotic systems in polar and spherical coordinate systems are also presented.

Chapter 1: Introduction

1.1 Background and Motivation

Interest in chaos theory and chaotic systems research dates back to 1963 [1]. Chaotic systems may be given by discrete-time difference equations or continuous-time differential equations with nonlinear terms, which are deterministic on the short term. Yet, for specific parameter ranges, their outputs are nearly aperiodic, random and unpredictable on the long term evolution. In addition, they exhibit increased sensitivity to the initial conditions, or the so-called butterfly effect [1]. That is, initially nearby points can evolve quickly into very different states.

Such randomness, complexity, sensitivity and unpredictability properties are extensively required in many fields of applications. Consequently, chaotic systems are used to mathematically model behaviors of natural phenomena, physical systems and real-life applications in many fields such as: physics, electronics, circuit theory, biology, chemistry, meteorology, traffic and finance [2]. In addition, many applications utilize their output sequences as PRNGs in engineering and telecommunications applications such as chaos-based secure communication, modulation, synchronization, compression and cryptography.

To fulfill the needs of all these multidisciplinary fields, there is a continuous need to come up with modified, generalized and novel chaotic systems. These newly proposed or modified systems should at least preserve the chaotic dynamics of the original systems, if they do not boost them. They act as alternative models in modeling applications and novel sources of randomness in PRNG applications, which pushes forward the research in these fields as well. Chaotic systems with enhanced properties eventually improve the overall system's performance in their application fields. Meanwhile, and since chaotic systems are deterministic difference or differential equations, they are relatively simpler sources of randomness to study and implement. Consequently, their mathematical analysis, software numerical simulation, hardware analog and digital realization have been flourishing research fields in the last few decades.

The state-of-the-art on generalization and control of chaotic systems reveals a great deal of research that ranges from simple to more complicated methods of modification, generalization, control and searching for novel chaotic systems. After presenting the new equations, researchers target different perspectives of the topic, for example, they may carry out the mathematical analysis, study different chaotic properties, provide simulation-based validation of them, propose potential applications and/or present hardware realizations of their proposed systems.

This thesis proposes several generalization and non-autonomous control approaches of chaotic systems using extra parameters and affine transformations. In addition, the thesis uncovers another source of sensitivity besides the well-established parameters and initial values sensitivity, which is the implementation sensitivity and its potential applications. Having set the rules for reproducibility, digital applications and implementation of the proposed generalized systems are presented. The proposed generalization and control approaches enhance the chaotic properties and performance in such applications compared to recent related works.

1.2 List of Main Contributions

In this section, the main contributions of the thesis are listed briefly giving what is presented and clarifying how it is performed.

- A literature survey of generalized chaotic systems that control the chaotic output through parameters and/or transformations is presented.
- The first proposed generalization approach is specific for jerk-based chaotic systems. It makes use of generalized chaotic maps with extra parameters as the nonlinear term.
- Implementation sensitivity, specifically, the algebraic associativity property is assessed on changing the order of terms addition and multiplication in a digital implementation.
 - Floating-point software and fixed-point hardware implementations of several systems are considered.
 - Implications of this sensitivity on chaos-based communication applications are discussed.
 - The mismatch between different implementations is used as an alternative randomness source and successfully passes several well-established performance metrics. Reproducibility rules are set accordingly.
- A more generic framework for generalization and control of chaotic systems using affine transformations is presented, mathematically analyzed and validated for several systems through numerical simulations. The proposed generalized chaotic systems range from integer-order systems with self-excited attractors to fractional-order systems with hidden attractors.
 - Special cases of the affine transformations (scaling, reflection, rotation, translation and shearing) are studied thoroughly, which provides simpler alternatives serving different purposes and applications.
 - The introduced parameters represent dimensions for increased sensitivity and controllability preserving the chaotic dynamics.
 - Complicated forms of chaotic dynamics such as self-reproducing attractors, multi-scroll strange attractors and robust chaos are proposed using the forms of generalization presented.
 - Non-autonomous trajectory control and distributed self-reproduced attractors generation along an arbitrary line, curve or surface are achieved through dynamic parameters.
 - Encryption applications of the proposed generalized systems are presented and shown to perform well compared to the original systems.
- Since the rotation angle is the parameter corresponding to robust chaos generation, specific attention and a big portion of the thesis is dedicated to rotation transformation, followed by translation and scaling.

- Analysis, simulation, implementation and applications of dynamically planarly rotating systems are presented.
 - A multi-character writer is proposed and employed in writing letters, words and sentences.
 - The fractional-order system is utilized successfully in speech and image encryption applications and verified experimentally on FPGA using GL technique and CORDIC algorithm.
 - A novel synchronization-dependent secure communication and RGB image encryption application is proposed. The encryption scheme employs rotation angle modulation using the plaintext and XOR logic operation for plaintext image substitution. The encryption scheme performs well for three synchronization scenarios.
 - Three different implementations of spatially rotating simplest chaotic system: matrix-based, quaternions-based and shearing-based are presented and validated.
 - The rotation matrix-based implementation is experimentally verified for a fractional-order system.
- Preliminary results on generalized chaotic systems in polar and spherical coordinate systems are also presented with fewer number of terms than recent related works.

1.3 Publications out of this Thesis

The following international journal, conference papers and book chapter have been published out of this work.

1. Sayed, W. S., Radwan, A. G., Fahmy, H. A., and Elsedeeq, A. “Trajectory control and image encryption using affine transformation of Lorenz system.” *Egyptian Informatics Journal* (2020) [3] (IF: 3.119)
2. Sayed, W. S., and Radwan, A. G. “Generalized switched synchronization and dependent image encryption using dynamically rotating fractional-order chaotic systems.” *AEU-International Journal of Electronics and Communications* (2020), 153268 [4] (IF: 2.924)
3. Sayed, W. S., Radwan, A. G., Fahmy, H. A., and Elsedeeq, A. “Software and hardware implementation sensitivity of chaotic systems and impact on encryption applications.” *Circuits, Systems, and Signal Processing*, 39, 11 (2020), 5638–5655 [5] (IF: 1.681)
4. Sayed, W. S., Radwan, A. G., Fahmy, H. A., and Elsedeeq, A. “All-dynamic synchronization of rotating fractional-order chaotic systems.” *Novel Intelligent and Leading Emerging Sciences Conference (NILES)* (2019), vol. 1, IEEE, pp. 226–229 [6]

5. Sayed, W. S., Radwan, A. G., Elnawawy, M., Orabi, H., Sagahyoon, A., Aloul, F., Elwakil, A. S., Fahmy, H., and El-Sedeek, A. “Two-dimensional rotation of chaotic attractors: Demonstrative examples and FPGA realization.” *Circuits, Systems, and Signal Processing* 38, 10 (2019), 4890–4903 [7] (IF: 1.681)
6. Sayed, W. S., Radwan, A. G., and Fahmy, H. A. “Chaos and bifurcation in controllable jerk-based self-excited attractors.” *Nonlinear Dynamical Systems with Self-Excited and Hidden Attractors*. Springer, 2018, pp. 45–70 [8]
7. Sayed, W. S., Radwan, A. G., and Fahmy, H. A. “Chaotic systems based on jerk equation and discrete maps with scaling parameters.” 6th International Conference on Modern Circuits and Systems Technologies (MOCASST) (2017), IEEE, pp. 1–4 [9]
8. Sayed, W. S., and Radwan, A. G. “Self-reproducing hidden attractors in fractional-order chaotic systems using affine transformations,” *IEEE Open Journal of Circuits and Systems* (Accepted)

1.4 Thesis Organization

First, Chapter 2 presents a literature review on generalization and non-autonomous control of chaotic systems using extra parameters, transformations and other similar approaches. In addition, it reviews the implementations and applications of these approaches and other recent research on digital implementation and applications of chaotic systems. Then, Chapter 3 proposes our first generalization approach for jerk-based attractors and their control by employing generalized discrete maps with extra parameters as their nonlinear terms. In addition, it uncovers the impact of implementation sensitivity property on traditional chaos-based encryption schemes and utilizes the mismatch signals between slightly different implementations in PRNG and encryption applications. Moreover, it sets reproducibility rules to avoid this “chaotic” error. Then, Chapter 4 proposes the second approach suitable for any chaotic systems, where two-dimensional affine transformations provide scaling, reflection, rotation, shearing, translation and multi-scroll generation from the traditional systems with single or limited attractors. An encryption application is presented to validate the good cryptographic properties of and the role of the proposed generalization in enhancing the key space and, hence, the robustness against brute force attacks. In addition, Chapter 4 extends this approach to cover three-dimensional transformations and control hidden attractors in fractional-order systems. Using affine transformations, non-autonomous trajectory control and distributed self-reproduced attractors generation along an arbitrary line, curve or surface are achieved through dynamic parameters. Then, Chapter 5 focuses on planar rotation followed by translation and scaling and applies this modified approach to multi-scroll systems with already wide basin of attraction to be capable of covering the whole space. A multi-character chaotic writer is designed by a planarly rotating V-shape system with amplitude control and offset boosting. A fractional-order rotating translational system is also presented, utilized successfully in speech and image encryption applications and verified experimentally on FPGAs. In addition, Chapter 5 proposes a novel generalized switched synchronization-dependent secure communication setup, which is suitable for one-to-one, one-to-many, mutual interconnection and role

switching. An image encryption scheme is proposed, which modulates the rotation angle of a fractional-order chaotic system using the plaintext image and uses this system as a PRNG in data substitution. The scheme successfully passes the standard performance tests. Moreover, Chapter 5 extends the rotation transformation to present spatially rotating chaotic attractors. Three different implementations of three-dimensional rotation are presented: matrix-based, quaternions-based and shearing-based. The matrix-based implementation is verified experimentally as well. Preliminary results on chaotic systems in polar and spherical coordinate systems are also presented. Finally, Chapter 6 provides a discussion of the results, a conclusion of their implications, and suggestions for possible future work directions.

Chapter 2: Review of Literature

Chaotic systems are highly sensitive to initial conditions, system parameters and implementation. The significant properties of chaotic systems are highly required in many applications such as: modeling [2], motion control [10] and cryptography [11]. Several recent PRNG and encryption applications utilized discrete chaotic maps [12] and continuous chaotic systems [13].

To fulfill the needs of all these multidisciplinary fields and others, there is a continuous need to come up with controllable modified, generalized and novel chaotic systems. Such systems are expected to at least preserve the chaotic dynamics and even exhibit more complex dynamical behaviors with higher degree of disorder and randomness. The broadband nature of chaotic signals imposes some limitations on implementation and applications. Controllability of the amplitude of chaotic signals overcomes such limitations, e.g., linear amplifier design and threshold voltage of operational amplifiers in an analog implementation [14]. Polarity control enables utilization in applications that need a unipolar signal [15, 16]. Having the capability of moving the chaotic attractor to multiple locations on the phase space is a challenging goal and an opportunity for various practical applications, e.g., phenomena and behavior modeling, motion control and secure communication. A number of recent research works provided various controllable strange attractors and are reviewed in this chapter. Yet, we start by reviewing earlier foundations of this research field.

2.1 Evolution of Chaotic Generators

The foundation of chaos theory dates back to Lorenz in 1963 [1], who described the butterfly effect, i.e., how a slight change in a single state of a deterministic nonlinear model (a butterfly flapping its wings in China) can lead to massive differences in a future state (a hurricane in Texas). Since then, this apparently random behavior from deterministic relations and initial conditions sensitivity were pointed out in many nonlinear systems. Numerous researches were conducted on chaotic systems, the construction of chaotic models, their mathematical analysis, implementation and applications. The two main categories of chaotic systems are discrete chaotic systems based on difference equations or iterative maps and continuous ones based on differential equations with examples shown in Table 2.1.

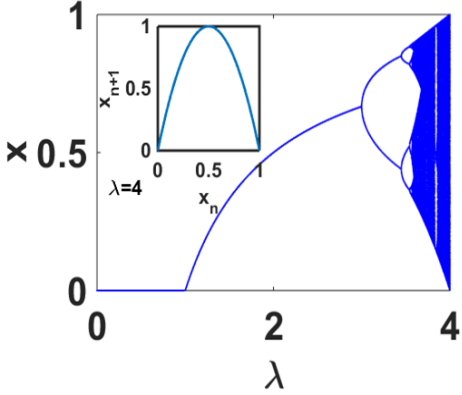
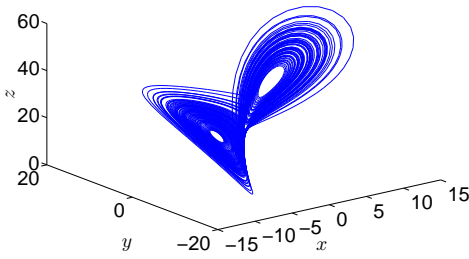
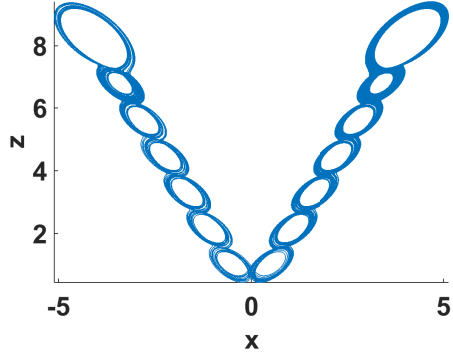
2.1.1 Discrete-Time Chaotic Maps

Discrete chaotic systems based on difference equations or iterative maps, in the form

$$x_{n+1} = f(x_n), \quad (2.1)$$

with nonlinear term(s). They generally have low dimension and are simple and easy to implement. One-dimensional maps include one iterative variable that change its value each iteration giving a time series. For example, Bernoulli shift map, the triangular (tent) map, the logistic map and the sine map. Higher-dimensional maps with more than one iterative variable were also presented [17]. There are continuous research advances in

Table 2.1: Examples of chaotic generators

Logistic map	Lorenz system
$x_{n+1} = \lambda x_n(1 - x_n)$	$\dot{x} = \sigma(y - x)$ $\dot{y} = x(\rho - z) - y$ $\dot{z} = xy - \beta z$ $(\sigma = 10, \rho = 28, \beta = 8/3)$
	
V-shape multi-scroll system	
$\dot{x} = y - x$ $\dot{y} = \text{sgn}(x)[1 - mz + G(z)],$ $\dot{z} = x - rz$	$G(z) = \begin{cases} 0 & z < s_0 \\ d_1 & s_0 < z < s_1 \\ \vdots & \\ d_{N-1} & z < s_{N-1} \end{cases}$
	

presenting novel chaotic maps with enhanced properties as will be explained in Chapter 3, which utilizes two examples of them in constructing continuous chaotic systems.

2.1.2 Continuous-Time Chaotic Systems

Continuous chaotic differential equations are more capable of modeling the continuity of natural phenomena and real world behaviors. In addition, they overpass discrete maps in performance because they have higher dimension, exhibit more complicated chaotic dynamics, richer chaotic properties and generally more suitable for applications that require multiple dependent chaotic outputs such as color image encryption. Continuous

chaotic systems require the implementation of integration/differentiation operations in analog circuits and discretization using numerical techniques in digital platforms.

Solving the system numerically results in chaotic time series corresponding to each state variable and a strange attractor in the phase space. Basic mathematical analysis of continuous chaotic systems start by finding the equilibrium points at which the derivatives equal zero. Then, the stability of the system is studied using the eigenvalues of the Jacobian matrix, which are evaluated at the equilibrium points [17]. It has been conceived for a long time that strange attractors can only be located near unstable equilibrium point(s) of type saddle focus, i.e., when the equilibrium point has one real eigenvalue whose sign is opposite to the sign of a pair of complex conjugate eigenvalues. The number of eigenvalues with positive real part is called the index and determines whether the resulting strange attractor has one or two scrolls. Such systems are called self-excited attractors; however, new types of attractors with different conditions were discovered in the last decade [18] as detailed in Subsection 2.1.2.3.

One of the more advanced measures to quantify chaotic behavior are the Lyapunov Exponents (LE), which measure the sensitivity to initial conditions through the exponential divergence of nearby trajectories. The Maximum Lyapunov Exponent (MLE) should be finite positive for chaotic systems and systems with more than one positive Lyapunov exponents are called hyper-chaotic systems.

2.1.2.1 Multi-Stability and Co-existing Attractors

An attractor's basin of attraction means all the initial conditions that converge to this attractor. Multi-stability is the co-existence of different attractors when starting from different initial conditions for a given set of parameters. The range or set of parameter values that converge to an attractor are also referred to as its parameter basin of attraction [19].

2.1.2.2 Multi-Scroll and Multi-Wing Chaotic Attractors

Chaotic systems exhibit interesting and more complex topologies when they generate a larger number of scrolls. Various nonlinear signals with breakpoints were utilized as methods of multi-scroll and multi-wing generation, where both expressions are used interchangeably [20]. Other papers [21,22] described systems based on Chua family with piecewise nonlinearity as multi-scroll attractors and those based on Lorenz family with quadratic nonlinearity as multi-wing attractors.

For a relatively long time, these methods depended only on the phase space or state variables not time to maintain the autonomous, i.e., time invariant, characteristic. The state-of-the-art multi-valued nonlinear signals utilized in multi-scroll generation include piecewise-linear, saturated sequence, sawtooth, step wave, hysteresis series, switching, sine, and hyperbolic tangent signals, which are functions of the state variables [20]. The construction of these nonlinear signals generally involves one or more challenges such as: unsystematic complicated design, calculations, circuit realization, difficulty of scrolls regulation and the dependence on extending unstable equilibrium points, which is not generally applicable to hidden attractors [23]. Systems with grid scroll attractors and scrolls extending in multi-dimensional-planes are also generated when the nonlinear functions involve more than one state variable simultaneously.

Compared to autonomous multi-scroll generation methods, fewer researches employed non-autonomous methods to autonomous chaotic systems. Parameter sign switching by a square wave was utilized in [24]. A composite multilevel signal, which is constructed by applying a signum function on a sinusoidal function of time, was applied in [25], yet, to already non-autonomous chaotic oscillators. Switching methods based on thresholding using non-autonomous signals inspired by [25] were presented afterwards for autonomous chaotic systems and will be reviewed in Section 2.2.

2.1.2.3 Hidden Attractors

Attractors that can be located in the vicinity of unstable equilibrium points are called self-excited. Hidden attractors are computationally “hidden” because they can not be located using the same method. Their basins of attraction do not intersect with small neighborhoods of the unstable equilibrium point. Their types include systems without equilibria, with stable equilibria whether a single point or a line, and infinite number of equilibria [26].

2.1.2.4 Fractional Calculus and Chaotic Systems

Fractional-order calculus, which is the non-integer counterpart of the classical integer-order calculus, has a relatively long history in theory than applications. The fractional orders provide more controllability of the governing mathematical relations. Fractional-order chaotic systems exhibit the interesting aperiodicity, ergodicity, randomness, and sensitivity properties of their integer-order counterparts and more [27]. Fractional-order extensions of both discrete [28] and continuous chaotic systems [27] were presented. In this thesis, we focus more on continuous ones owing to their previously mentioned complexities and advantages. The derivative, e.g., Dx becomes $D^\alpha x$, where α can take non-integer values. Fractional calculus has always been known for its capability of describing and modeling a real object more accurately since it includes memory effect. That is, the solution of such equations does not only depend on the previous state, but also all the system’s states since its initial state. However, the solution and implementation of fractional-order systems started to flourish only a few decades ago with the advances in digital computers and digital realization technologies [29, 30]. Digital hardware realizations can use the short memory principal to reduce the number of terms to be summed and, hence, the hardware resources utilization and efficiency [31–34].

2.2 Generalization and Control of Chaotic Systems: Motivation and Review

This work was initiated based on the research questions: To what extent can we control the size, location and repetition of a strange attractor of a given chaotic system? Is it doable without modifying the nonlinear terms of its state variables similar to many multi-scroll generation approaches? and how can this be formulated and implemented? Collecting the relevant state-of-the-art researches was challenging and required continuous follow-up for the recently published papers, especially the ones citing the papers that we already reached. However, the terminologies are not unified between papers and use common

words such as: displacement, control, transform, transformation, novel system, method, technique, framework instead of clear unique techniques names. Instead, they focus on their objectives in the title and keywords of their articles such as multi-scroll generation or circuit realization. Consequently, they can not be easily identified among the flood of publications on novel chaotic systems.

Besides the conventional and emerging types of chaotic systems reviewed in the previous section, other attempts have flourished recently. Generalization results in a novel chaotic system with various cases of operation such that the unique attractor of the original system becomes a special case of the generalized one. When generalization involves additional control parameters, they provide extra degrees of freedom and controllability. Hence, several properties of a chaotic system, its time series, and hence, strange attractor can be controlled, e.g., the attractor's size, location and shape. The displacement or allocation of equilibrium points can be either static or dynamic. Static allocation preserves the same number of equilibria, but enables different combinations of initial values and/or parameters. That is, it widens the basin of attraction and/or parameter basin of attraction. Dynamic allocation results in systems with a variable or infinite number of equilibria and, hence, it can be further used in multi-scroll attractors generation. The researches reviewed in this section address different combinations of these controllable properties of the strange attractor.

2.2.1 Amplitude Control

Amplitude control or rescaling of the chaotic time series and/or chaotic attractor usually takes place through multiplicative parameters or coefficients. J.C. Sprott initiated this approach for simple jerk-based chaotic systems that involve a differential equation of at least third order

$$\ddot{x} = f(\ddot{x}, \dot{x}, x) \quad (2.2)$$

and a nonlinearity [35–37]. The nature of the systems such as simplicity and mostly unified degree enabled the appearance of such terms. These scales were employed in the proposed implementation to guarantee suitable voltage level that is immune against noise and opamps saturation, but not utilized in applications.

Amplitude control of systems with quadratic nonlinearities was presented in [38] by introducing control functions in the form of m , $1/m$ and e^m to these quadratic nonlinear terms as their coefficients. This results in the control of the size of the attractor making it larger or smaller with the same topological properties and geometric structure. It has three modes: total amplitude control where there are unified coefficients for all quadratic terms, composite amplitude control where the coefficients are different and partial amplitude control where some quadratic terms have coefficients equal to unity. In all cases m is a fixed number. In addition, [39–41] investigated the opportunities offered by amplitude control technique to identify and study multi-stability with coexisting, sometimes hidden, attractors through exploring all possible initial conditions. The effects of amplitude control parameters on the frequency of the chaotic signals and rescaling the basins of attraction were shown to endanger the system chaotic dynamics imposing some complications in practical applications.

The same amplitude control modes of [38], led by Li and Sprott, were applied in subsequent researches to different chaotic systems alone [42] or combined with offset

boosting and/or frequency control as discussed in the following subsection. Yet, only very few recent papers have modified or generalized the idea instead of applying the same procedure. For example, [43] applied them to their proposed system with single quadratic nonlinearity. Amplitude control parameters enabled equilibrium points and strange attractor allocation.

Dynamic amplitude control for multi-scroll attractors generation has also been recently applied in [23], yet, formulated as a transformation. This paper is different from other amplitude control papers because scaling is performed via transformation of each state variable by a new one multiplied by a variable parameter in the form of a multilevel pulse signal. Similar to [43], this enables generating a number of scrolls without redesigning the nonlinear function of the original system, but via changing the dynamic parameter. Yet, regulating the number of scrolls through the amplitudes of the pulse signals in [23] can be considered more generic. Although the authors did not consider this comparison, their transformation approach may also overcome the limitations of the amplitude control in [38] as detailed in our related work throughout the rest of the thesis. Other more complicated forms of transformations are soon reviewed in Subsection 2.2.4.

2.2.2 Offset Boosting

Constant additive thresholds were added to the state variables in [21], which will be reviewed in Subsection 2.2.4 as it applied other transforms as a part of a multi-wing construction method. More recently, additive parameters and their usage for offset or translation of the chaotic attractor has flourished under the title “Offset Boosting”. It generally aims at generating attractors of the same size and shape but distributed in different spatial positions or shifted in any desired direction.

Firstly, [44] combined amplitude control with offset boosting for chaotic systems satisfying specific conditions such as: only quadratic nonlinearities and the presence of some terms in only one of the equations such that it has no self feedback and affects only one of the state variables directly. Offset boosting of other chaotic systems [45–47] that share the same specific conditions was also presented. The parameters affected different state variables such as an amplitude control parameter k_{xy} for the term xy and an offset parameter k_w for the state variable w in [45]. Such researches did not present a generic procedure or analysis why the parameters are inserted in these terms of the equations specifically; only some characteristics that give the selected system amplitude control and/or offset boosting potential.

One offset parameter used to boost a state variable enables attractor location control along a line in the direction of this state variable. The possibility of line (across direction), lattice (plane) and grid (space) of variable attractors was discussed in [48]. This allows propagation in as many directions as its degrees of freedom, i.e., number of offset state variables, provide. The utilized system is a fractional-order extension of a special case of the financial chaotic system setting some of its parameters to fixed values. It is worth mentioning that the systems exhibits chaotic behavior for fractional-orders only. Control/offset was enabled by the unique properties of the system itself to be valid for any value of the systems’ parameters. In these works [44–48], no switching, dynamic change of the offset parameters, multi-scroll generation or simultaneous attractors replication were proposed and they were limited to static offset boosting.

Similar to [39–41] in the case of amplitude control, [49] investigated the opportunities offered by offset boosting technique to identify and study multi-stability with coexisting attractors through exploring all possible initial conditions.

Several researches utilized the same idea of static parameter without modification as a part of illustrating the offset boostable capability of their proposed chaotic systems [50–53]. Yet, fewer papers have modified or generalized the idea similar to what happened with amplitude control. For example, Hong *et al.* led a concurrent research on non-autonomous or dynamic offset boosting control [54–57] for multi-scroll generation. The same composite function of [25] was utilized in [54] as a multilevel pulse excitation for multi-scroll generation, where the number of scrolls increases with increasing these levels. It was applied to three self-excited chaotic systems with double-scroll attractors, where the signal was added to one of the chaotic equations instead of a state variable. The same multilevel signal approach was utilized in [55], but for the three state variables simultaneously, to generate multi-directional multi-scroll attractors. The method was validated for a very simple Sprott system and Chua’s circuit in [55] and more systems in [56, 57]. Particularly for Sprott C system in [57], the authors suggested converting such non-autonomous chaotic systems to autonomous ones through defining time as an additional state variable and presented the consequent analysis. They showed that, theoretically, constant offset boosting changes the distribution of equilibria keeping the chaotic dynamics, i.e., eigenvalues, stability and Lyapunov exponents. On the other hand, dynamic offset boosting can result in systems with no equilibria; not only converting the system to be autonomous, but also converting its attractor type from self-excited to hidden. Recently, [26] extended the idea to chaotic systems with hidden attractors. The authors utilized a multilevel signal as the offset parameter to generate multi-scrolls. This composite multilevel signal is constructed by applying a sigmoid function, instead of signum as in [25], on a sinusoidal function of time. In this set of researches, except [55], neither the conditions on the state variable or chaotic equation to add the multilevel signal nor the limiting conditions were discussed.

All these controllable systems with offset boosting move the strange attractor along a line, a lattice or a grid. Alternatively, [58] proposed a novel idea that moves the equilibrium points of a given system and, hence, its strange attractor along a curve. The utilized system was a four-wing modified Lorenz attractor formed by a multilevel pulse signal as a coefficient for xy term, which is the same composite function [25]. An offset transformation is used to simply move state variables and, hence, equilibrium points and attractor’s origin point, to new coordinate points, on condition that these points lie on a given curve. This offset is applied to two or three state variables according to the required propagation directions. Hence, the proposed approach represents a non-autonomous dynamic offset control. The procedure was validated to produce oval-shaped (ellipse), circular, piecewise-linear (triangular), heart-shaped (two ellipses), and cube-shaped distributed attractors. This should not be confused with being interested in the shape of equilibrium points curve only. The later approach does not modify an existing attractor but construct novel system equations resulting in a new strange attractor as will be discussed in Subsection 2.2.3. Other applications of composite functions and transformations, yet, of state variables instead of time, in proposing novel and modified chaotic attractors are soon reviewed in Subsection 2.2.4.

Sometimes, both amplitude and offset control can be referred to as polarity control

when the polarity of the chaotic signal is the main concern of analog implementations. Amplitude control with negative scales has also been referred to as phase reversal, mirror image versions, or reflections. Frequency control was also presented [59] by rescaling the independent time variable or index in case of discretized solutions. Other works such as [60–63] presented systems with each of the state variables that are controllable in different ways, similar to [45]. These researches and others again emphasized the special characteristics required in the system equations to be capable of inserting such extra parameters without affecting the chaotic dynamics. The selected systems should exhibit the special features of amplitude control and/or offset boosting. As elaborated in [39–41, 49] and other papers, there is a possibility of different dynamical behaviors corresponding to different settings of the introduced parameters in most of these reviewed papers. Preserving the chaotic dynamics requires experimental adjustment of parameters and initial conditions. That is, the initial conditions in the state variables affected by amplitude control or offset boosting may need to be correspondingly adjusted to remain in the basin of attraction. Moreover, the authors of [64] referred to the process of state variables shifting or translation and similar changes in the coordinates as a self-reproducing system.

2.2.3 More Systems with a Variable/Infinite Number of Equilibrium Points

Several recent researches started referring to the systems formed by the previously reviewed techniques as systems with a variable or infinite number of equilibrium points. Whether they perform rescaling, reflection by negative scaling parameters or offset by additive parameters on the state variables, this affects the location of the equilibrium points and it becomes no longer fixed for a unique attractor. When the rescaling, reflection or offset is performed via a transformation, the new equilibrium points can be more clearly deduced. For instance, systems with offset parameters are described to have a line of equilibrium points. Moreover, they can be classified as another form of hidden attractors. Under the same classification, systems with closed and open curves of equilibria were also presented and are reviewed in this subsection. Most of these researches built their systems based on exhaustive computer search methods through chaos localization techniques. In such methods, chaotic behavior is quantified and detected against wide ranges of parameters and initial values using MLE or otherwise in assumed chaotic models with unknown parameters.

Several systems with closed curves of equilibrium points were presented in the past few years. Such curves include circle-shaped [65] and a square-shaped system modified from it through degree modification (linearization) [66], rounded-square-shaped [67], cloud-shaped [68], heart-shaped [69], axe-shaped [70], pear-shaped [71], three-leaved-clover flower-shaped [72], Boomerang-shaped [73], two circles of equilibrium points [74] and more. A generalization of [65] was presented in [75] that enables employing different nonlinear functions, which result in circular, ellipse or square-shaped equilibria. Some of these papers discussed the coexistence of multiple attractors, e.g., [65] showed how their proposed system possesses several attractors corresponding to different parameter ranges and/or initial conditions outside or inside the equilibrium curve. Although the strange attractors exhibit interesting and unique shapes [73], these researches barely observed or

constructed multi-scroll attractors literally from their proposed systems.

Meanwhile, systems with open curves of equilibrium points were also presented including piecewise linear (absolute) curve [76], exponential curve [77], line and hyperbolic curve [78], hyperbolic tangent curve [79] and hyperbolic sine curve [80]. Again, although the dynamic behaviors are interesting compared to conventional systems with finite countable equilibrium points, no multi-scroll attractors were observed in or constructed from the proposed systems.

In addition to all these chaotic systems, a hyper-chaotic system was constructed by a feedback controller to the classical Lorenz system [81]. It has a curve of equilibrium points and can display coexisting attractors with different types of dynamics. Twelve simple chaotic flows with surface equilibrium were converted to systems with surface equilibria through multiplying the right hand sides of the differential equations by a function of several variables [82].

Systems with closed or open curves of equilibria theoretically possess an infinite number of equilibrium points. Yet, being hidden attractors, the number of equilibrium points does not directly affect the number of scrolls. Hence, this technique is not generally considered as a method of multi-scroll generation. They are reviewed from the viewpoint of having infinite number of equilibrium points, but are not closely related to the techniques presented in the rest of the thesis. In fact, we are more interested in attractors size, shape and/or location control rather than the equilibrium points themselves.

2.2.4 Polarity and Degree Modification, Functions and Transformations

The previously discussed extra parameters approaches: amplitude control and offset boosting enabled the control of the size and location of the strange attractor, respectively. Yet, when these parameters are static, the number of scrolls is still fixed. When the parameters become dynamic, the chaotic system can yield more scrolls. No other modification to the terms of the chaotic equations and state variables, beside introducing extra additive and multiplicative parameters, was involved. For ideas with further modifications, we attempt to limit our review to papers related to amplitude control, offset boosting, non-autonomous parameters and coordinate transformations. Research works on multi-scroll and multi-wing generation methods briefly reviewed in Subsection 2.1.2.2 are too numerous, mostly employ non-autonomous methods, focus on their own objective of numerous scrolls generation and extend beyond our main topic.

In this subsection, we review the researches that modified the terms through applying functions to selected terms of the right hand side of the chaotic equations on the one hand and those that applied systematic coordinate transformations on the other hand. One of the earliest works on terms altering, degree modification and coordinate transformations was presented in [21]. Coordinate translation, i.e., offset, followed by absolute value function, i.e., polarity modification, were applied to three of the state variables of a hyperchaotic system resulting in a multi-wing attractor.

Unlike multiplicative parameters/coefficients as in [38], amplitude control through degree unification was presented in [14]. Two approaches were proposed: either by linearization of quadratic terms through replacing variables by signum functions of them, or raising the degree via multiplication by absolute value function. The method is limited

to systems with few nonlinear terms like the utilized Sprott B systems whose symmetry and amplitude control potential is clear. It requires caution when choosing initial values and the expected equilibrium points.

Quadratic terms in the form of a squared state variable were replaced by the multiplication of this state variable by its absolute value [19]. Each of the other state variables that appear only in one of the chaotic equations can be replaced by its absolute value minus an offset parameter all multiplied by a scaling parameter, resulting in coexisting attractors. Both the attractor size and location are controllable, yet, without multi-scroll generation.

Allocation of attractor by periodic functions was presented in [83], which uncovers another form of coexisting attractors or multistability that does not depend on offset parameters. Alternatively, it applies a scaling transformation followed by replacing the state variable by a bounded periodic function applied to it, e.g., sinusoidal. Periodicity allows having attractors in the vicinity of $x_0 + 2\pi i$, $i \in \{\dots, -2, -1, 0, 1, 2, \dots\}$ as well as x_0 . Similar ideas employing periodic functions were presented in [84, 85] for other chaotic system focusing on offset boostable state variables instead. A further generalization for hyperchaotic systems and criteria of periodic functions selection were presented in [86]. Applying periodic functions overcome the limiting conditions on systems with amplitude control and/or offset boosting potential still with the precautions on selecting initial values within the new basin of attraction. In these works [83–86], only attractor location control was presented without simultaneous attractors replication or multi-scroll generation.

Afterwards, [87] combined ideas from [21, 83–85], where piecewise nonlinearities, nested offset boosting and periodic functions were used for doubling the number of scrolls. The proposed offset boosting technique depends on modification of the chaotic equations by signum and/or absolute value functions of one of the state variables together with an offset parameter/booster. Nesting this technique can further yield redoubling of the number of scrolls. In addition, applying periodic functions to the other state variables through composition enables the generation of a lattice of scrolls, simultaneously, generating multi-scrolls.

The rotation transformation of chaotic systems was first presented in [88], where x is replaced by $(|x - x_0| + x_0)\cos(\theta) - (|z - z_0| + z_0)\sin(\theta)$ and z is replaced by $(|x - x_0| + x_0)\sin(\theta) + (|z - z_0| + z_0)\cos(\theta)$. The new chaotic equations of \dot{x} and \dot{z} are formed by a similar rotation transformation of the right hand sides of the original ones. Three generalization approaches via transformations were presented in [89] and validated for 1D grid multi-scroll Chua attractors (along x -axis). The first two approaches are closer to the conventional multi-directional multi-scroll generation via autonomous nonlinear signals with breakpoints than the non-autonomous parameter control we are interested in. The third approach is the one we are interested in as it performs a series of interesting and novel transformations. It applies offset, absolute value function and a rotation transformation (x - y) similar to [88]. The new chaotic equations are formed by a similar rotation transformation of the right hand sides of the original ones of $(\dot{x}$ and $\dot{y})$. The result of this transformation is then multiplied by a piecewise function of x or y , respectively, constructed from difference between shifted versions of an absolute value function. The turning points x_0 and y_0 were obtained by trial-and-error, where these turning points and the angle θ have fixed values throughout the simulation. The system was shown to exhibit a circular grid of multi-scroll attractors with symmetrical distribution. A very similar rotation transformation was applied in one of the approaches presented in [90].

An algorithm for 3D multi-wing attractors generation from systems with double-wing attractors was presented in [22]. The algorithm employed translation, reflection, absolute value function, followed by another translation along the x -axis direction. The number of scrolls was further enlarged by applying a series of mirror reflections using a product of signum functions. The algorithm is applicable to systems whose saddle-focus equilibria with index 2 lie on the plane $y = 0$, i.e., x -axis. For systems that do not satisfy this condition, a rotation transformation with a fixed angle is applied at first, e.g., $\theta = \pi/4$ is used to rotate Lorenz system's equilibria from $y = x$ to $y = 0$. Multi-directional grid of attractors were generated by translation of y and z state variables as well using staircase functions. The utilized functions are all autonomous functions of the state variables and closer to the conventional multi-directional multi-scroll generation via autonomous nonlinear signals with breakpoints than the non-autonomous parameter control we are interested in. Yet, we are particularly interested in translation, reflection, absolute value function and rotation transformation. The authors describe the algorithm as a convenient one because it avoids the troublesome parameters setting compared with other common even-symmetrical switching function methods.

Besides applying functions directly to the state variables and systematic coordinate transformations, another approach of novel attractors generation employed complex transformations in chaotic systems to increase the number of scrolls/wings [22, 90, 91]. Firstly, a methodology of constructing chaotic systems with any preassigned number of equilibria, not scrolls, from a system with one stable equilibrium was presented in [92]. The methodology depends on additional symmetry across arbitrary axes through coordinate transformations $(x + iz)^n = (u + iw)$ such that for each point in the new coordinates $u - v - w$, there are n symmetric points in the original coordinates $x - y - z$ and, hence, n equilibria. Yet, this does not affect the number of scrolls in such a system with hidden attractor and the obtained attractors resemble those of Section 2.2.3. An approach quite similar to [92] was adopted in [91], which performed the transformation in $x - y$ instead of $x - z$ and preceded by a static offset similar to that in [21]. The approach was extended in [91] with the objective of attractor location control. The idea of scaling and periodic functions, which was previously presented by the same authors in [83], was employed as a systematic coordinate transformation applied to the state variable on both sides of the chaotic equation not only on the right side. Yet, no comparison between [83, 91] or reason behind the modification were included.

Another approach presented in [90] depends on binary and ternary fractal transformation processes. It is a complex transformation similar to [91, 92], yet, inspired from fractal complex iterative maps iterated in reverse time direction. Most importantly, this transformation is applied as a post-processing to the given chaotic signals. Other works focused solely on fractal transformations [93–97] and can be similarly understood.

2.2.5 Chaotic Systems in Spherical Coordinates

This is a very novel approach that has recently been researched and few works were published [98–100]. The systems' equations are rather complicated with much linear and nonlinear terms. Systems' equations construction does not follow an analytical approach. Alternatively, the authors include different combinations of linear and nonlinear terms with unknown parameters, then experimentally search the parameter space for fixed values

that generate chaos, i.e., same exhaustive search techniques previously mentioned. The original system model and construction procedure are not explicitly given, but referred to [44, 59] ensuring the presence of equilibrium points.

2.2.6 Classification of the Reviewed Papers

From the previous subsections, it can be concluded that the research on generalization and control of chaotic systems using extra parameters and transformations is recent, branched and the attempts are still discrete and not fully connected. Besides Sprott’s works including a static scaling parameter in 2000, Fig. 2.1 shows a stacked bar graph, based on the reviewed journal articles, of the number of publications in the period 2010-end of May 2020 with their topics given in the legend. The contribution of the relatively large number of papers on static amplitude control and offset boosting techniques was not exactly in this area of research. They just showed the amplitude and offset control potential of their proposed systems as a minor part of their work. Most of the works on static offset control combined it with amplitude and frequency control. The papers on dynamic offset boosting are all centered on moving the strange attractor a long line, lattice or grid except [58], which moves it a long a curve. Papers utilizing polarity and degree modification, as well as periodic functions, often included static amplitude or offset control too. While “nested functions” is used to describe papers that applied nested degree modification, offset and periodic functions for multi-wing generation, “nested transformations” is used to describe papers that depended on cascade systematic coordinate transformations.

The figure does not show four papers in 2014-2017 on multi-stability identification using amplitude and offset control as tools. In addition, it does not include the works reviewed in Subsection 2.2.3, which were published in 2015-2019, as they are the least related to the work presented in the rest of the thesis as previously discussed. While most of the reviewed papers start from a given chaotic system and then apply their modifications, only the systems with open curves, closed curves or surfaces of equilibria in Subsection 2.2.3 and the systems in the spherical coordinate system are built from scratch

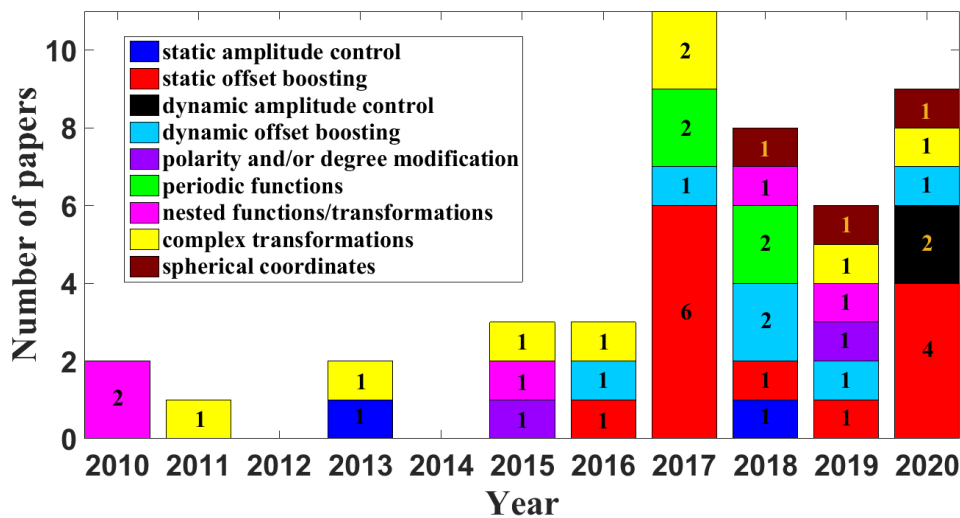


Figure 2.1: Classification of the reviewed paper and their publication years.

using assumed models and exhaustive search for parameter values.

It can be inferred from Fig. 2.1 that most of the papers appeared in the period 2017-present, i.e., concurrent with the work presented in this thesis. Some control features such as using multilevel pulse signals for dynamic amplitude control [23,43] and offset boosting of hidden strange attractors [26] were published in 2020, i.e., only months ago. Although the recent few years witnessed an increase in the number and diversity of publications relevant to the topic, the propagation and evolution of new research ideas among research groups is not rapid enough and the number of contributors is limited. For example, 4 and another 2 out of the 8 publications on complex transformations belong to the same research groups, respectively. There are common coauthors among the three papers on chaotic systems in spherical coordinates as well. Four out of 6 papers on dynamic offset boosting and 1 out of 2 papers on dynamic amplitude control also have common names in their authors list. In addition, Li and Sprott coauthored 3 out of the 4 papers utilizing periodic functions and contributed in proposing systems utilizing degree modification and nested functions. Li and Sprott also coauthored the leading researches on amplitude control and offset boosting, which presented these terminologies in the field of chaos control.

2.3 Chaotic Synchronization and Encryption Applications

The papers reviewed in the previous section barely discussed any applications of their proposed continuous chaotic systems or their performance as PRNGs or in encryption schemes [23, 56, 58]. Meanwhile, separate image encryption research was ongoing [101–104] based on discrete-time chaotic maps including some transformations as separate encryption stages.

Chaotic synchronization has been utilized in data encryption and secure communication applications in different forms. For secure communication applications, the message or information signal is embedded in a carrier signal (one or more of the chaotic outputs) through modulation. Embedding is either performed in the dynamical equations [105–110] or applied as a post processing through addition [111–118] or multiplication [119]. The former method imposes conditions on the amplitudes of the message and hence not always suitable, especially for digital encoded signals such as images. Integer-order chaotic systems synchronization has been applied for image encryption [70, 120–124, 124–127]. Due to the more complex behaviors, fractional-order chaotic synchronization is a more challenging task. Although fewer works utilized fractional-order chaotic systems, they have flourished recently and more papers appeared presenting fractional-order chaotic systems synchronization-dependent encryption. Secure communication of simple signals [128] and voice signals [129, 130] were presented based on fractional-order chaotic systems synchronization. Furthermore, researches in image encryption field include [131–137].

2.4 Implementation of Chaotic Systems

Software and hardware digital realizations of chaotic systems are increasingly required for this wide spectrum of applications. Software encryption schemes [11], digital hardware

realizations on FPGAs [138–140] and analog realizations based on transistor level [141] or different building blocks [142] were presented.

2.4.1 Digitally Implemented Generalized Chaotic Systems

The accompanying complicated simulation and implementation is the main challenge facing these different approaches to novel and generalized chaotic systems formation [143]. While some of the papers reviewed in this chapter presented analog circuit simulations or implementations of their proposed generalized controllable chaotic systems [14, 22, 23, 26, 35, 57] and most of the systems with closed curve of equilibrium points, fewer works presented digital implementations [77, 89, 90]. In both types of implementations, very few researches included realization of transcendental elementary functions such as exponential [77] and hyperbolic functions [79, 80], while almost no papers included trigonometric functions. In order that chaotic systems take part in real-world applications, implementations that generate the chaotic signal are required rather than the computer-simulated numerical form [34, 144]. Digital hardware FPGA, especially when using fixed-point registers, provide many advantages such as: easy design, programmability, fast prototyping, reduced hardware cost, high speed, noise immunity, reliability, reconfigurability and reproducibility. These advantages strongly encourages utilizing FPGAs for fractional-order chaotic systems implementation [34] as long as accuracy and dynamical degradation limitations are considered in numerical approximations, bit representation and precision decisions [34].

2.4.2 Hidden Potential of Implementation Sensitivity

For continuous-time systems, discretization techniques employ a time step such that the system becomes suitable for digital implementation. Various numerical techniques are available to perform discretization. In addition, there are various alternatives for implementations including floating-point versus fixed-point arithmetic, variable versus fixed precision, the number of bits and the order in which the sequence of operations takes place.

Implementation sensitivity of chaotic systems is rarely considered and under-utilized in the literature compared to the widely discussed sensitivities to initial conditions and parameter variation. The effect of numerical solution accuracy on the digital implementation of differential chaos generators was studied and compared for four chaotic systems in [145] using Euler, mid-point, and Runge-Kutta fourth order numerical techniques. Using randomness measures, it was found that Euler implementations yield better chaotic responses because the numerical solution error adds an extra nonlinearity to the chaotic system. Effect of precision on the chaotic behavior of digitally implemented systems was studied in [146] setting precision thresholds below which MLE is not positive and, hence, the system is not chaotic. Precision and order of execution effects were studied in [147] for the logistic map. The period of the generated sequence was found to be affected and the changes due to varying precision can not always be expected owing to the increased sensitivity, where the map could even be drifted away from chaotic behavior. Interval arithmetic was also applied to simulation of dynamical systems [148]. The finite precision error between different natural interval extensions of Chua's circuit was even applied for image encryption [149]. Simple mathematical properties such as algebraic associativity

do not hold in digital computation environments due to rounding errors, let alone several factors that vary among such environments, as will be discussed in Chapter 3.

Having reviewed the applications and implementations linked to the thesis topic, the following chapters explain our proposed approaches to the generalization and control of chaotic systems using extra parameters and affine transformations with the accompanying analysis, implementation and applications. The possibility of nonautonomous control of autonomous chaotic systems through the proposed approaches is discussed and utilized in several applications.

Chapter 3: Controllable Jerk-Based Attractors and Reproducibility

This chapter focuses on simple jerk-based chaotic systems and discrete maps and utilizes them in the first proposed generalization approach. In addition, in the next chapters, more generalized and controllable chaotic equations will be presented, implemented in software and sometimes hardware. The provided applications rely on parameters and initial conditions as sensitivity sources, e.g., in encryption key design. However, there is an underutilized implementation sensitivity property in chaotic systems, which is also focused on in this chapter.

The first generalization and control approach, extra parameters, is inspired by [36]. Why should we bother designing a nonlinear function with scaling parameter for jerk-based chaotic systems while we already have numerous research on generalized discrete maps? The nonlinear function can be directly set as these maps and the resulting systems are expected to possess similar controllable properties. In this section, we validate this idea by proposing two systems based on the jerk-equation and discrete maps with scaling parameters in the form of piece-wise nonlinearity and quadratic nonlinearity. The effects of different parameters on the type of the response of each system are studied. Time series, phase portraits, bifurcation diagrams and MLE are investigated against all system parameters. It is shown that the role of each parameter is related to its role in the corresponding case of discrete maps. Possibility of fractional-order extension is also assessed [8, 9].

3.1 Two Modified Non-Linearities

This subsection reviews generalized forms of two well-known discrete-time chaotic maps, which will be utilized as the nonlinear function of the jerk-equation. The two generalizations are the scaled tent map with piece-wise nonlinearity and the scaled logistic map with quadratic nonlinearity. The complete bifurcation diagram using negatively valued parameters in tent and logistic maps has been recently analyzed in [150, 151]. The new parameter range provides a controlling capability resulting in a wider output range.

3.1.1 Piece-Wise Nonlinearity: Scaled Tent Map

Scaled tent map [152] with piece-wise nonlinearity is given by:

$$f(x) = \begin{cases} \mu \operatorname{sgn}(b)x, & x \leq \frac{a}{b+\operatorname{sgn}(b)} \\ \mu(a-bx), & x > \frac{a}{b+\operatorname{sgn}(b)} \end{cases}, \quad (3.1)$$

where μ , a and b are parameters, $a \in R^+$, $b \in R - \{0\}$ and $\operatorname{sgn}(b)$ is the sign or signum that extracts the sign of b as follows:

$$\operatorname{sgn}(b) = \begin{cases} -1, & b < 0 \\ 0, & b = 0 \\ 1, & b > 0 \end{cases} \quad (3.2)$$

The forms of the scaled tent map can be classified into positive, mostly positive, negative, and mostly negative maps named after the sign of the obtained output range. Figure 3.1 shows the graphs of the map equation for the first two forms, in which $b > 0$, expressing the output ranges in terms of the map parameters.

For a discrete-time map represented as a recurrence relation, the bifurcation diagram is a plot of its steady state solution versus the control parameter(s) of the map. Plotting bifurcation diagrams is one of the approaches towards identifying the effective range of parameters through which the system exhibits bounded responses. In addition, it is used to classify the corresponding qualitative type of the post-transient solution into stable, periodic or chaotic. Figure 3.2 shows the general schematic of the bidirectional bifurcation diagram of the scaled tent map, which changes its shape as the parameter b exceeds 1. The main bifurcation points and the ranges of the parameter μ and the output x are also given in Fig. 3.2. From Fig. 3.2, it can also be inferred that the effective range of the parameter μ , in which the output is bounded, depends on the scaling parameter b in an inverse proportionality relation. In addition, the output range depends on both scaling parameters, where it widens as the value of the parameter a increases and/or the value of the parameter b decreases. These effects can be further validated by the three-dimensional snapshots of bifurcation diagrams against the main system parameter μ for different values of the scaling parameters a and b , which are shown in Figs. 3.3(a) and (b), respectively.

3.1.2 Quadratic Nonlinearity: Scaled Logistic Map

Similarly, scaled logistic map [151] with quadratic nonlinearity is given by:

$$f(x) = \mu \operatorname{sgn}(b)x(a - bx), \quad (3.3)$$

resulting in four forms similar to the scaled tent map. Figures 3.4 shows two map versions and Fig. 3.5 shows their bidirectional bifurcation diagrams. The dependence of the range of the output x on the scaling parameters is similar to the scaled tent map. However, the effective range of the parameter μ depends on the scaling parameter a in an inverse proportionality relation. Bifurcation diagrams against the scaling parameters and more detailed analyses of the different aspects of the scaled tent and logistic maps can be found in [151, 152].

3.2 Generalized Controllable Jerk-Based Systems Using Extra Parameters

Substituting either the scaled tent map (3.1) or the scaled logistic map (3.3) in the jerk-system

$$\ddot{x} + r\dot{x} + \dot{x} = f(x) \quad (3.4)$$

of [36] as $f(x)$ yields the piece-wise nonlinearity system and the quadratic nonlinearity system, respectively. The systems are solved numerically using Euler technique as follows:

$$\begin{aligned} x_{i+1} &= x_i + h(y_i), \\ y_{i+1} &= y_i + h(z_i), \\ z_{i+1} &= z_i + h(-r z_i - y_i + f(x_i)). \end{aligned} \quad (3.5)$$

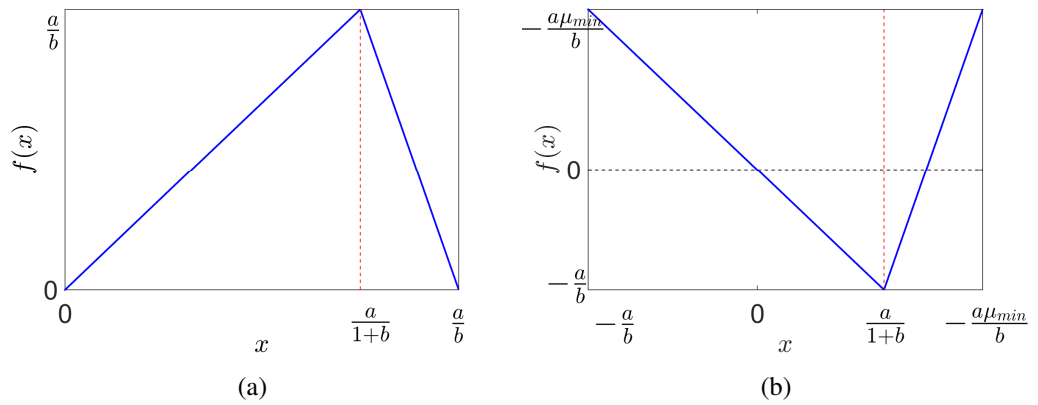


Figure 3.1: Scaled (a) positive and (b) mostly positive tent maps, where $\mu_{min} = -\left(1 + \frac{1}{b}\right)$.

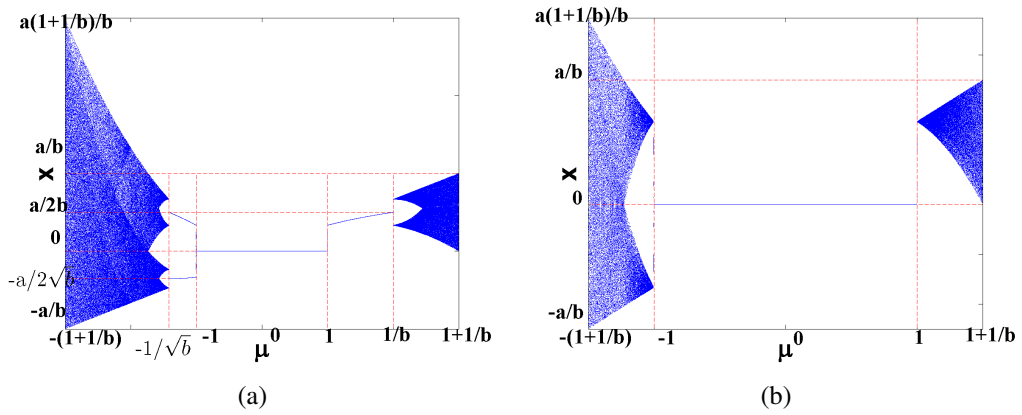


Figure 3.2: Generic bifurcations of the scaled tent map in both sides of μ (a) $b < 1$, (b) $b > 1$.

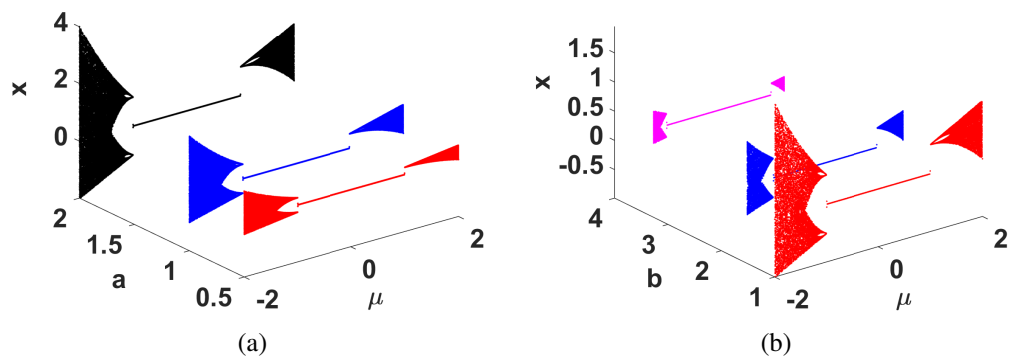


Figure 3.3: Bifurcations of the scaled tent map at (a) $b = 1$ and $a = \{0.5, 1, 2\}$ and (b) $a = 1$ and $b = \{1, 2, 4\}$.

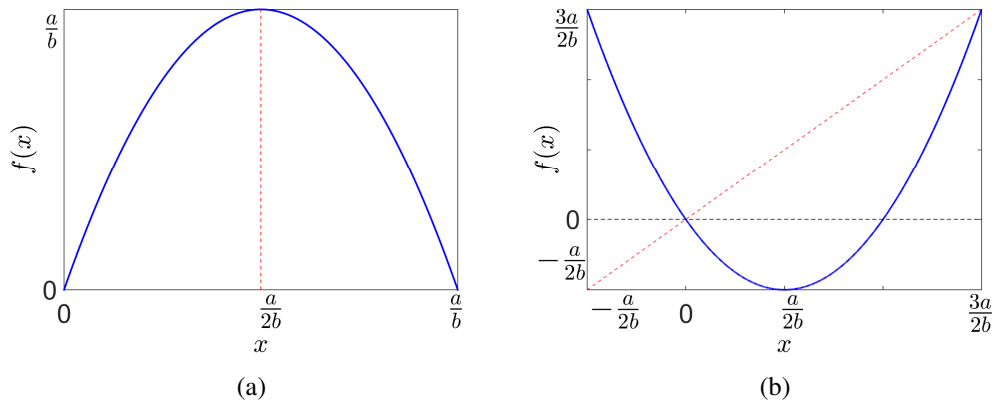


Figure 3.4: Scaled (a) positive and (b) mostly positive logistic maps.

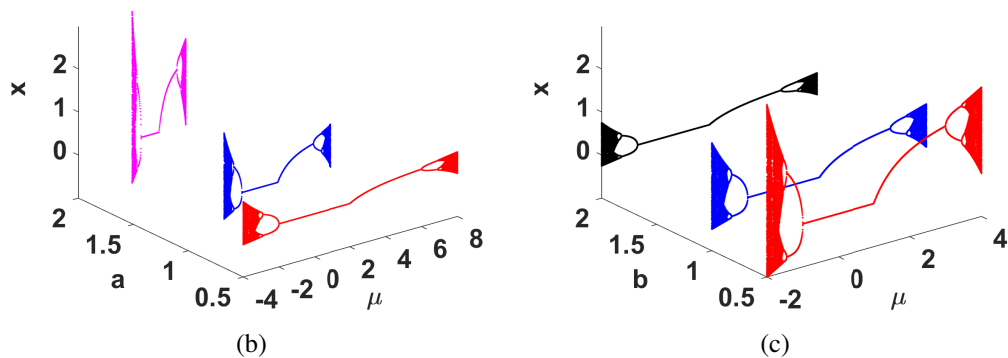
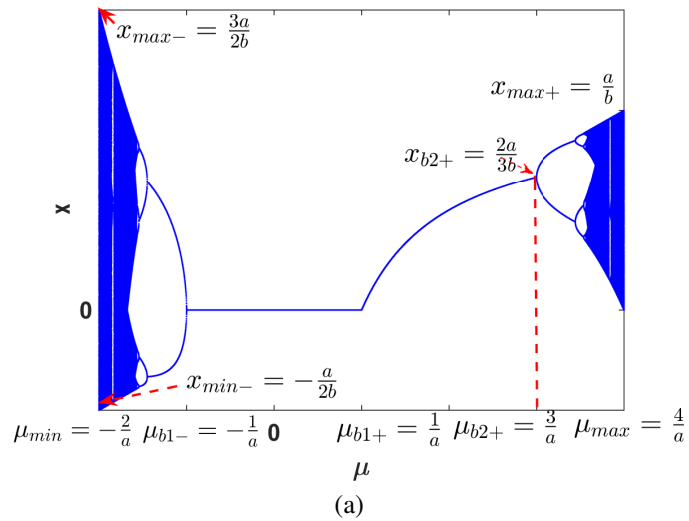


Figure 3.5: (a) Generic bifurcations of the scaled logistic map and numerical examples at (b) $b = 1$ and $a = \{0.5, 1, 2\}$ and (c) $a = 1$ and $b = \{0.5, 1, 2\}$.

For both systems, the equations, attractor diagrams in the three-dimensional space and different projections, and LEs at the specified parameter values are shown in Table 3.1.

Table 3.1: Proposed systems and their properties

System	Piece-wise nonlinearity	Quadratic nonlinearity
Nonlinearity	$f(x) = \begin{cases} \mu \operatorname{sgn}(b)x, & x \leq x_k \\ \mu(a - bx), & x > x_k \end{cases}$ $x_k = \frac{a}{b + \operatorname{sgn}(b)}$	$f(x) = \mu \operatorname{sgn}(b)x(a - bx)$
Parameter Values	$\mu = 1$ $a = 1$ $b = 1$ $r = 0.6$	$\mu = 1$ $a = 1$ $b = 1$ $r = 0.5$
Attractor Diagram		
LEs	(0.038, 0, -0.64)	(0.092, 0, -0.59)

The attractor diagrams and the projections of the two systems resemble those of the two systems with similar nonlinearities which were introduced in [36]. However, they do not exhibit the same ranges of the three state space variables x , y and z . The obtained values for LEs for the two systems are in the same range obtained for the similar systems [36]. Both systems belong to the dissipative systems category because the sum of the three LEs for each system is negative [2]. Moreover, they exhibit chaotic strange attractors since the MLE is finite positive.

The equilibrium points are $(x^*, 0, 0)$, where $x^* = \{x|f(x) = 0\}$, and yields $x^* = 0, a/b$ for both forms of $f(x)$. Hence, there are two equilibrium points $(0, 0, 0)$ and $(a/b, 0, 0)$. Hence, the sign of the x -coordinate of the nontrivial equilibrium point, x^* , depends on the sign of the parameter b and some consequences of this property will be discussed in Subsection 3.2.3.

For the two presented systems, the type of response obtained at the different values of the four parameters (r, μ, a, b) and the sensitivity to parameter variation need to be studied. This study can be carried out in a discrete manner, where the phase portrait and the time series are plotted at chosen values of each parameter fixing the other parameters. Continuous bifurcation diagrams provide a better representation of the systems behavior, which is also more consistent with the continuous description where parameters vary in narrow steps. Figure 3.6 shows the procedure of generating the bifurcation diagram versus a chosen parameter for continuous chaotic systems through plotting the value of x every time it reaches a local maximum by sampling the time series as shown in Fig. 3.6. The resulting bifurcation diagram reveals whether the time series is stable, periodic or chaotic similar to the discrete case.

As previously detailed, LEs measure the sensitivity to initial conditions through the exponential divergence of nearby trajectories. MLE exhibits finite positive values for parameter ranges which correspond to chaotic behavior. To further indicate which parameter ranges exhibit chaotic behavior, MLE values are plotted against each studied parameter.

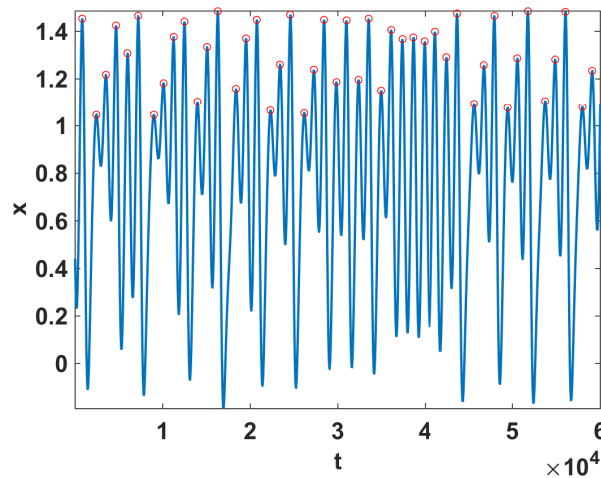


Figure 3.6: Time series sampling to decide the type of system response.

3.2.1 Sensitivity to Main System Parameters

To study the effect of parameters r and μ , the scaling parameters a and b are kept constant $a = b = 1$ corresponding to the unity scaling case. For the piece-wise nonlinearity system, Tables 3.2 and 3.3 show its responses at different values of r and μ , respectively. The post-transient attractor diagrams, time series, and the obtained response type at different values of the parameter r within a chosen interval are plotted in Table 3.2 fixing the other parameter values to 1. The value of r is fixed at 0.6 to study responses at different values of the parameter μ , which are given in Table 3.3. Negative values of μ can be studied similarly.

Table 3.2: Responses against the parameter r at $a = b = \mu = 1$

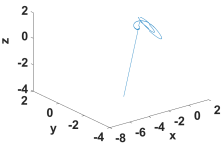
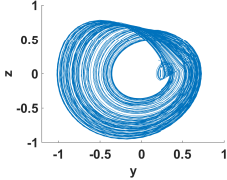
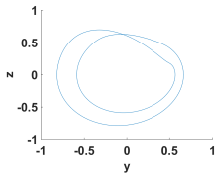
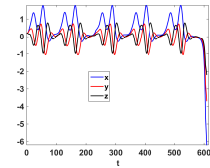
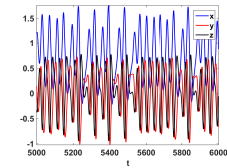
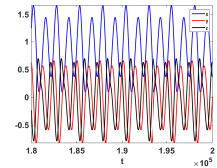
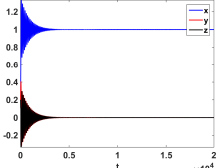
$r = 0.55$	$r = 0.57$	$r = 0.7$	$r = 1.1$
			Single point
			
Divergent	Chaotic	Periodic	Stable

Table 3.3: Responses against the parameter μ at $a = b = 1$ and $r = 0.6$

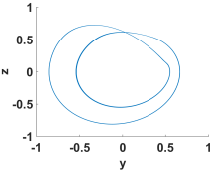
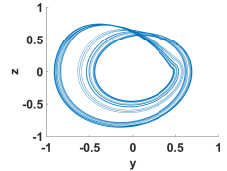
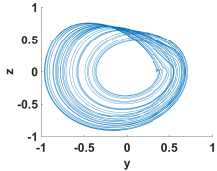
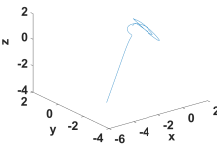
$\mu = 0.9$	$\mu = 0.95$	$\mu = 1$	$\mu = 1.1$
			
Periodic	Chaotic	Chaotic	Divergent

Figure 3.7 shows the bifurcation diagrams of both systems versus the system parameter r . For both systems, at $\mu = a = b = 1$, chaotic behavior is reported starting at a critical value of r , below which no bounded responses can be found and the solution diverges. A series of reverse bifurcations from the chaotic state to periodic orbits is noticed as the value of r increases, then stable responses prevail. The results discussed earlier are further indicated by MLE plots, which appear below each bifurcation diagram. MLE exhibits finite positive values for ranges of r which correspond to chaotic behavior, whereas it is negative in the regions of stable solution. It roughly equals zero for ranges of r which correspond to periodic responses.

Fixing r at 0.6 for the piece-wise nonlinearity system and 0.5 for the quadratic non-linearity system and studying the effect of μ yields the diagrams shown in Table 3.4. Bounded responses are reported when the value of the parameter μ belongs to a given interval, where around the middle of the interval, stable responses are obtained. Then, the response type changes gradually to periodic in a series of period doubling bifurcations as $|\mu|$ increases. Afterwards, the response becomes chaotic as μ approaches the lower and upper bounds. The possibility of bounded responses and the generation of chaotic sequences at both positive and negative values of μ in a double sided bifurcation are

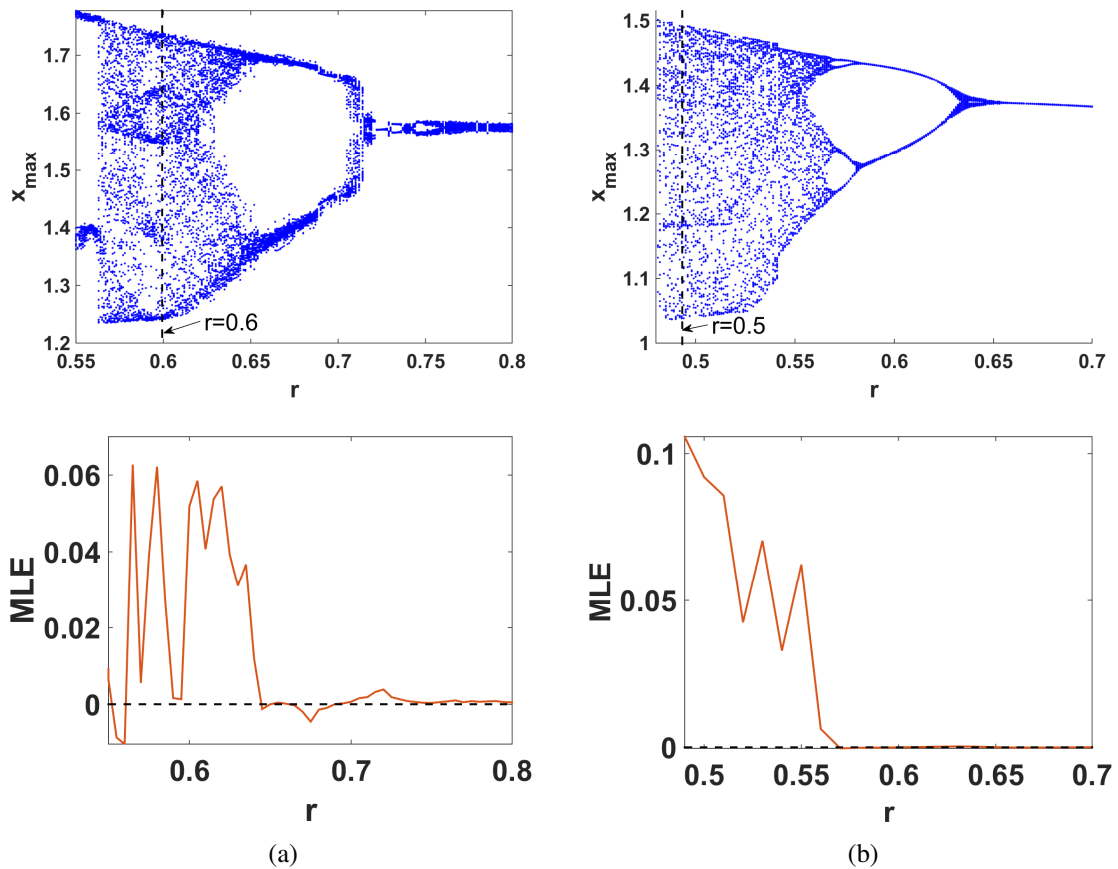
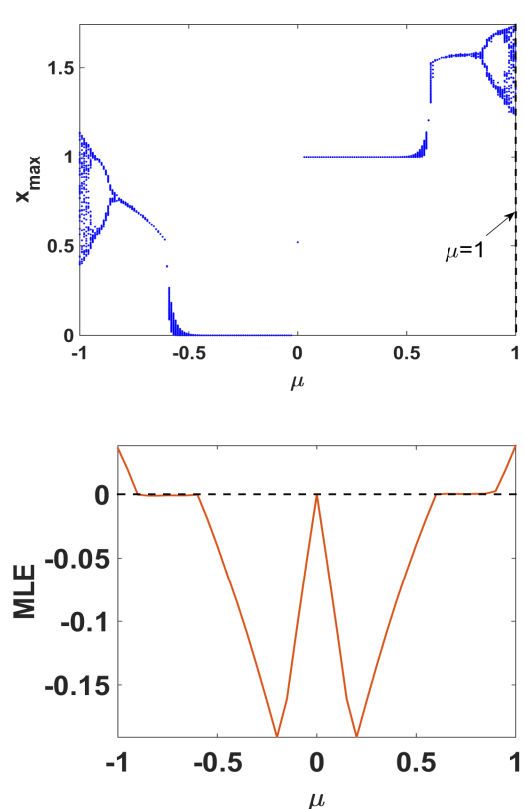
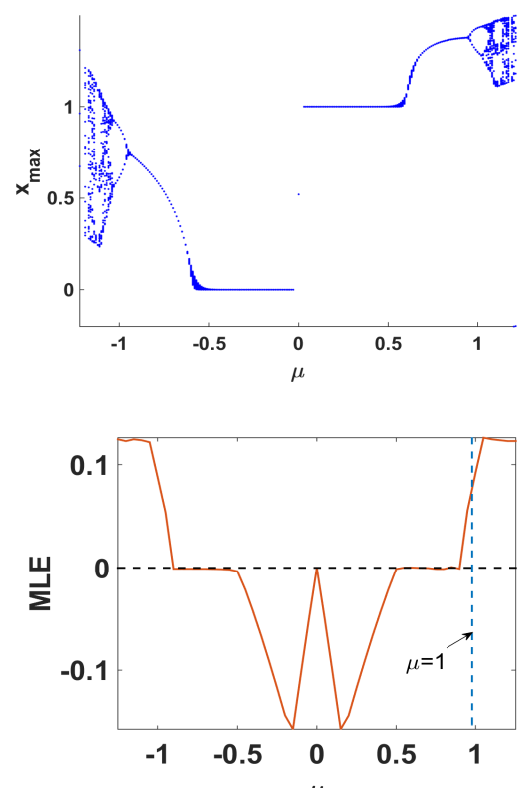


Figure 3.7: Bifurcation diagram and MLE against the parameter r for (a) the piece-wise nonlinearity system at $\mu = a = b = 1$ and (b) the quadratic non-linearity system at $\mu = a = b = 1$.

Table 3.4: Summary of the sensitivity to the system parameter μ and the similarities with the discrete scaled tent and logistic maps

	Bifurcation and MLE	Properties
Piece-wise nonlinearity	 <p>The top plot shows the maximum value of the system, x_{\max}, as a function of the parameter μ. The x-axis ranges from -1 to 1, and the y-axis ranges from 0 to 1.5. The plot shows a blue curve that is zero for $\mu \in [-0.5, 0]$ and increases from 0 to 1 for $\mu \in [0, 1]$. There are blue dots representing the system's state for $\mu < -0.5$ and $\mu > 0.5$. The bottom plot shows the Maximum Lyapunov Exponent (MLE) as a function of μ. The x-axis ranges from -1 to 1, and the y-axis ranges from -0.15 to 0. The MLE is zero for $\mu \in [-0.5, 0]$ and $\mu \in [0.5, 1]$, and negative for $\mu \in [0, 0.5]$. There are two sharp negative peaks at $\mu \approx \pm 0.25$.</p>	<p>Properties</p> <ul style="list-style-type: none"> - Double sided bifurcations versus μ. - Bounded responses are reported in the range $\mu \in [-1, 1]$. - Period doubling bifurcation towards chaos as μ increases.
Quadratic nonlinearity	 <p>The top plot shows the maximum value of the system, x_{\max}, as a function of the parameter μ. The x-axis ranges from -1 to 1, and the y-axis ranges from 0 to 1.5. The plot shows a blue curve that is zero for $\mu \in [-0.5, 0]$ and increases from 0 to 1 for $\mu \in [0, 1]$. There are blue dots representing the system's state for $\mu < -0.5$ and $\mu > 0.5$. The bottom plot shows the Maximum Lyapunov Exponent (MLE) as a function of μ. The x-axis ranges from -1 to 1, and the y-axis ranges from -0.1 to 0.1. The MLE is zero for $\mu \in [-0.5, 0]$ and $\mu \in [0.5, 1]$, and negative for $\mu \in [0, 0.5]$. There are two sharp negative peaks at $\mu \approx \pm 0.25$. A vertical dashed line is drawn at $\mu = 1$.</p>	<ul style="list-style-type: none"> - Almost similar except for the range, which is wider in this case.

analogous to the behavior in the discrete domain [151, 152].

3.2.2 Sensitivity to Scaling Parameters

This section studies the effects of scaling parameters a and b on the system responses. For the piece-wise nonlinearity system, Table 3.5 shows the responses at different values of the parameter b , which was noticed to be related to the variation of the parameter μ . In addition, Table 3.6 shows the continuous bifurcation diagrams and MLE values against both scaling parameters a and b . The response type does not change as the value of the parameter a increases. The response is chaotic for almost all values of a , where the range of the obtained solution gets wider as the value of a increases. MLE value is almost kept constant when varying the value of the parameter a . The parameter a acts only as a scaling parameter that widens the range of the solution, which can be further inferred from Fig. 3.8, where increasing the value of a increases the size of the attractor diagram. Table 3.6 shows that b is a signed parameter and that the system response exhibits double sided period doubling bifurcations when varying the value of b . In addition, the bifurcation diagram is limited by a value b_{max} controlled by the value of μ analogous to discrete scaled tent map case [152]. The corresponding MLE plot exhibits values that match the response types shown in the bifurcation diagram.

For the quadratic nonlinearity system, bifurcation diagrams and MLE versus the scaling parameters are shown in Table 3.7, which can be described similar to the piece-wise nonlinearity system. The effects of the scaling parameters a and b on the output range remain the same, where the range of the system output increases as a increases. In addition, the bifurcation diagram is limited by a value a_{max} controlled by the value of μ . The parameter b acts only as a scaling parameter, where as $|b|$ increases the output ranges and the attractor size decrease as shown in Fig. 3.9.

Figure 3.10(a) shows the dependence of the effective range of the parameter μ on the value of b . For $b > 0$, the range of μ that yields bounded responses decreases as b increases and sometimes no chaotic behavior can be reported. The dependence between μ and b resemble their dependence for discrete scaled tent map [152]. Figure 3.10(a) also shows

Table 3.5: Piece-wise nonlinearity system attractor diagrams and time series for different combinations of the parameters b and μ at $a = 1$ and $r = 0.6$

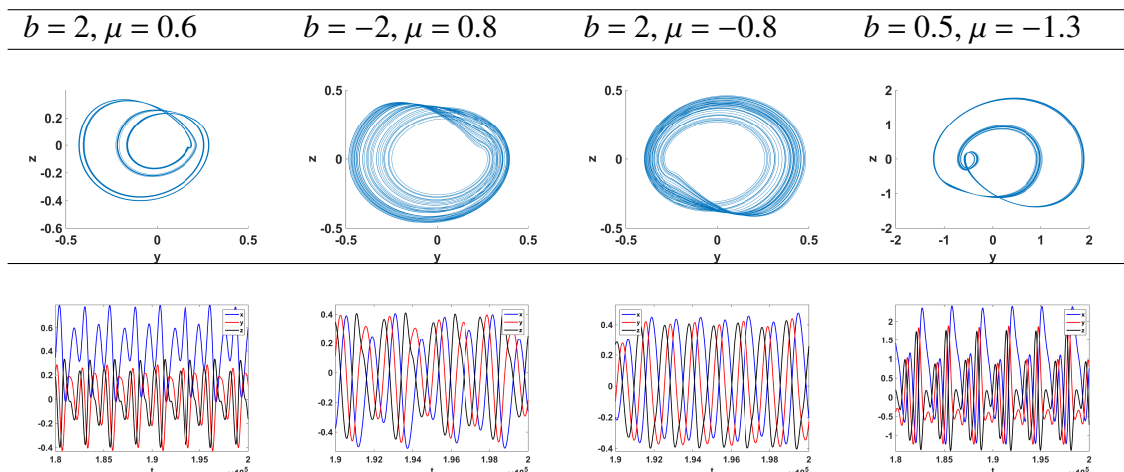
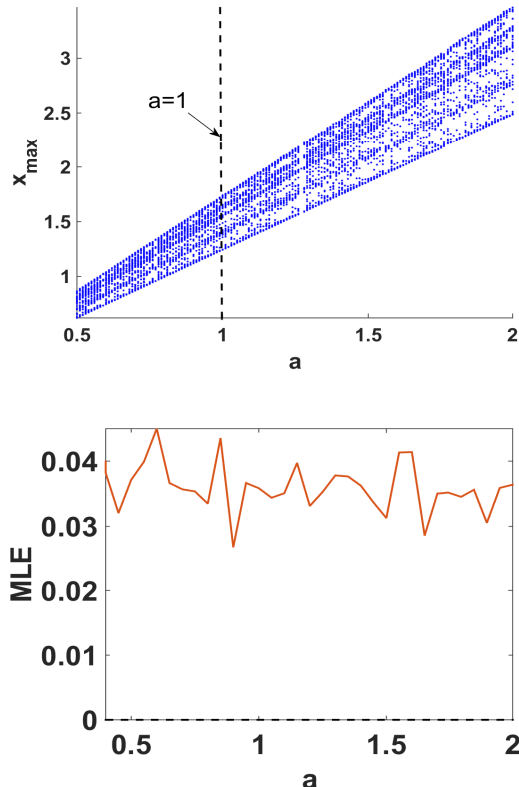
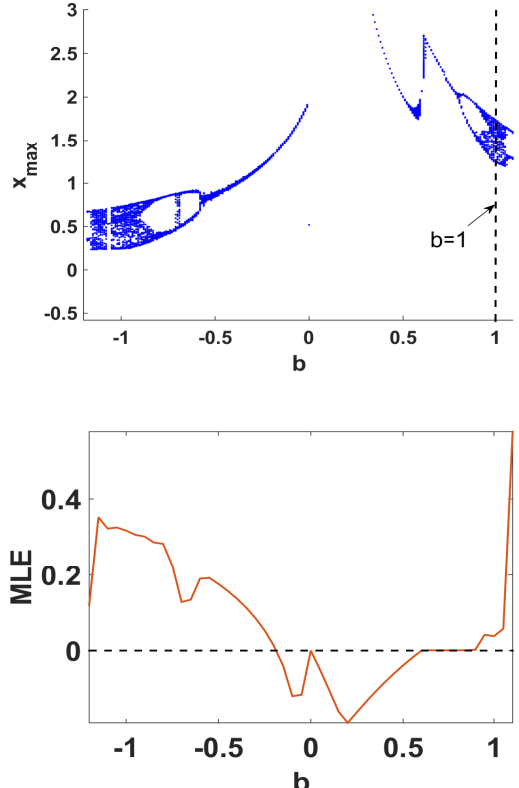
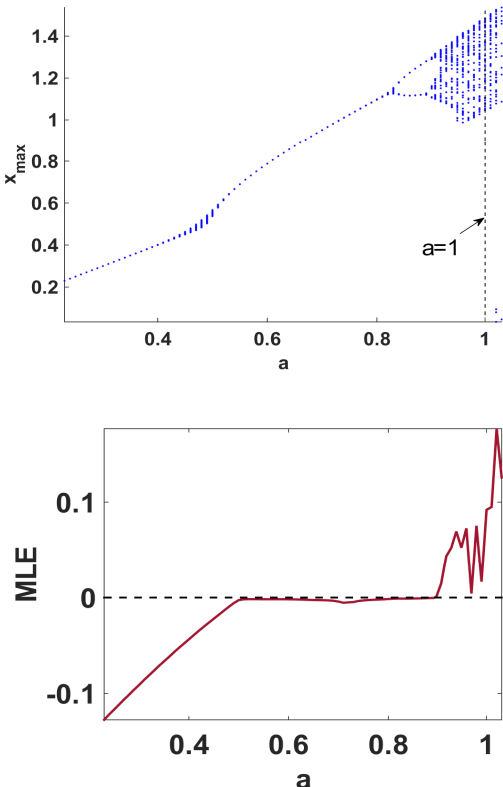
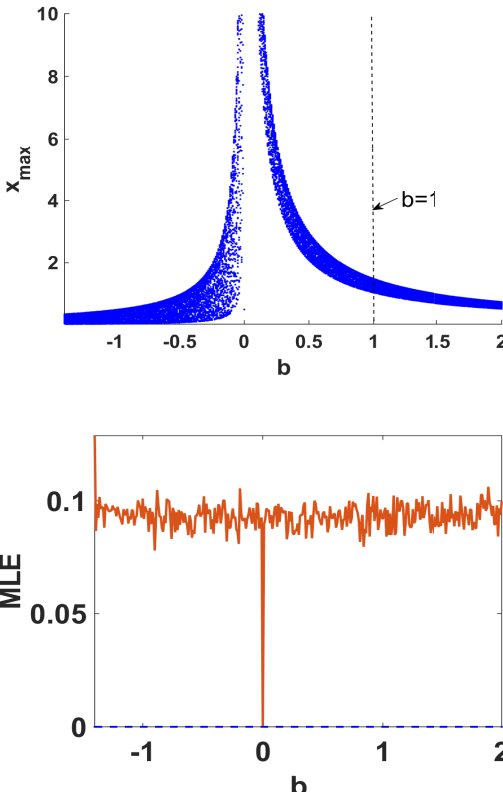


Table 3.6: Summary of the sensitivity of the piece-wise nonlinearity system to the scaling parameters a and b and the similarities with the discrete scaled tent map

Bifurcation and MLE	Properties
	<p>- The response is chaotic for almost all values of a, where the range of the obtained solution gets wider as the value of a increases. MLE values are positive and slightly vary versus a.</p> <p>- The range of μ decreases as b increases. The bifurcation diagram is limited by a value b_{max} controlled by the value of μ.</p> <p>- a acts only as a scaling parameter, where as a increases the output ranges and the size of the attractor diagram increases.</p>
	

- Double sided period doubling bifurcations towards chaos exist as $|b|$ increases.

Table 3.7: Summary of the sensitivity of the quadratic nonlinearity system to the scaling parameters a and b and the similarities with the discrete scaled logistic map

Bifurcation and MLE	Properties
 <p>The top plot shows a bifurcation diagram of x_{\max} versus a. The x-axis ranges from 0.4 to 1.0, and the y-axis ranges from 0.2 to 1.4. A vertical dashed line at $a=1$ indicates a transition to chaos. The bottom plot shows the Maximum Likelihood Estimate (MLE) versus a. The x-axis ranges from 0.4 to 1.0, and the y-axis ranges from -0.1 to 0.1. A horizontal dashed line is at MLE = 0. The MLE is zero for $a < 1$ and shows a sharp peak at $a=1$.</p>	<ul style="list-style-type: none"> - The effects of a and b differ from their effects on the first system. The roles are exchanged with respect to their effect on the solution type, bifurcation shape and range of the main system parameter μ. - Their effects on the output range remain the same, which increases as the absolute values of a increases and/or b decreases. - The range of μ decreases as a increases. The bifurcation diagram is limited by a value a_{\max} controlled by the value of μ.
 <p>The top plot shows a bifurcation diagram of x_{\max} versus b. The x-axis ranges from -1 to 2, and the y-axis ranges from 0 to 10. A vertical dashed line at $b=1$ is shown. The bottom plot shows the Maximum Likelihood Estimate (MLE) versus b. The x-axis ranges from -1 to 2, and the y-axis ranges from 0 to 0.1. A horizontal dashed line is at MLE = 0. The MLE is approximately 0.1 for $b \neq 0$ and has a sharp dip to 0 at $b=0$.</p>	<ul style="list-style-type: none"> - b acts only as a scaling parameter, where as b increases the output ranges and the attractor size decreases. - $b = 0$ is a vertical asymptote.

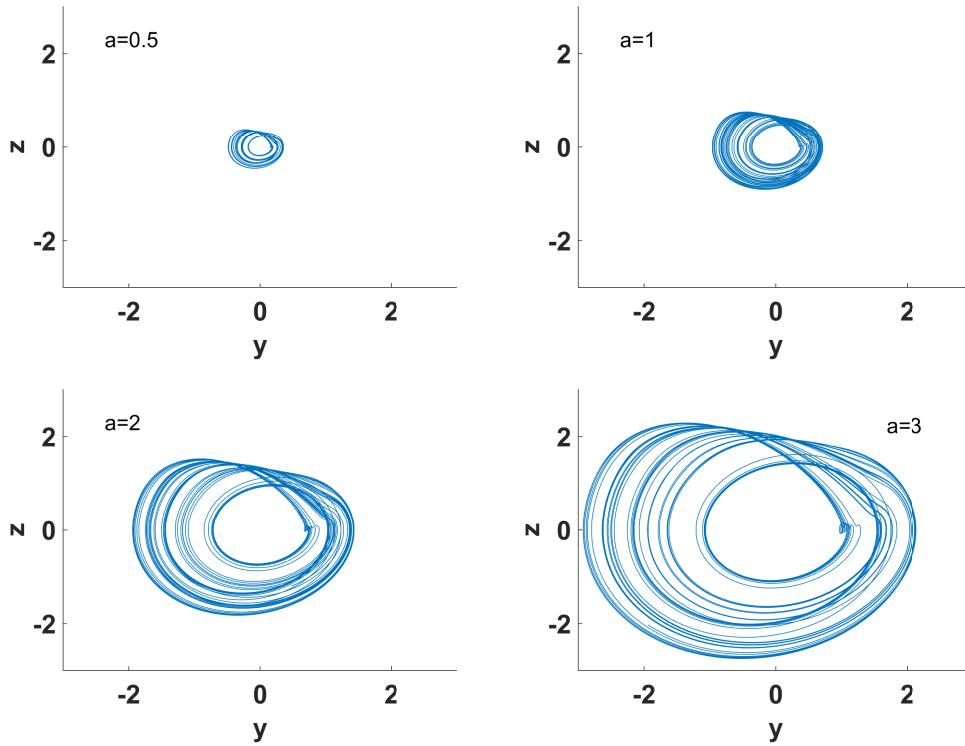


Figure 3.8: Scaled chaotic responses of the piece-wise nonlinearity system for different values of the parameter a at $b = \mu = 1$, $r = 0.6$.

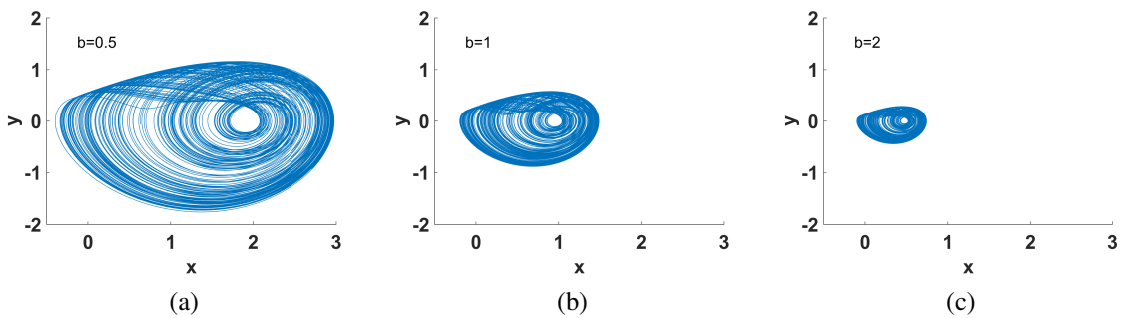


Figure 3.9: Scaled chaotic responses of the quadratic nonlinearity system for different values of the parameter b at $a = \mu = 1$ and $r = 0.5$.

that the range of the solution shrinks as the absolute value of b increases. On the other hand, the parameter a does not affect the range of μ . The effects of a and b on the quadratic nonlinearity system differ from their effects on the piece-wise nonlinearity system from the viewpoint of the effective range of μ , where the roles are exchanged. The effective range of μ is affected by the value of a analogous to the discrete scaled logistic map [151], where it decreases as a increases as shown in Fig. 3.10(b).

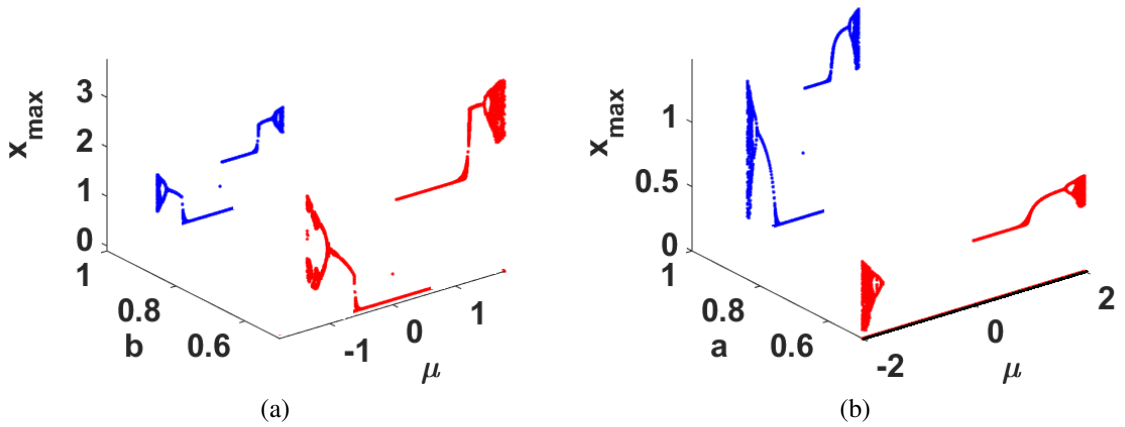


Figure 3.10: Bifurcation diagrams versus μ of (a) the piece-wise nonlinearity system at $b = \{0.5, 1\}$ and (b) the quadratic nonlinearity system at $a = \{0.5, 1\}$.

3.2.3 Self-Reproducing and Multi-Scroll Attractors

Each of the two studied systems (3.5) and Table 3.1 can exhibit self-reproducing attractors at different locations for different signs of the parameter b , which controls the sign of the x -coordinate of the equilibrium point as mentioned before as shown in Fig. 3.11. Two different attractor diagrams can be obtained at distinct values and/or signs of b along the x -axis, which are colored differently. An online colored version of the thesis can be found in <http://eecs.cu.edu/~hfahmy/thesis.html>. In addition, if the parameter b varies dynamically with time and switches its value and sign as time advances, then multi-scroll attractors can be generated similar to the procedure given in [24]. The derivative of such non-autonomous parameters can be considered zero, since the angular frequency of the multi-level pulse signals is sufficiently small compared with the chaotic oscillator. Figure 3.12 shows various examples in which parameter switching is used to

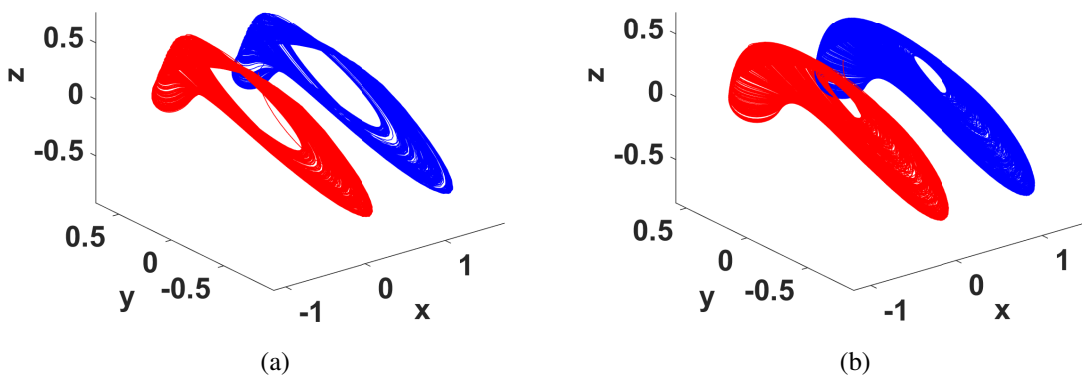


Figure 3.11: Differently allocated attractor diagrams at $b > 0$ (darker) and $b < 0$ (lighter) for (a) the piece-wise nonlinearity system and (b) the quadratic nonlinearity system.

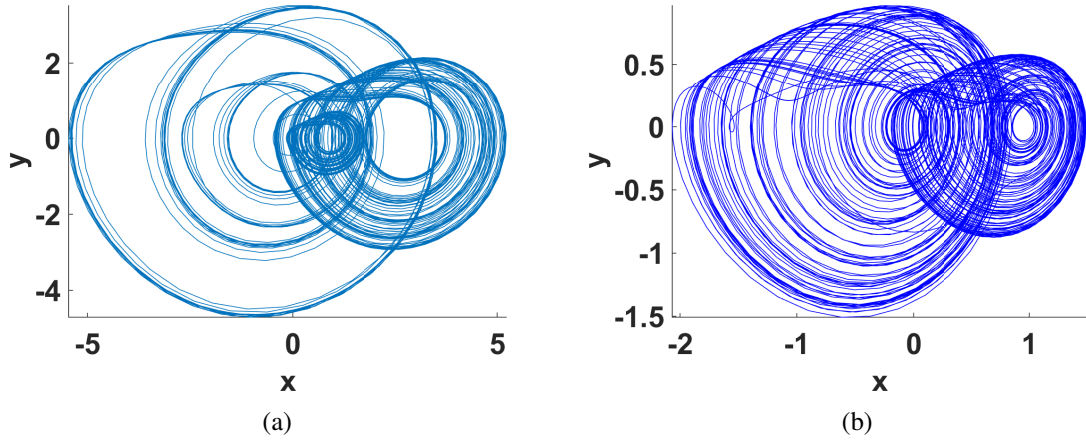


Figure 3.12: (a) Four-scroll attractor using the piece-wise nonlinearity system and (b) Double-scroll attractor using the quadratic nonlinearity system.

generate multi-scroll chaotic attractors from the two systems. In this case, the attractor diagrams are joined and undergo switching from side to side throughout the simulation time. Figure 3.12(a) generates a four-scroll attractor from the piece-wise nonlinearity system through switching the parameter values from $a = b = 1$, to $a = 2$ and $b = -0.7$, followed by $a = 3$ and $b = 1$, and finally $a = 4$ and $b = -0.7$, each case for quarter the simulation time, respectively, where $r = 0.6$ and $\mu = 1$. Figure 3.12(b) generates a double-scroll attractor from the quadratic nonlinearity system through switching the value of the parameter b from 1 to -0.6 after half of the simulation time passes, where $r = 0.5$ and $a = \mu = 1$.

3.2.4 Fractional-Order Extension and Sensitivity to Fractional Orders

The fractional derivative of order α , based on Caputo definition [27], is given by:

$$D^\alpha f(t) = \begin{cases} \frac{1}{\Gamma(m-\alpha)} \int_0^t \frac{f^m(\tau)}{(t-\tau)^{\alpha-m+1}} d\tau & m-1 < \alpha < m \\ \frac{d^m}{dt^m} f(t) & \alpha = m \end{cases}, \quad (3.6)$$

where $m = \lceil \alpha \rceil$ and $\Gamma(\cdot)$ is the gamma function given by:

$$\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt, \quad \Gamma(z+1) = z\Gamma(z). \quad (3.7)$$

In order to solve fractional-order systems numerically with a step size h , Grünwald-Letnikov (GL) method of approximation [31] is used, which is given by:

$$D^\alpha f(t) \approx h^{-\alpha} \sum_{j=0}^k (-1)^j \binom{\alpha}{j} f(t_{k-j}). \quad (3.8)$$

Consequently, a fractional-order autonomous differential equation $D^\alpha y(t) = f(y(t))$ can be discretized using (3.8) as follows:

$$y(t_k) = f(y(t_{k-1}))h^\alpha - \sum_{j=1}^k c_j^{(\alpha)} y(t_{k-j}), \quad (3.9)$$

where $t_k = kh$, and the coefficients $c_j^{(\alpha)}$ are computed using:

$$c_j^{(\alpha)} = \left(1 - \frac{1+\alpha}{j}\right) c_{j-1}^{(\alpha)}, \quad j = 1, 2, 3, \dots, \quad c_0^{(\alpha)} = 1. \quad (3.10)$$

Same algebraic manipulation can be applied to a system of three fractional-order differential equations to get the fractional-order counterpart of (3.4), which is given by:

$$\begin{aligned} D^\alpha x &= y, \\ D^\alpha y &= z, \\ D^\alpha z &= -r z - y + f(x). \end{aligned} \quad (3.11)$$

and its numerical solution using GL is given by:

$$\begin{aligned} x_{i+1} &= (y_i) h^\alpha - \sum_{j=1}^i c_j^{(\alpha)} x_{i-j+1}, \\ y_{i+1} &= (z_i) h^\alpha - \sum_{j=1}^i c_j^{(\alpha)} y_{i-j+1}, \\ z_{i+1} &= (-r z_i - y_i + f(x_i)) h^\alpha - \sum_{j=1}^i c_j^{(\alpha)} z_{i-j+1}. \end{aligned} \quad (3.12)$$

Tables 3.8 and 3.9 show the time series of the three phase space dimensions x , y and z as well as the post-transient attractor diagram illustrating the obtained type of solution for different values of the fractional-order. It can be inferred that as α decreases than 1, the fractional-order counterparts are easily drifted from chaotic behavior.

3.3 Reproducibility Rules and Implementation Sensitivity

In floating-point arithmetic environments, the algebraic associativity property no longer holds [153] because of rounding errors and the order of execution matters [153]. This section uncovers the implementation sensitivity of chaotic systems in floating-point, as well as fixed-point, computations and its implications [5]. Figure 3.13 summarizes the studied cases and factors including discretization step and precision effects.

3.3.1 Sensitivity to Order of Additions

Three chaotic systems were selected [36, 154] and discretized using Euler technique, each having two terms including x_i in the z_{i+1} equation. For each system, three cases

Table 3.8: Piece-wise nonlinearity system responses versus the fractional-order α at parameter values $a = b = \mu = 1$ and $r = 0.6$

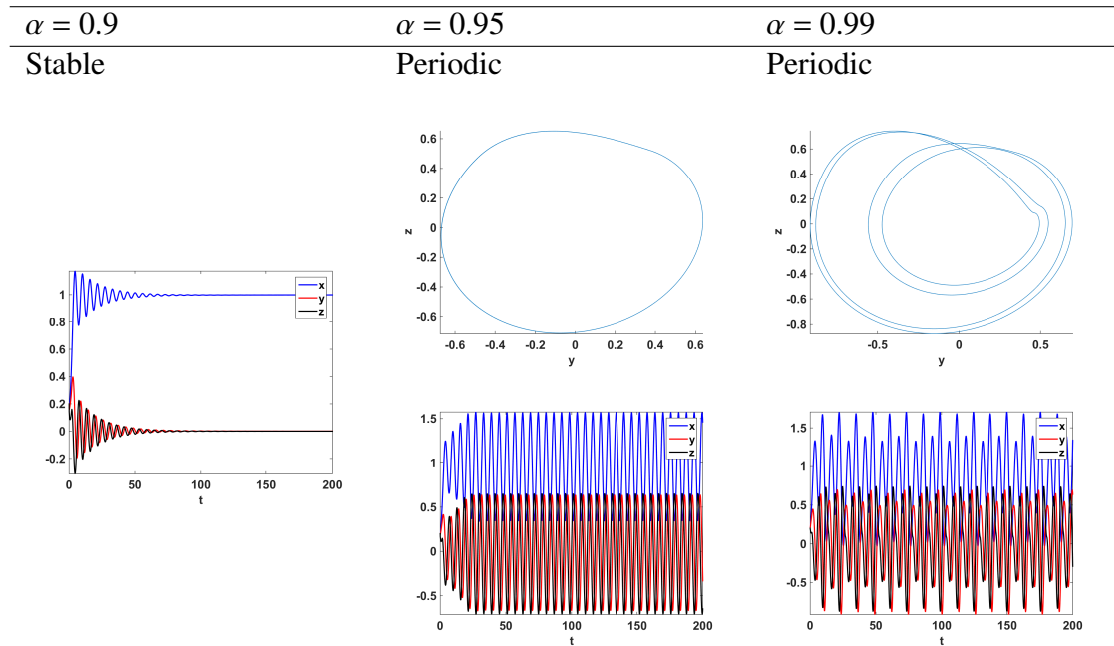
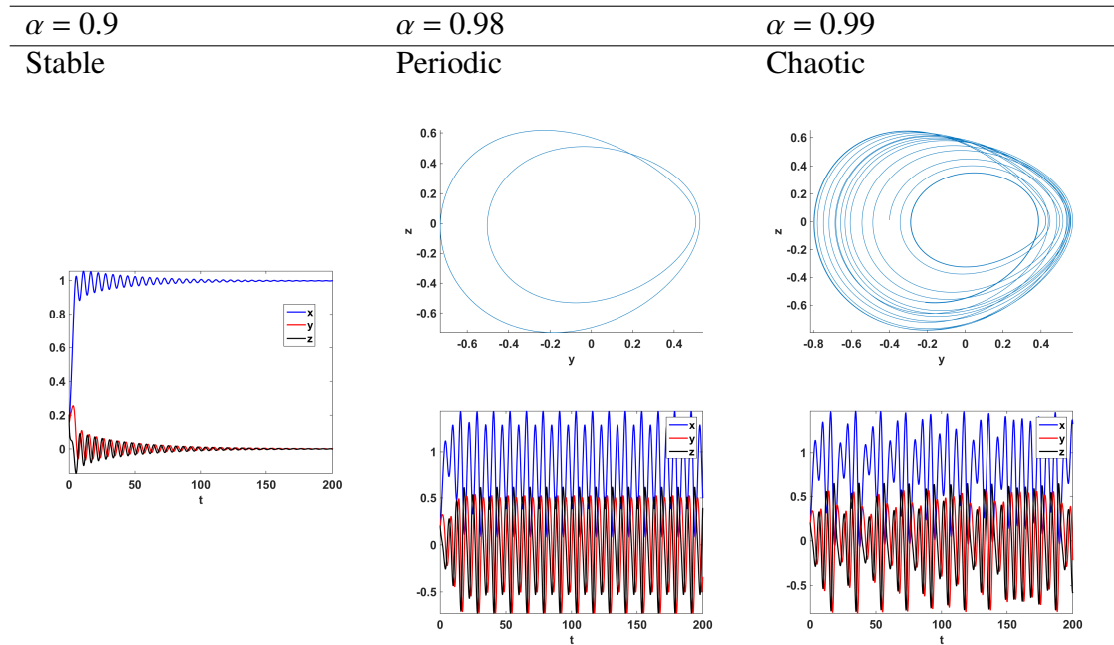


Table 3.9: Quadratic nonlinearity system responses versus the fractional-order α at parameter values $a = b = \mu = 1$ and $r = 0.5$



corresponding to different orders of execution of z_{i+1} are selected, which are given in Table 3.10, where:

$$x_{i+1} = x_i + hy_i, \quad y_{i+1} = y_i + hz_i, \quad \text{sgn}(x) = \begin{cases} -1, & x < 0 \\ 0, & x = 0 \\ 1, & x > 0 \end{cases}, \quad (3.13)$$

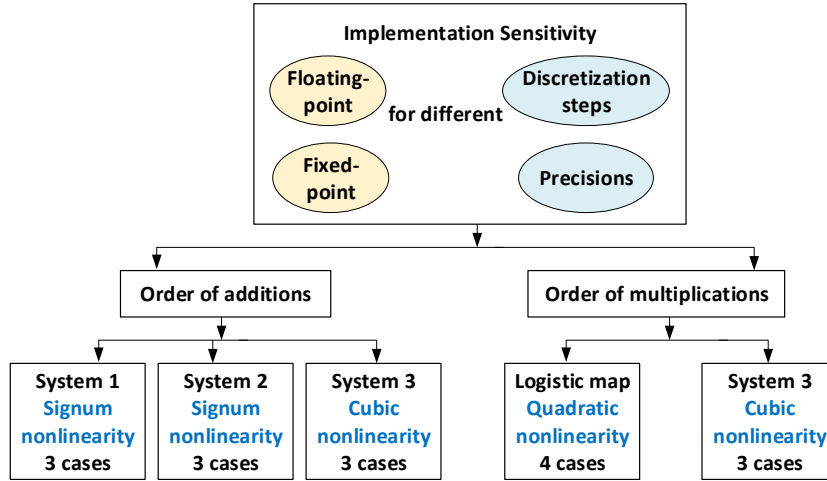


Figure 3.13: The studied chaotic systems and map, their implementation cases and sensitivity factors.

h is the discretization step and $sgn(x)$ is the sign function or signum function that extracts the sign of x as defined before.

3.3.1.1 Software Floating-Point Implementation

Figure 3.14 shows the results of the three cases of system 1 in software double-precision floating-point implementation. All software computations are performed using Matlab R2014b. In addition, different initial values yield mismatches, but the results are shown

Table 3.10: Different implementations of three chaotic systems corresponding to different orders of addition

Sys.	Case I	Case II	Case III
1	$z_{i+1} = z_i -$ $0.8h(z_i + y_i + x_i - sgn(x_i))$	$z_{i+1} = z_i -$ $0.8h(x_i + z_i + y_i - sgn(x_i))$	$z_{i+1} = z_i -$ $0.8h(x_i + y_i + z_i - sgn(x_i))$
2	$z_{i+1} = z_i +$ $h(-0.6z_i - y_i + 1.2x_i - sgn(x_i))$	$z_{i+1} = z_i +$ $h(1.2x_i - 0.6z_i - y_i - sgn(x_i))$	$z_{i+1} = z_i +$ $h(1.2x_i - y_i - 0.6z_i - sgn(x_i))$
3	$z_{i+1} = z_i +$ $h(-0.6z_i - y_i + 1.6x_i^3 - 1.6x_i)$	$z_{i+1} = z_i +$ $h(1.6x_i^3 - 0.6z_i - y_i - 1.6x_i)$	$z_{i+1} = z_i +$ $h(1.6x_i^3 - y_i - 0.6z_i - 1.6x_i)$

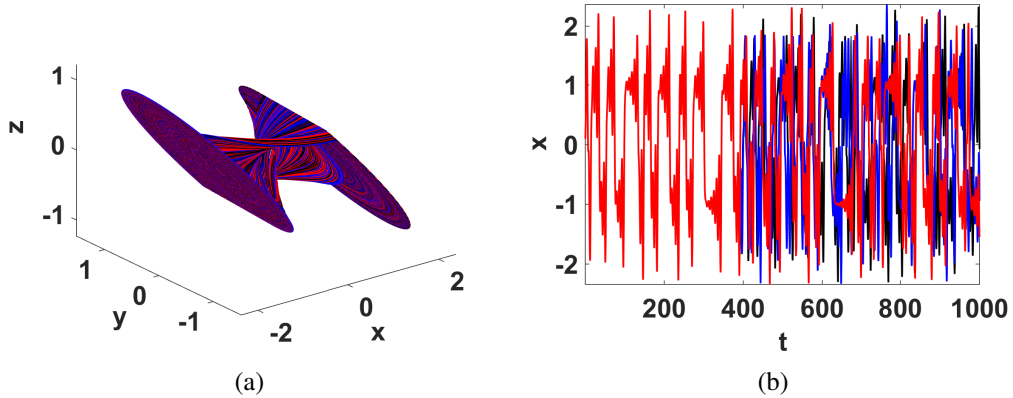


Figure 3.14: (a) Attractor diagrams and (b) mismatches in x time series of the three cases of system 1 in software double-precision floating-point implementation.

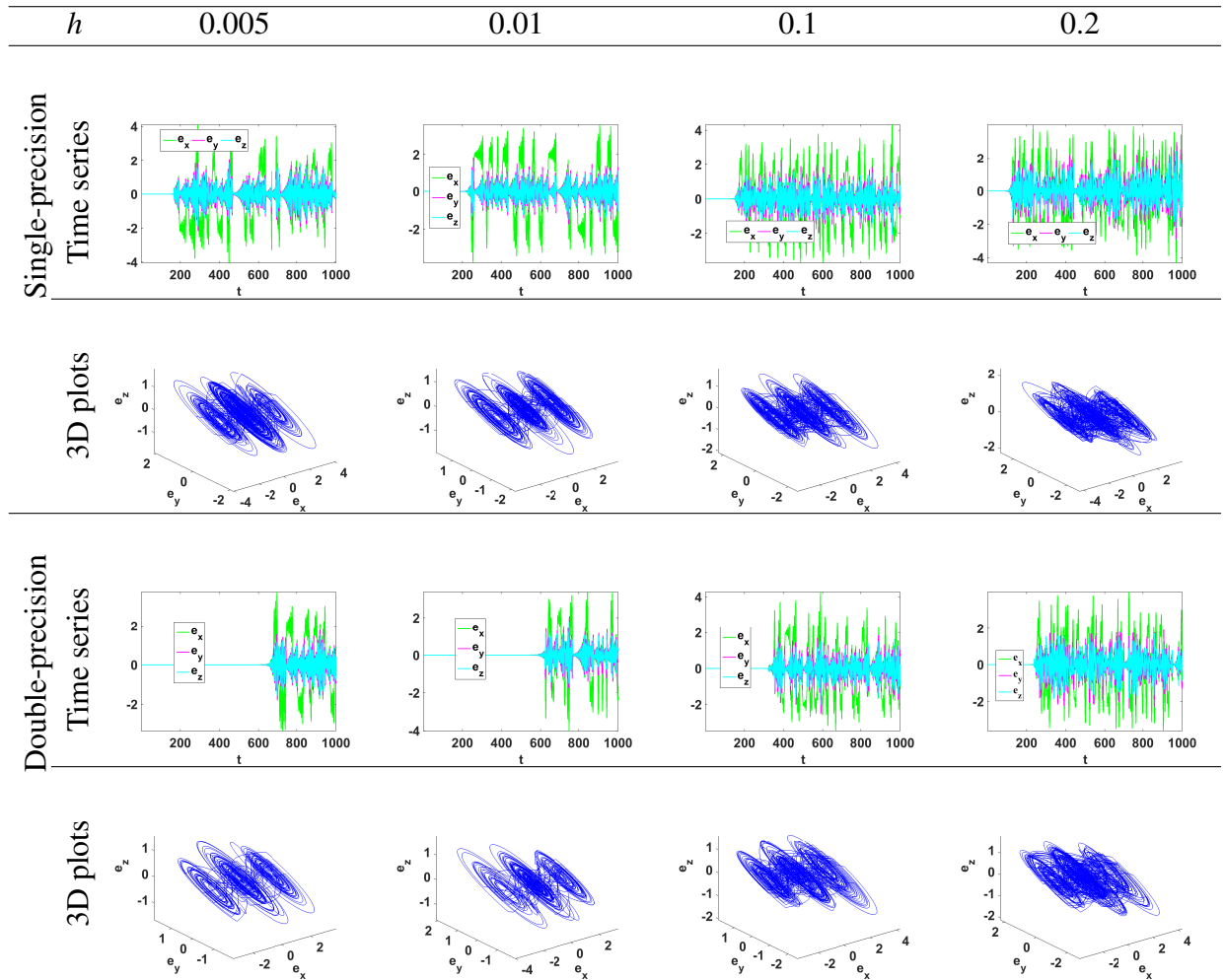
for $(x_0, y_0, z_0) = (0.1, 0.25, 0.5)$. Although the shape and size of the attractor look similar for the three implementations (Fig. 3.14(a)), the system becomes sensitive to the order of terms in implementation on the long term evolution. This can be inferred from Fig. 3.14(b) for x time series, where the three implementations are plotted altogether. Both y and z time series are similarly affected by the order of terms. Figure 3.14(a) also indicates that the three state variables have the same order of magnitudes.

The system is solved using $h = 0.1$ from $t = 0$ to 30 000, i.e., 300 000 points. The time series resulting from the three different orders appear to be roughly the same in the first 350 time units. However, the absolute value of the error between the time series yielded by each pair of implementation orders increases gradually from $O(10^{-16})$ near the beginning until it reaches $O(10^{-2})$ starting at around $t = 350$ in z time series and then these higher values of error propagate to the two other time series. The absolute value of the error is limited, hence the system is not drifted away from chaotic behavior and does not diverge. It remains chaotic, but with different time series. Moreover, Table 3.11 shows that a strange attractor can be formed by the x , y and z components of the errors in case of mismatch, which exhibits three-scrolls. These scroll-shaped attractor diagrams formed by the mismatch or error can themselves be used as alternative sources of randomness as will be discussed in Section 3.5.

Table 3.11 shows the effect of the time step h on the error between the time series yielded by cases I and III for both single and double-precision floating-point implementations. For double-precision, it can be inferred that as the value of the time step h increases, the gradual increase of the absolute value of the error from 0 starts at an earlier time t and the maximum limit the error reaches in the shown time interval increases. That is, the time step h should approach zero to diminish the error, which is impractical from the viewpoints of memory usage and time complexity.

Single-precision representation has a narrower precision and range of magnitudes that can be represented. For single-precision implementation and using $h = 0.1$, the absolute value of the error between the time series of Cases I and III increases gradually from $O(10^{-7})$ near the beginning until it reaches $O(10^{-2})$ starting at around $t = 125$. That is, for single-precision implementation, the error starts to appear earlier than it does for

Table 3.11: Time series and three-dimensional plots of the error between cases I and III of system 1 for different time steps and precisions in a floating-point implementation

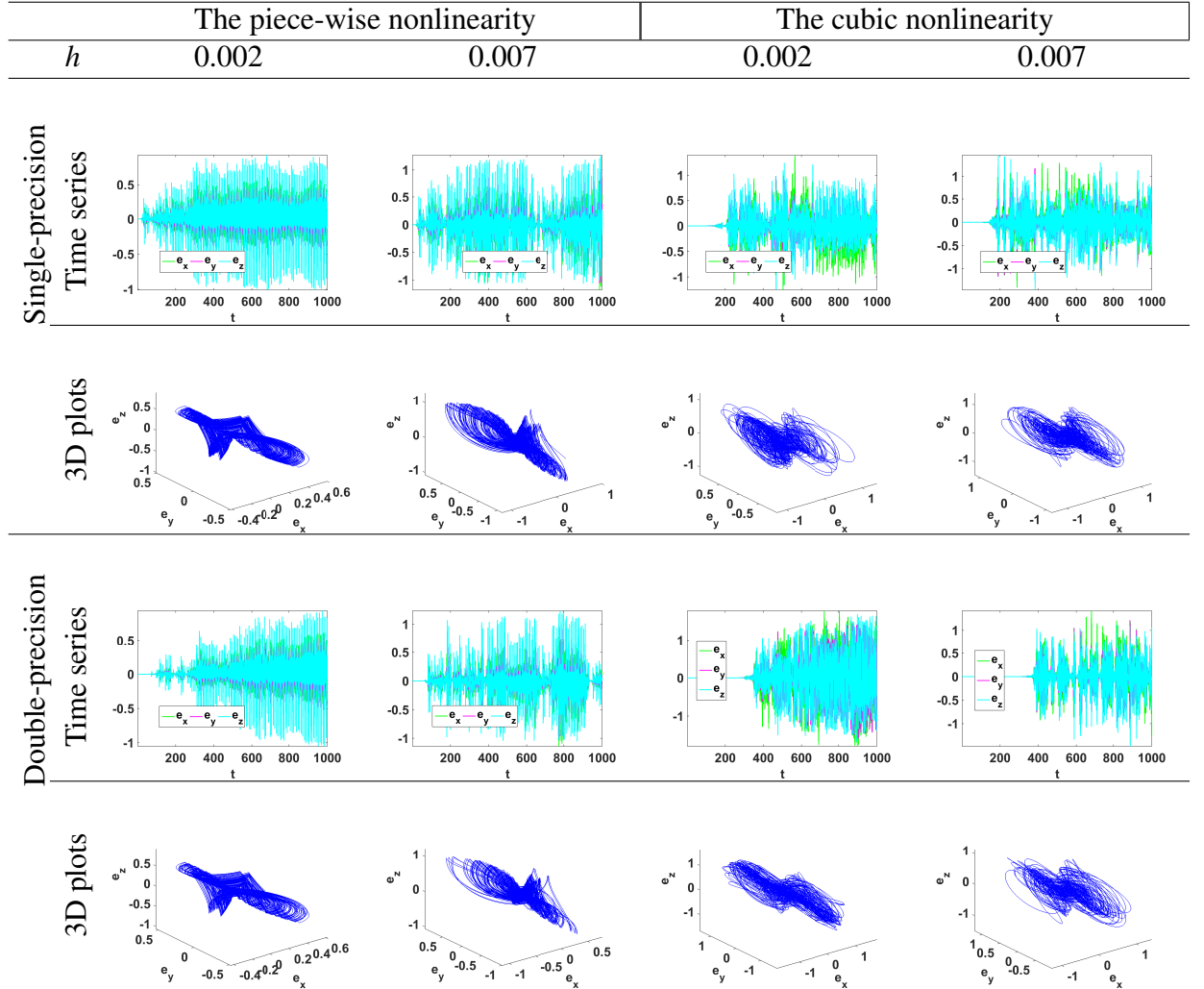


double-precision implementation. However, the effect of h on the starting time of the error is less significant than it is in the double-precision implementation.

For the two other systems, Table 3.12 shows the effects of h and precision on the error time series and 3D plots in software floating-point implementations. One of the reported forms of step size sensitivity and consistency is that for system 2, the response diverges when h is increased above 0.007. Consequently, results corresponding to small values of h are reported in Table 3.12. Although the difference in h is not large, similar notes to those reported for system 1 apply. That is, the starting time and the maximum limit of the error increase as h increases. In addition, the starting time is earlier for single-precision implementation.

To further indicate that all different studied cases of the systems exhibit chaotic behavior, bifurcation diagrams and LEs are investigated for the different cases using Wolf's LEs computation algorithm [155, 156] and found to be roughly equal. The constant values 0.8 and 0.6 are replaced by parameters a and b for systems 1 and 3, respectively. Figure 3.15 (a) shows the bifurcation diagram of system 1 against the parameter a , where it diverges for values of a less than roughly 0.48, then it becomes chaotic in the approximate interval $[0.48, 1)$, then it becomes stable. LEs of system 3 are computed for $a = 0.6$ and

Table 3.12: Time series and three-dimensional plots of the error between cases I and III of systems 2 and 3 for different time steps and precisions in a software floating-point implementation



are shown in Fig. 3.15(c). MLE versus b is shown in Fig. 3.15(d), which matches the bifurcation diagram against b of Fig. 3.15(b) in the chaotic and stable regions.

3.3.1.2 Hardware Fixed-Point Implementation

The reason behind the sensitivity to order of additions in floating-point computations is the mantissa alignment step if exponents are different [157]. On the other hand, fixed-point representation uses integer hardware operations controlled by a given convention about the location of the fractional point and fixed register size for all variables. While in floating-point arithmetic gaps between adjacent numbers are not uniformly spaced, the gaps between adjacent numbers always equal a value of one in fixed-point arithmetic.

The different cases of the studied systems are designed and simulated in fixed-point arithmetic using Xilinx ISE 14.7 and realized on Artix-7 XC7A100T FPGA. However, no mismatches are reported and the time series corresponding to different cases are identical. This is not the case for orders of multiplication as will be demonstrated in the next section.

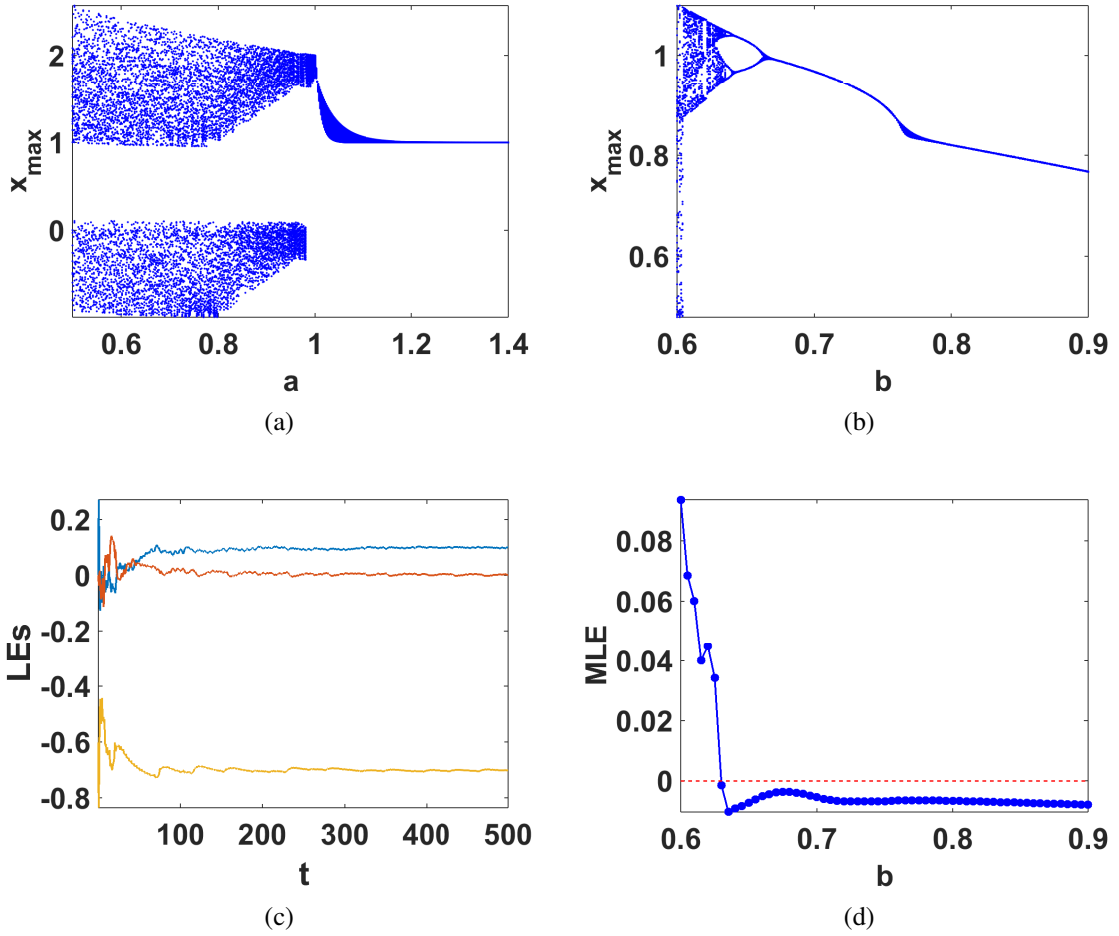


Figure 3.15: Bifurcation diagrams of (a) system 1, (b) system 3, (c) LEs of system 3 at $b = 0.6$ and (d) MLE versus b .

3.3.2 Sensitivity to Order of Multiplications

In this section, the well-known logistic map with four different implementations, which are given by:

$$\begin{aligned} f_1(x_i) &= \lambda x_i(1 - x_i), & f_2(x_i) &= \lambda(1 - x_i)x_i, \\ f_3(x_i) &= \lambda(x_i - x_i^2), & f_4(x_i) &= \lambda x_i - \lambda x_i^2 \end{aligned} \quad (3.14)$$

is considered to demonstrate the implementation sensitivity of the map for digital computations which involve rounding, more specifically, sensitivity to the order of multiplications. As another example on the sensitivity to the order of multiplications, system 3 can be implemented in different orders of terms, e.g., besides case I from Table 3.10, case IV uses $z_{i+1} = z_i + h(-0.6z_i - y_i + 1.6(x_i^2 - 1)x_i)$ and case V uses $z_{i+1} = z_i + h(-0.6z_i - y_i + 1.6x_i(x_i^2 - 1))$.

3.3.2.1 Software Floating-Point Implementation

Figure 3.16(b) shows examples on the differences between the four cases, which are implemented in double-precision floating-point arithmetic. The cases differ from each

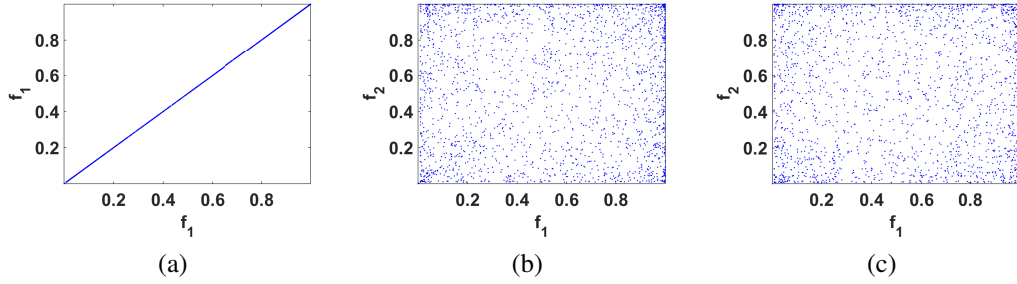


Figure 3.16: (a) Exact implementation, f_1 versus f_1 . (b) Double-precision and (c) single-precision floating-point different implementations, f_2 versus f_1 , of the logistic map.

other after very few iterations and result in different chaotic sequences. The error starts off with values of $O(10^{-16})$ till it reaches $O(10^{-3})$ around $n = 50$ and accumulates to higher values as time advances. Similarly, all of f_1 , f_2 , f_3 and f_4 results differ from each other demonstrating the sensitivity of the same mathematical function to computations. Similar results were obtained for single-precision computations as shown in Fig. 3.16(c), where the error starts off with values of $O(10^{-9})$ and reaches $O(10^{-3})$ around $n = 24$, i.e., earlier due to the more limited precision. Floating-point implementation mismatches for system 3 are given in Table 3.13 and can be described similar to the sensitivity to the order of additions.

3.3.2.2 Hardware Fixed-Point Implementation

The four cases of the logistic map are designed and simulated in fixed-point arithmetic using Xilinx ISE 14.7 and realized on Artix-7 XC7A100T FPGA. The ranges $x \in (0, 1)$ and $\lambda < 4$ can be increased to accommodate the sign if the convex logistic map is considered [151]. Low or intermediate precision, i.e., number of bits, may drift the map from chaotic behavior [147]. The registers are represented as 3 integer bits, to avoid overflow, and $p_f = 24, 32$ and 48 fractional bits with the results given in Fig. 3.17. Mismatches are reported and all f_1 , f_2 , f_3 and f_4 differ from each other similarly. These results are obtained using fixed register size and applying truncation to this size just after each basic operation. If wider intermediate precisions are allowed, mismatches can be eliminated.

Figure 3.18 shows how different number representations used to implement one case of the chaotic map result in different time series. Yet, they still exhibit similar chaotic properties such as the value of MLE, which is computed numerically using forward difference approximation of the first derivative as in [147].

Mismatches were reported for fixed-point implementation of system 3 as well, which are given in Table 3.14 using 2 integer bits and 16 and 24 fractional bits.

For hardware realization, the final output is truncated to 12 bits to be suitable for the experiment using FPGA and oscilloscope. All proposed implementations have been experimentally verified on Artix-7 XC7A100T FPGA. An example of the experimental result on the oscilloscope for one of the discretized systems is shown in Fig. 3.19. A summary of the hardware resources utilization and efficiency of producing the mismatch signal for the discrete logistic map and discretized system 3 is given in Table 3.15 corresponding to 18 and 19 bit precisions (i.e. $p_f = 16$), respectively. Throughput is computed through

Table 3.13: Time series and three-dimensional plots of the error between cases I and V of system 3 for different time steps and precisions in a floating-point implementation on Matlab

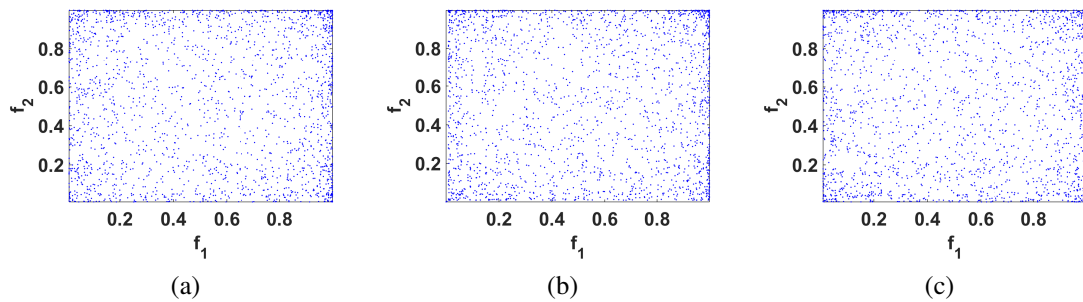
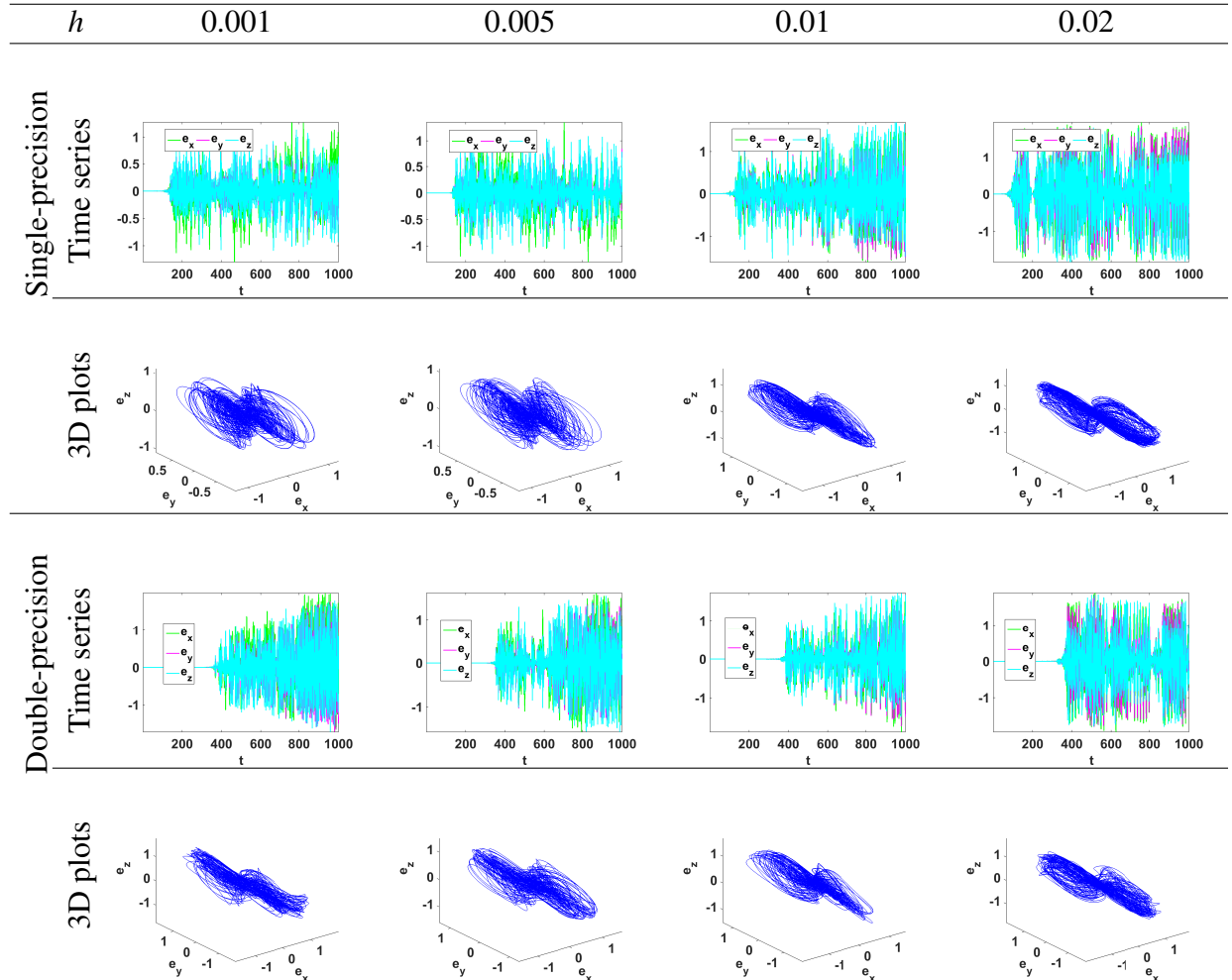


Figure 3.17: Fixed-point computations sensitivity of the logistic map (a) $p_f = 24$, (b) $p_f = 32$ and (c) $p_f = 48$.

multiplying the maximum frequency by the number of output bits per clock cycle.

From Sections 3.3.1 and 3.3.2, it can be inferred that as the value of the time step h increases, the gradual increase of the absolute value of the error from 0 starts at an

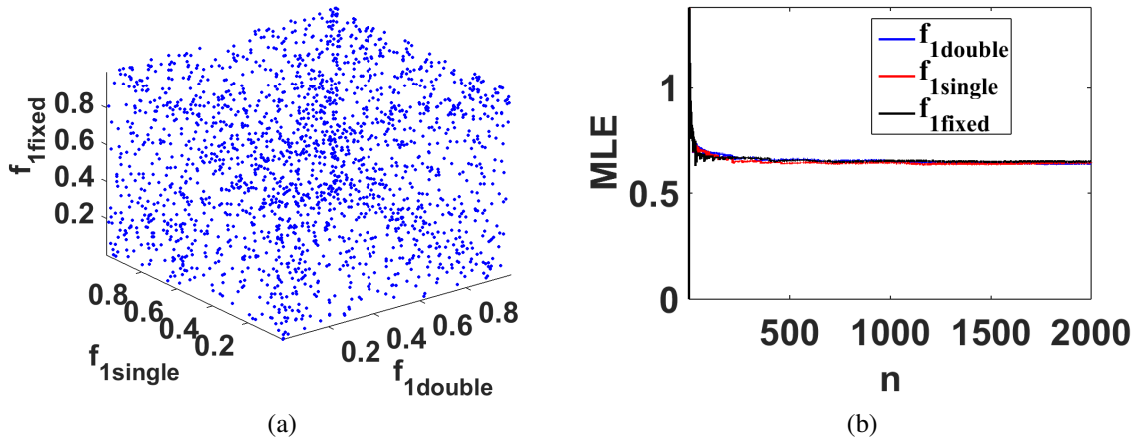


Figure 3.18: Chaotic properties of f_1 in double, single floating-point and fixed point ($p_f = 32$) computations (a) time series and (b) MLE.

Table 3.14: Time series and three-dimensional plots of the error between cases I and V of system 3 for different time steps and precisions in a fixed-point implementation

h	$p_f = 16$		$p_f = 24$	
	Time series	3D plots	Time series	3D plots
2^{-8}				
2^{-6}				

earlier time t and the maximum limit the error reaches in the shown time interval increases. That is, the time step h should approach zero and similarly the precision should approach infinity to diminish the error, which is impractical from the viewpoints of memory usage and time complexity. Reducing the discretization step and increasing the precision can delay the significant increase in the error, yet, it does not eliminate it. Fixed-point may not suffer from mismatch and allow more reproducibility when the changes are limited to the order of additions only and on using wider intermediate precisions in case of varying order of multiplications. Generally, the changes due to varying implementation factors can not always be expected owing to the increased sensitivity of chaotic systems, which agrees with the results obtained for finite precision logistic map [147]. Consequently, all implementation details should be carefully considered for reproducibility and to achieve successful chaotic communication.

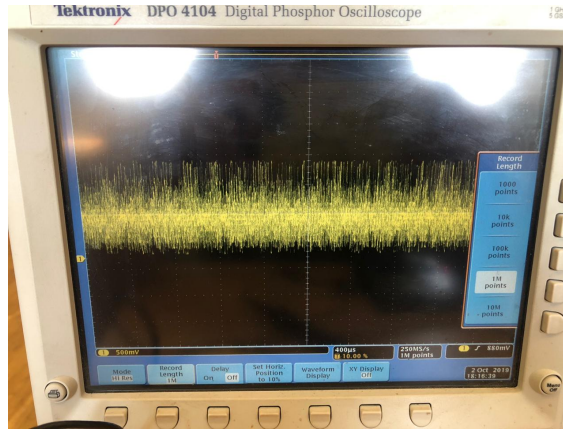


Figure 3.19: Oscilloscope experimental mismatch signal result between two different cases of system 3.

Table 3.15: Hardware resources utilization and efficiency of mismatch signals production

	No of slices	No of slice registers	Maximum Frequency “MHz”	Multipliers	Throughput “Gbit/s”
Logistic map	226	50	90.59	4	1.5924
System 3	479	144	66.593	9	3.7068

3.4 Sensitivity Effect on Image Encryption

This section studies the effect of the mismatch between the three cases of system 3 on applications in software double-precision floating-point implementation. A simple software image encryption scheme is used, where case V is used for encryption and cases I, IV and V are used one at a time for decryption.

3.4.1 Encryption and Decryption Schemes

Figure 3.20(a) shows a simple substitution-based stream cipher scheme with feedback, which is used for symmetric-key encryption. The chaotic signals are multiplied by a scaling factor of 10^9 to be suitable for conversion to an integer value. The original color image is decomposed into three channels: red, green and blue. Each component is xored with the 8 Least Significant Bits (LSBs) of the integer-represented chaotic signals, respectively, xored together with a feedback element from a channel of the previously encrypted pixel selected by the least significant bits of its channels [11] according to the multiplexing procedure given in Fig. 3.20(b). In the decryption scheme, all operations are reversed. The encryption key is subdivided as shown in Fig. 3.20(b) with a total of 128 bits, i.e., 2^{128} possibilities, which can resist brute force attacks in which the hacker tries all possible combinations of the encryption key as specified by the Advanced Encryption Standard (AES) [11]. The value P_{sum} represents the input dependent term, which enhances the resistance to different attacks, and equals the sum of all pixels of the input image [11].

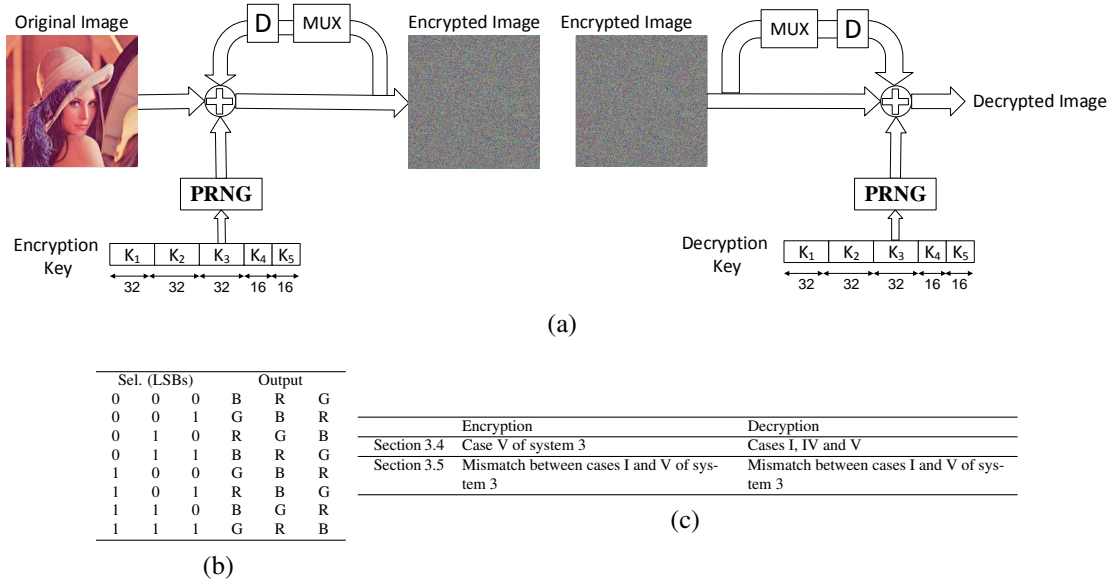


Figure 3.20: (a) Encryption and decryption block diagrams of the stream cipher system with feedback, (b) multiplexing table and (c) the utilized PRNG.

The chaotic system parameters are computed from the key as follows:

$$\begin{aligned}
 x_0 &= x_{fix} + K_1 \times 2^{-36} + \text{mod}(P_{sum}, 10)/1000, \\
 y_0 &= y_{fix} + K_2 \times 2^{-36} + \text{mod}(P_{sum}, 10)/1000, \\
 z_0 &= z_{fix} + K_3 \times 2^{-36} + \text{mod}(P_{sum}, 10)/1000, \\
 a &= a_{fix} + K_4 \times 2^{-36} + \text{mod}(P_{sum}, 10)/1000, \\
 b &= b_{fix} + K_5 \times 2^{-36} + \text{mod}(P_{sum}, 10)/1000
 \end{aligned} \tag{3.15}$$

where the fixed parts are set to values within the ranges corresponding to chaotic behavior and the constants 0.6 and 1.6 are replaced by parameters a and b , respectively.

3.4.2 Wrong Decryption Results

In this section, one implementation (case V) of system 3 is used for encryption and each of cases I, IV, and V is used for decryption once as shown in Fig. 3.20. The corresponding decrypted images are analyzed using several performance metrics, which are defined in Table 3.16. Table 3.16 lists the encryption performance tests that will be used throughout the rest of the thesis.

Table 3.17 summarizes the decryption results, where only case V, which was used for encryption, succeeds in correct decryption of the image. While the correct decrypted image using case V has correlation coefficients close to one, indicating that it is identical to the corresponding original image, the two other implementations have correlation coefficients close to zero, indicating that they are weakly correlated. The samples of the wrong decrypted images are uniformly distributed, as shown in the histogram plots, unlike the original and the correct decrypted images. MSE equals zero in case of correct decryption and much higher values in case of wrong decryption. The wrong decrypted images have higher values of entropy than the correct one since they are nearly random.

Their entropy value are close to the ideal value 8 that corresponds to the number of bits required to represent a pixel channel value.

3.5 Encryption Application of the Mismatch Signal

In this section, the PRNG of Fig. 3.20 is the mismatch signal between cases I and V of system 3, which is shown in Table 3.13 using double-precision implementation and $h = 0.02$ and discarding the first 500 time units, i.e., 25 000 iterations. Figure 3.21 shows the randomness properties of the chaotic mismatch signal e_x , which has nearly aperiodic time series, flat frequency distribution and histogram, and an autocorrelation function that roughly equals zero for lag values other than zero. Similar results were obtained for e_y and e_z .

Table 3.18 shows the encrypted image and histogram of the red channel. In addition, it gives the values of the performance metrics averaged over the three channels. The image encryption scheme successfully passes the statistical and sensitivity tests with very low horizontal, vertical and diagonal correlation. In addition, high MSE values and entropy close to 8 are reported for slight perturbation in the decryption key indicating key sensitivity. Moreover, it is robust against brute force attacks owing to its key space of 2^{128} and against differential attacks since the values of UACI and NPCR approach the recommended values 33.3 % and 100 %, respectively.

Table 3.16: Performance metrics of image encryption systems

$$\chi_{\text{test}}^2 = \sum_{i=1}^k \frac{(o_i - e_i)^2}{e_i}, \quad k = 256 \text{ is the number of levels in a color, } o_i \text{ and } e_i \text{ are the observed and expected occurrence frequencies of each color level (0 - 255), respectively. For } 1024 \times 1024 \text{ image, } e_i = 1024 \times 1024 / 256 = 4096.$$

Correlation coefficient (ρ) = $\frac{\text{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$, where

$$\text{cov}(x,y) = \frac{1}{S} \sum_{i=1}^S \left(x_i - \frac{1}{S} \sum_{j=1}^S x_j \right) \left(y_i - \frac{1}{S} \sum_{j=1}^S y_j \right), \quad D(x) = \frac{1}{S} \sum_{i=1}^S \left(x_i - \frac{1}{S} \sum_{j=1}^S x_j \right)^2, \quad S = M \text{ (height)} \times N \text{ (width)}.$$

Mean Squared Error (MSE) = $\frac{1}{M \times N} \sum_{i=1}^N \sum_{j=1}^M (P(i,j) - D(i,j))^2$, where $P(i,j)$, $D(i,j)$ are the original & wrong decrypted image pixels

Entropy = $-\sum_{i=1}^{2^8} p(s_i) \log_2 p(s_i)$, where $p(s_i)$ is the probability of symbol s_i


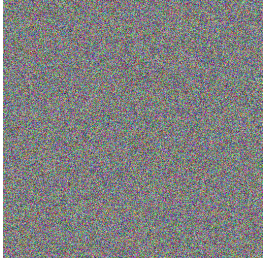
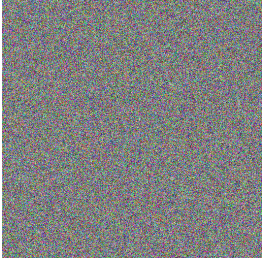
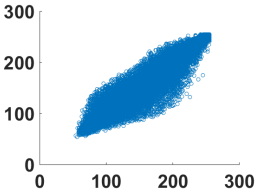
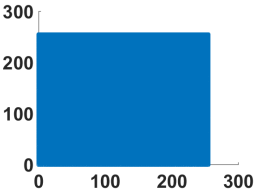
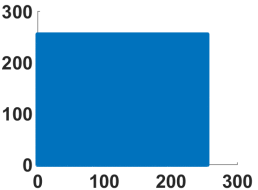
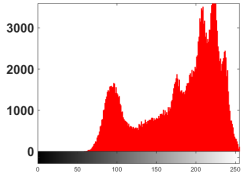
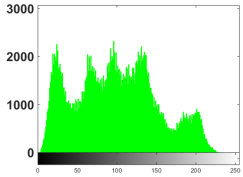
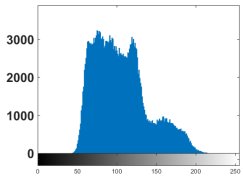
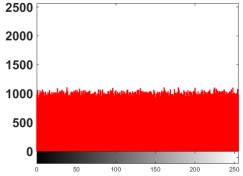
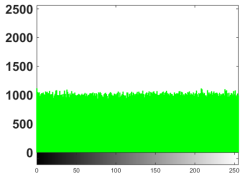
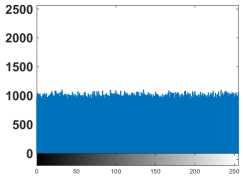
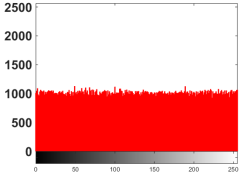
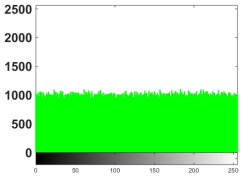
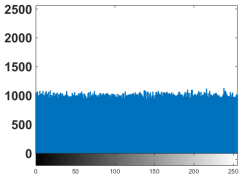
Peak Signal-to-Noise Ratio (PSNR) = $20 \log_{10} \left(\frac{I_{\text{max}}}{\sqrt{\text{MSE}}} \right)$, where I_{max} is the maximum pixel value in the image.

Number of Pixel Change Rate (NPCR) = $\frac{1}{N \times M} \sum_{i=1}^N \sum_{j=1}^M D(i,j) \times 100$,

Unified Average Changing Intensity (UACI) = $\frac{1}{M \times N} \sum_{i=1}^N \sum_{j=1}^M \left| \frac{C_1(i,j) - C_2(i,j)}{255} \right| \times 100$,

where $D(i,j) = \begin{cases} 1, & C_1(i,j) \neq C_2(i,j) \\ 0, & C_1(i,j) = C_2(i,j) \end{cases}$, C_1 is the ciphered pixel and C_2 is the ciphered pixel corresponding to a slightly modified original image.

Table 3.17: Decryption results for each of cases I, IV and V using case V in encryption

	Case V	Case I	Case IV
Dec. Im.			
Vert. Corr.	 0.9893	 0.0003	 0.0022
Horizon.	0.9798	-0.0042	-0.0029
Diag.	0.9737	0.0021	-0.0016
Hist.	  	  	  
MSE	0	8944.56	8953.25
Entropy	7.2718	7.9993	7.9993

More advanced statistical tests are provided by National Institute of Standards & Technology (NIST) statistical test suite [158], which is a statistical test suite for random and pseudo-random number generators for cryptographic applications. The tests are designed to examine the randomness characteristics of a sequence of bits by evaluating the P-value distribution (PV) and the proportion of passing sequences (PP). The test are carried out on the 8 LSBs of each chaotic output in the same manner in which they are

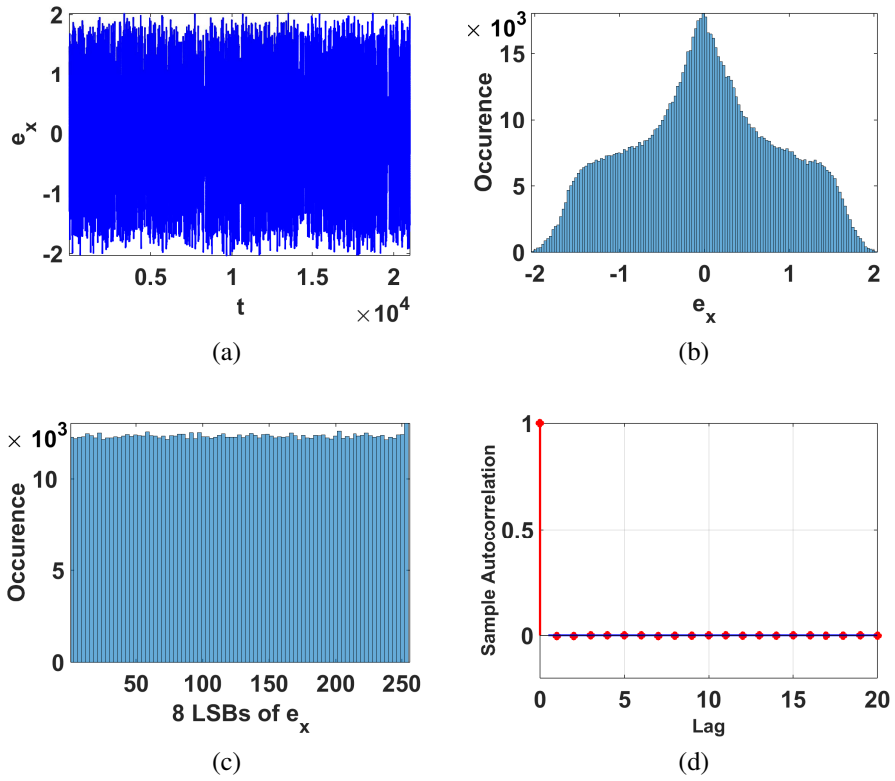
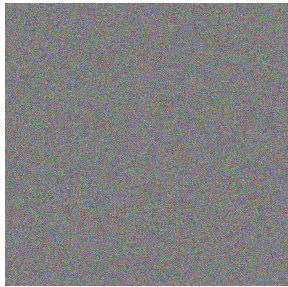
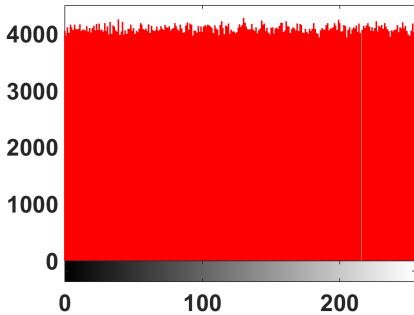


Figure 3.21: (a) Time series, (b) frequency distribution of the outputs, (c) histogram and (d) auto-correlation function of the PRNG based on the mismatch signal.

Table 3.18: Performance evaluation of the image encryption scheme based on the mismatch signal

Encrypted Image		Histogram	
			
Horizon.	Vert.	Diag. Correlation	
0.0005	0.0003	0.0002	
Key sensitivity (ΔK_1)		Differential attack	
MSE	Entropy	UACI (%)	NPCR (%)
8933.37	7.9998	33.4624	99.5607

used in the substitution of the 8-bit pixels. Table 3.19 shows that both the PRNG and encrypted image successfully pass the tests.

Table 3.19: NIST results for the PRNG based on the mismatch signal and encrypted images

Test	PRNG		Encrypted image	
	PV	PP	PV	PP
Frequency	✓	1	✓	1
Block Frequency	✓	1	✓	0.958
Cumulative Sums	✓	1	✓	1
Runs	✓	1	✓	1
Longest Run	✓	1	✓	1
Rank	✓	0.958	✓	1
FFT	✓	1	✓	1
Non-overlapping Template	✓	0.989	✓	0.988
Overlapping Template	✓	0.958	✓	1
Universal	✓	1	✓	1
Approximate Entropy	✓	1	✓	1
Random Excursions	✓	0.985	✓	0.983
Random Excursions Variant	✓	1	✓	0.981
Serial	✓	0.979	✓	1
Linear Complexity	✓	1	✓	0.958
Final result	Passed		Passed	

From this chapter, we set a reproducibility rule that all implementation details should be carefully considered in order to achieve successful chaotic communication. In addition, we can conclude that the first generalization and control enables attractor size and location change through both parameters a and b . It is a simple modification that replaces constant additive and multiplicative terms by parameters in the nonlinear term, inspired by generalized discrete maps. Hence, it enables easy analog and digital realizations as already proposed in previous similar works starting [36]. It paves the road towards employing high frequently proposed novel and generalized discrete maps as nonlinearities in continuous chaotic systems. Consequently, these more complicated and higher dimensional systems can be enhanced by importing the properties and characteristics of such maps. It is different from previous works on offset boosting [44–48] in achieving attractor location change through a multiplicative parameter b rather than an additive parameter. The idea of generating self-reproducing and multi-scroll attractors by non-autonomous time varying parameters has not been widely discussed prior to this work as it started in [54]. Yet, this approach has some limitations as it is only suitable for jerk-based chaotic systems not generic for any system. In addition, it enables equilibrium point offset along x -axis direction only. Moreover, these jerk-based systems are not necessarily suitable for extension to the fractional-order domain. Thus, we move to a second more generic approach in the next chapter.

Chapter 4: 2D and 3D Affine Transformations-Based Control

The second proposed generalization approach utilizes affine transformations to achieve more comprehensive controllability. This chapter sets the rules for two-dimensional transformations of chaotic systems and their applications. In addition, it extends the affine transformations-based control technique to three-dimensional space and applies it on fractional-order systems with hidden attractors.

Two-dimensional affine transformations are firstly utilized with six introduced parameters to achieve scaling, reflection, rotation, translation and/or shearing. Hence, the size, polarity, phase, location and shape of the strange attractor in space can be controlled without changing its chaotic dynamics. In addition, the embedded parameters enhance the randomness and sensitivity of the system and control its response. This approach is suitable for any general chaotic system not only jerk-based unlike the first approach of Chapter 3. It certainly overpasses performing the transformations as post-processing stages by applying them on the resulting time series in unpredictability. Trajectory control through dynamic parameters is demonstrated. Simulation results validate the proposed analysis for the simplest and Lorenz chaotic systems. An image encryption scheme is implemented using transformed Lorenz system resulting in a more secure encryption scheme in comparison to Lorenz and other recent related works. The scheme exhibits good performance when assessed using the standard tests [3].

4.1 Two-Dimensional Affine Transformations

Two-dimensional affine transformations can be applied to any pair of axes constructing a plane in the coordinate systems. They result in relatively simple equations and allow clear visualization in the different planes of the Cartesian coordinate system. Consider a point represented in the three-dimensional space with the coordinates (x, y, z) , its two-dimensional affine transformation from the x - y to the u - v plane in the three-dimensional space can be written as:

$$\begin{bmatrix} u \\ v \\ w \end{bmatrix} = \begin{bmatrix} a & b & 0 \\ d & e & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} c \\ f \\ 0 \end{bmatrix}, \quad (4.1)$$

with the inverse transformation

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{1}{\alpha} \begin{bmatrix} e & -b & 0 \\ -d & a & 0 \\ 0 & 0 & \alpha \end{bmatrix} \begin{bmatrix} u \\ v \\ w \end{bmatrix} + \frac{1}{\alpha} \begin{bmatrix} bf - ce \\ cd - af \\ 0 \end{bmatrix}, \quad (4.2)$$

where $\alpha = ae - bd$ and the third coordinate $w = z$. The u - v - w coordinates reduce to the x - y - z coordinates at $a = e = 1$ and $b = c = d = f = 0$.

4.2 Validation Examples

4.2.1 Validation Example 1: Generalized Simplest System

A very simple jerk-based system with piecewise nonlinearity, which is generated by a signum function, was presented in [154]. In its original form, the system is given by:

$$\begin{aligned} \dot{x} &= y, \\ \dot{y} &= z, \\ \dot{z} &= -0.8(z + y + x - \text{sgn}(x)), \end{aligned} \quad \text{where } \text{sgn}(x) = \begin{cases} -1, & x < 0 \\ 0, & x = 0 \\ 1, & x > 0 \end{cases} \quad (4.3)$$

Solving the system results in the chaotic attractor and time series shown in Fig. 4.1. The equilibrium points of the system are $(\pm 1, 0, 0)$ and the Jacobian matrix is independent of the equilibrium points with eigenvalues $\lambda_1 = -0.8994$ and $\lambda_{2,3} = 0.0497 \pm i 0.9418$. Saddle points of index two result in double-scroll attractors.

Using the inverse transformation (4.2), a transformed system in the u - v - w coordinate system is obtained, which is given by:

$$\begin{aligned} \dot{u} &= \frac{a}{\alpha}(-du + av + cd - af) + bw + c, \\ \dot{v} &= \frac{d}{\alpha}(-du + av + cd - af) + ew + f, \\ \dot{w} &= -0.8\left(w + \frac{1}{\alpha}((e-d)u + (a-b)v) - \text{sgn}\left(\frac{1}{\alpha}(eu - bv)\right)\right). \end{aligned} \quad (4.4)$$

The response of the system reduces to that of (4.3) at $a = e = 1$ and $b = c = d = f = 0$ as shown in Fig. 4.1, where the response of the transformed (original) system is plotted in dark/blue (light/red) color (see the online colored version).

The six added parameters provide controllability of the attractor diagram, or its projection in the u - v plane. In addition, the effect on each coordinate can be inferred from the time series. Table 4.1 provides the analyses of simplified versions: scaling (increase or decrease the values), reflection, translation with fixed distance, and shearing processes.

Table 4.2 shows the time series and attractor diagrams of the transformed and original coordinates. The transformations given by (4.1) on the original time series, i.e., post-processing results are also plotted in dark/black and the new equilibrium points are marked as 'x'.

Stability analysis can also be performed for the systems of Table 4.1. For example, in

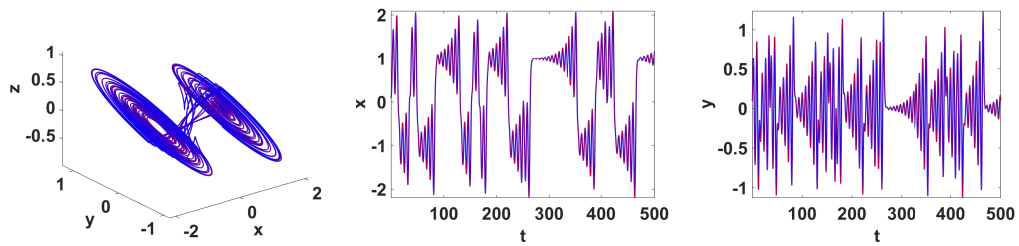


Figure 4.1: Attractor diagram and time series of system (4.3).

Table 4.1: Example transformations of the simplest chaotic system

Scaling (+ve), Reflection (-ve)	Rotation
$\dot{u} = \frac{a}{e}v,$ $\dot{v} = ew,$ $\dot{w} = -0.8\left(w + \frac{u}{a} + \frac{v}{e} - \text{sgn}\left(\frac{u}{a}\right)\right)$	$\dot{u} = \cos\theta(\sin\theta u + \cos\theta v) + \sin\theta w,$ $\dot{v} = -\sin\theta(\sin\theta u + \cos\theta v) + \cos\theta w,$ $\dot{w} = -0.8(w + (\cos\theta + \sin\theta)u + (\cos\theta - \sin\theta)v - \text{sgn}(\cos\theta u - \sin\theta v)),$
Equilibria: ($\pm a, 0, 0$)	Equilibria: ($\pm \cos\theta, \mp \sin\theta, 0$)
Scaling and translation	Shearing
$\dot{u} = \frac{a}{e}(v - f) + c,$ $\dot{v} = ew + f,$ $\dot{w} = -0.8\left(w + \frac{u}{a} + \frac{v}{e} - \text{sgn}\left(\frac{u}{a}\right)\right).$	$\dot{u} = \frac{1}{1-bd}(-du + v) + bw,$ $\dot{v} = \frac{d}{1-bd}(-du + v) + w,$ $\dot{w} = -0.8\left(w + \frac{1}{1-bd}((1-d)u + (1-b)v) - \text{sgn}\left(\frac{u-bv}{1-bd}\right)\right),$
Equilibria: ($a\left(\frac{c}{a} \pm 1\right), -\frac{ce}{a} + f, -\frac{f}{e}$)	Equilibria: ($\pm 1, \pm d, 0$)

case of rotation, the Jacobian matrix is given by:

$$J = \begin{bmatrix} \cos\theta \sin\theta & \cos^2\theta & \sin\theta \\ -\sin^2\theta & -\cos\theta \sin\theta & \cos\theta \\ 1.6\cos\theta\delta(u\cos\theta - v\sin\theta) - 0.8(\cos\theta + \sin\theta) & -0.8(\cos\theta - \sin\theta) & -0.8 \end{bmatrix}. \quad (4.5)$$

The characteristic polynomial is given by:

$$\lambda^3 - \text{tr}(J)\lambda^2 + (M_{11} + M_{22} + M_{33})\lambda - |J| = 0, \quad (4.6)$$

where $\text{tr}(J)$, $|J|$, M_{ik} are the trace, determinant and minor determinant of J eliminating row i and column k , respectively. The coefficients of the characteristic polynomial are obtained as follows:

- $\text{tr}(J) = -\frac{4}{5}$ and $|J| = \frac{8}{5}\delta(u\cos\theta - v\sin\theta) - \frac{4}{5}$.
- $M_{11} = \frac{4}{5}\cos^2\theta + \frac{4}{5}\sin 2\theta\delta(u\cos\theta - v\sin\theta),$
 $M_{22} = \frac{4}{5}\sin^2\theta - \frac{4}{5}\sin 2\theta\delta(u\cos\theta - v\sin\theta),$
 $M_{33} = 0$ and hence $M_{11} + M_{22} + M_{33} = \frac{4}{5}$.

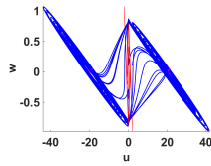
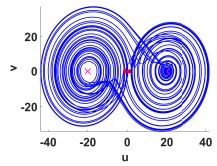
Consequently, $\text{tr}(J)$ and $M_{11} + M_{22} + M_{33}$ do not depend on θ and $|J| = -\frac{4}{5}$ evaluated at the equilibrium. Consequently, the transformed system has the same eigenvalues as the original system.

The eigenvectors of the Jacobian matrix are also affected by the transformation. Defining the Eigenvectors Inclination (EVI) as the angle between two eigenvectors at $\theta = 0$ and another value, i.e., $\Delta\theta = \theta$, we plot EVI against θ . For vectors x and y in a real inner product space, the cosine of the angle between them is given by $\cos\phi = \frac{\langle x, y \rangle}{\|x\|\|y\|}$. The real part of this cosine defines the Euclidean angle as $\cos\phi_E = \frac{\Re\{\langle x, y \rangle\}}{\|x\|\|y\|}$ in a complex vector space. Figure 4.2 shows that EVI (ϕ_E), at the equilibrium points, follows a pattern similar to that of the rotating system.

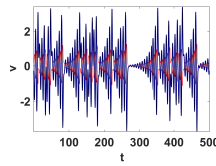
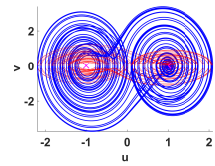
Table 4.2: Transformations of the simplest chaotic system: results and discussion

Scaling (+ve), Reflection (-ve) ($b = d = c = f = 0$)

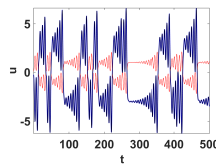
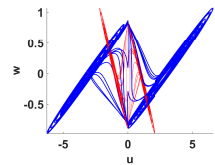
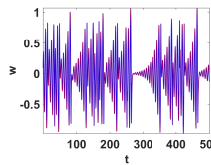
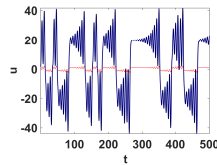
$a = 20, e = 30$



$a = 1, e = -3$

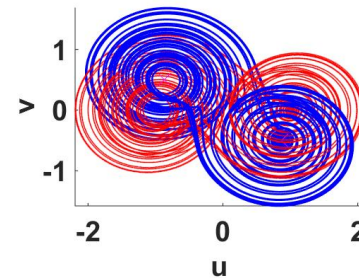


$a = -3, e = 1$

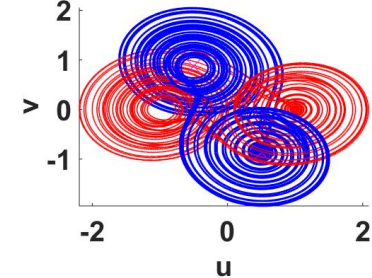


Rotation ($a = e = \cos(\theta), b = -d = \sin(\theta), c = f = 0$)

$\theta = \frac{\pi}{6}$



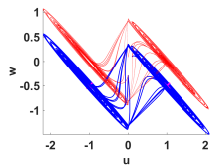
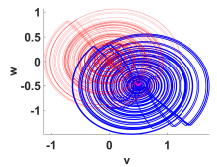
$\theta = \frac{\pi}{3}$



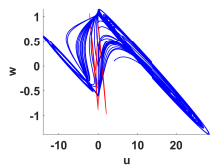
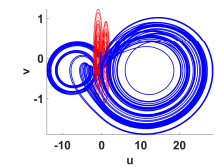
-Roughly equivalent.

Scaling and translation ($b = d = 0$)

$a = e = 1, c = 0, f = 0.5$

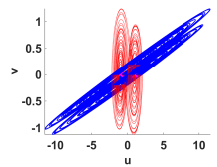


$a = 10, e = 1, c = 3, f = 0$

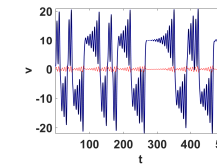
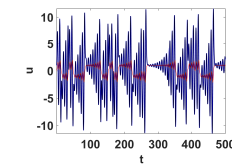
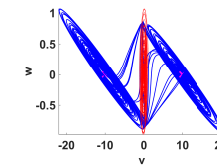


Shearing ($a = e = 1, c = f = 0$)

$b = 10, d = 0$



$b = 0, d = 10$



- Overcome the limited range of translation only.

- Not equivalent.

- Increased sensitivity is maintained.

- Roughly equivalent when either b or d is varied.

- Increased sensitivity when both are varied together.

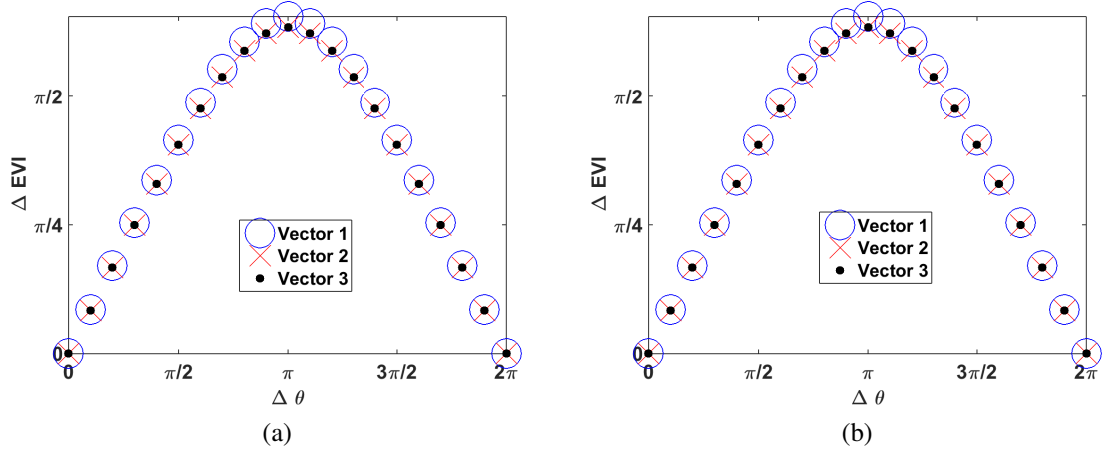


Figure 4.2: EVI against θ at the (a) first and (b) second equilibrium points.

4.2.2 Validation Example 2: Generalized Lorenz System

Lorenz system is given by:

$$\dot{x} = 10(y - x), \quad \dot{y} = (28 - z)x - y, \quad \dot{z} = xy - \frac{8}{3}z. \quad (4.7)$$

Transformed Lorenz system can be obtained similarly, where for example:

$$\begin{aligned} \dot{u} = & -\frac{10}{\alpha}a((u - c)(d + e) - (v - f)(a + b)) \\ & + \frac{b}{\alpha}((u - c)(d + (28 - w)e) - (v - f)(a + (28 - w)b)) + c, \end{aligned} \quad (4.8)$$

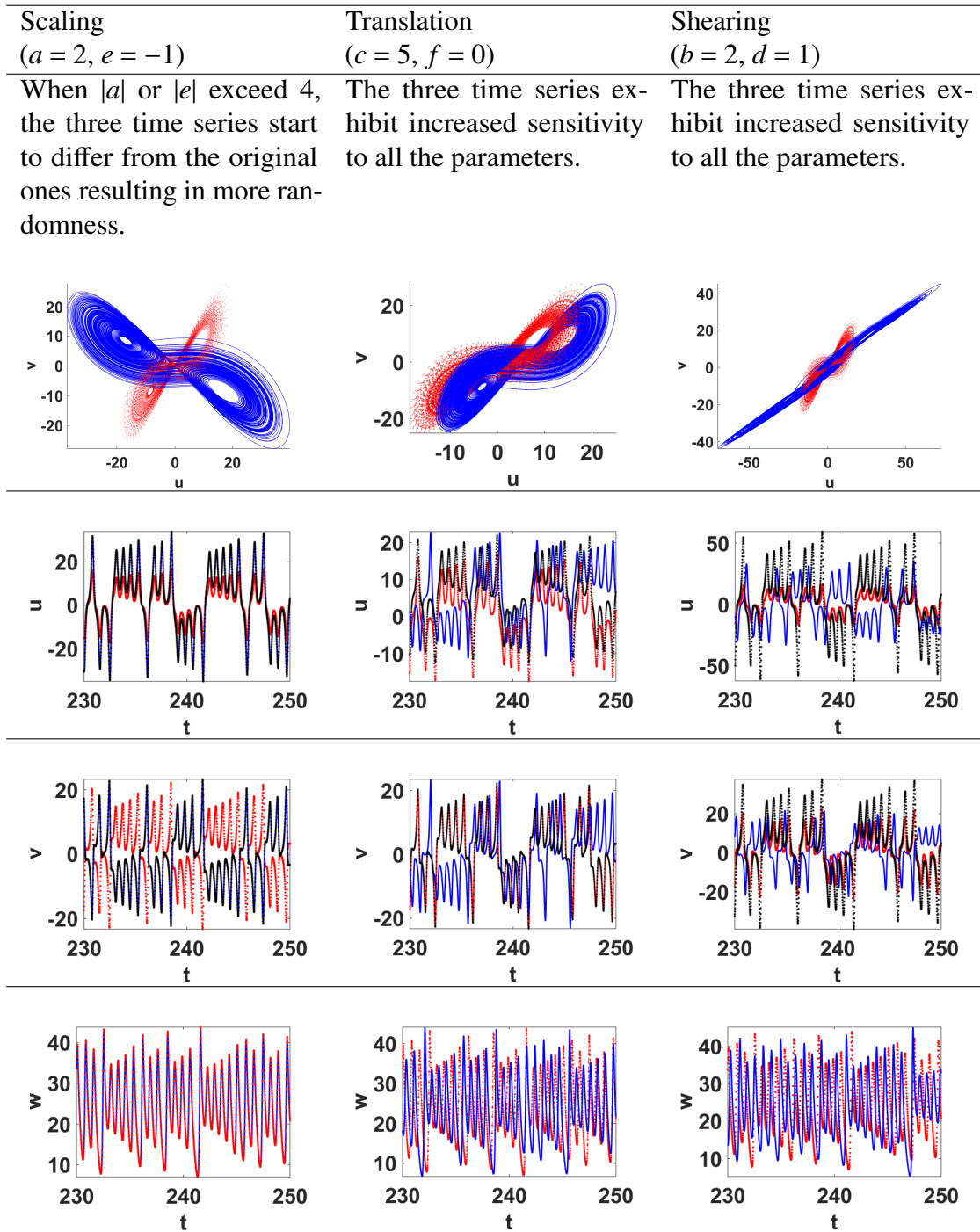
Table 4.3 shows the scaling (reflection), translation and shearing transformations of Lorenz system. Chaotic time series is identified using LEs, which quantify the divergence and convergence properties of an attractor [2]. Using Wolf's algorithm as implemented in [156], the system is shown to exhibit chaotic strange attractors since the MLE is finite positive against the parameters corresponding to the different cases as shown in Fig. 4.3.

4.3 Trajectory Control by Dynamic Translation

The translation parameters c and f can be used to move the equilibrium points and, hence, the attractor diagram. The translation along x -axis, c , can be changed in a piece-wise manner giving sufficient time for each value. In addition, the translation along y -axis, f , is given as a function of c , which is the trajectory. The scaling parameters are kept to control the output range and simplify the visualization of results. Scaled and translated system can be obtained by setting $b = d = 0$ in (4.8) yielding:

$$\begin{aligned} \dot{u} = & -\frac{10}{e}(e(u - c) - a(v - f)) + c, \\ \dot{v} = & \frac{1}{a}((u - c)((28 - w)e) - a(v - f)) + f, \\ \dot{w} = & -\frac{1}{ae}(u - c)(v - f) - \frac{8}{3}w. \end{aligned} \quad (4.9)$$

Table 4.3: Attractor diagrams and time series of (4.8)



As previously mentioned, the derivative of such non-autonomous parameters can be considered zero, since the angular frequency of the multi-level pulse signals is sufficiently small compared with the chaotic oscillator. Figure 4.4 shows different trajectories that the system follows dynamically in discrete steps. To be capable of visualizing the dynamic translation of the attractor, scaling parameters are used to control the output range. For Lorenz system, the output ranges are wide, hence, the scaling parameters a and e are set to values less than one. However, the translation parameters c and f have limited ranges that

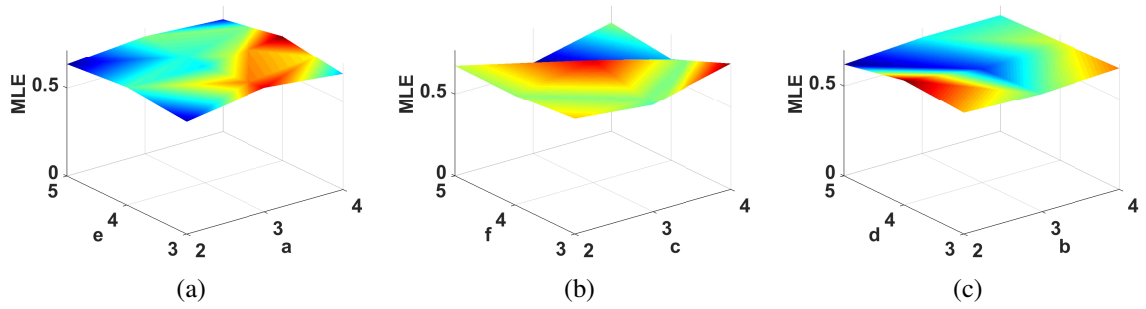


Figure 4.3: MLE of (4.8) against the parameters in (a) Scaling, (b) Translation and (c) Shearing cases.

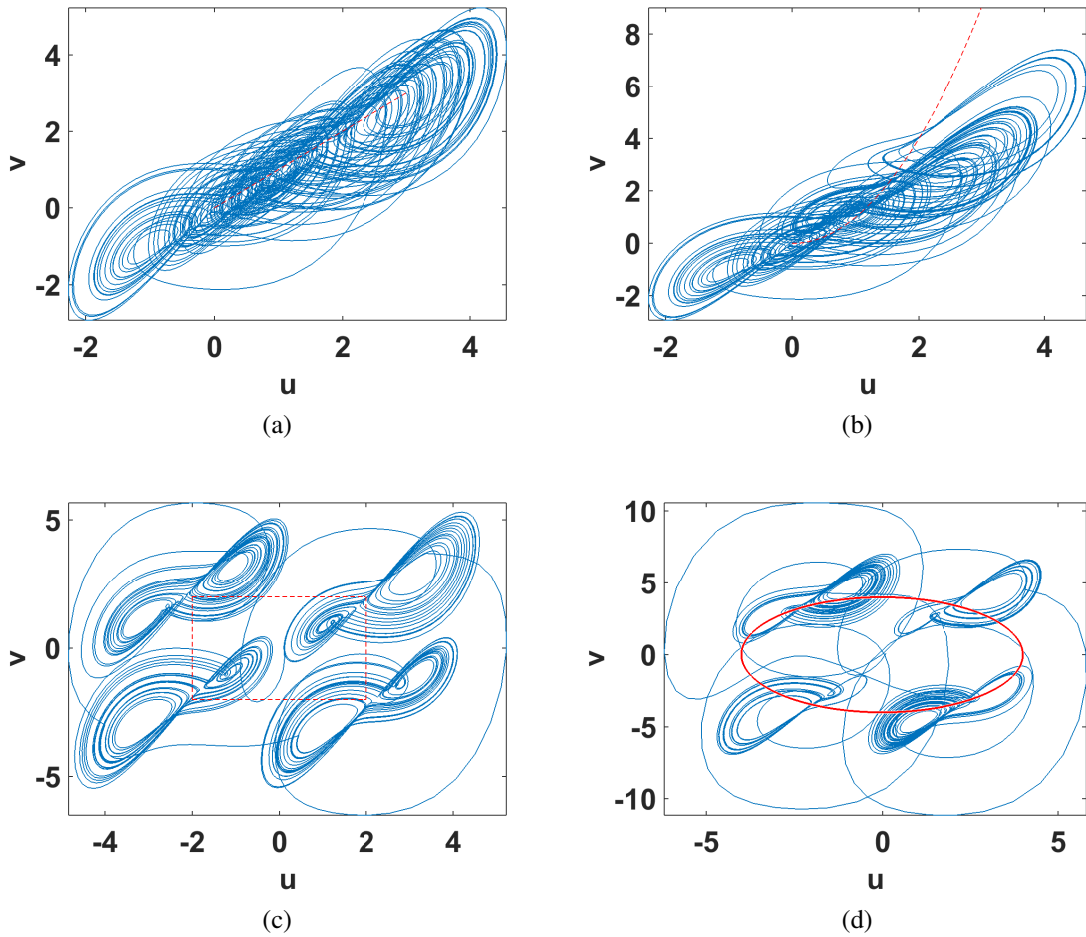


Figure 4.4: Trajectory control of transformed Lorenz chaotic system by scaling and translation for (a) line $f = c$, (b) parabola $f = c^2$, (c) a square and (d) a circle of radius 4 ($c^2 + f^2 = 16$) at $a = e = \frac{1}{8}$.

correspond to chaotic behavior as shown in the bifurcation diagrams of Fig. 4.5. Hence, it is more suitable to have a closed trajectory rather than open ones, which resembles multiple versions of the same attractor generated along a curve of [58].

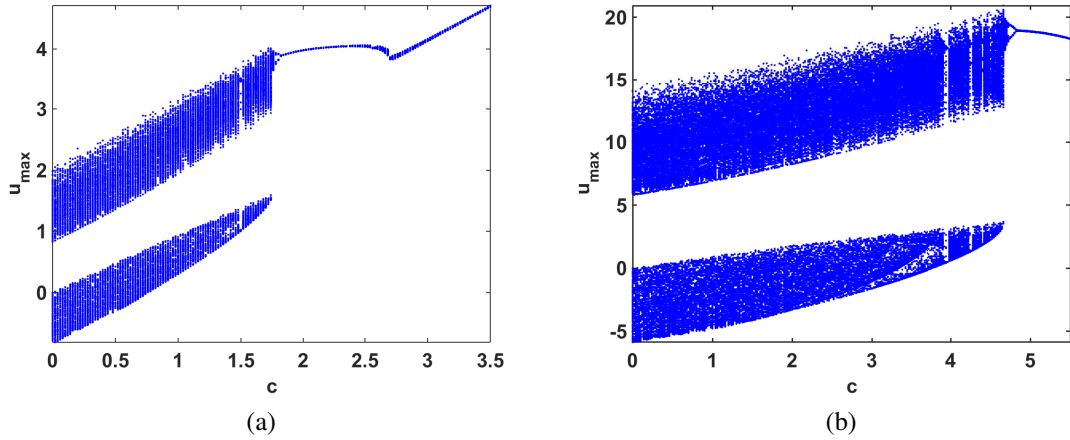


Figure 4.5: Bifurcation diagrams of transformed Lorenz chaotic system against the translation parameter c for the parabolic trajectory $f = c^2$ and different values of the scaling parameters (a) $a = e = 0.1$ and (b) $a = e = 0.7$.

Table 4.4 shows a continuous motion of the attractor along different trajectories, where [159] provides more examples of plane curves. This is achieved by keeping c constant for a period of time, such that it is sufficient to plot a clear part of the diagram. Then, the value of c is changed a little bit and so on in gradual steps that take the shape of staircase. The parameter c can be generated using the equation:

$$c(t) = \sum_{i=1}^n A(i)(H(t - B(i)) - H(t - B(i + 1))), \quad (4.10)$$

where $H(t)$ is the unit step or Heaviside function given by:

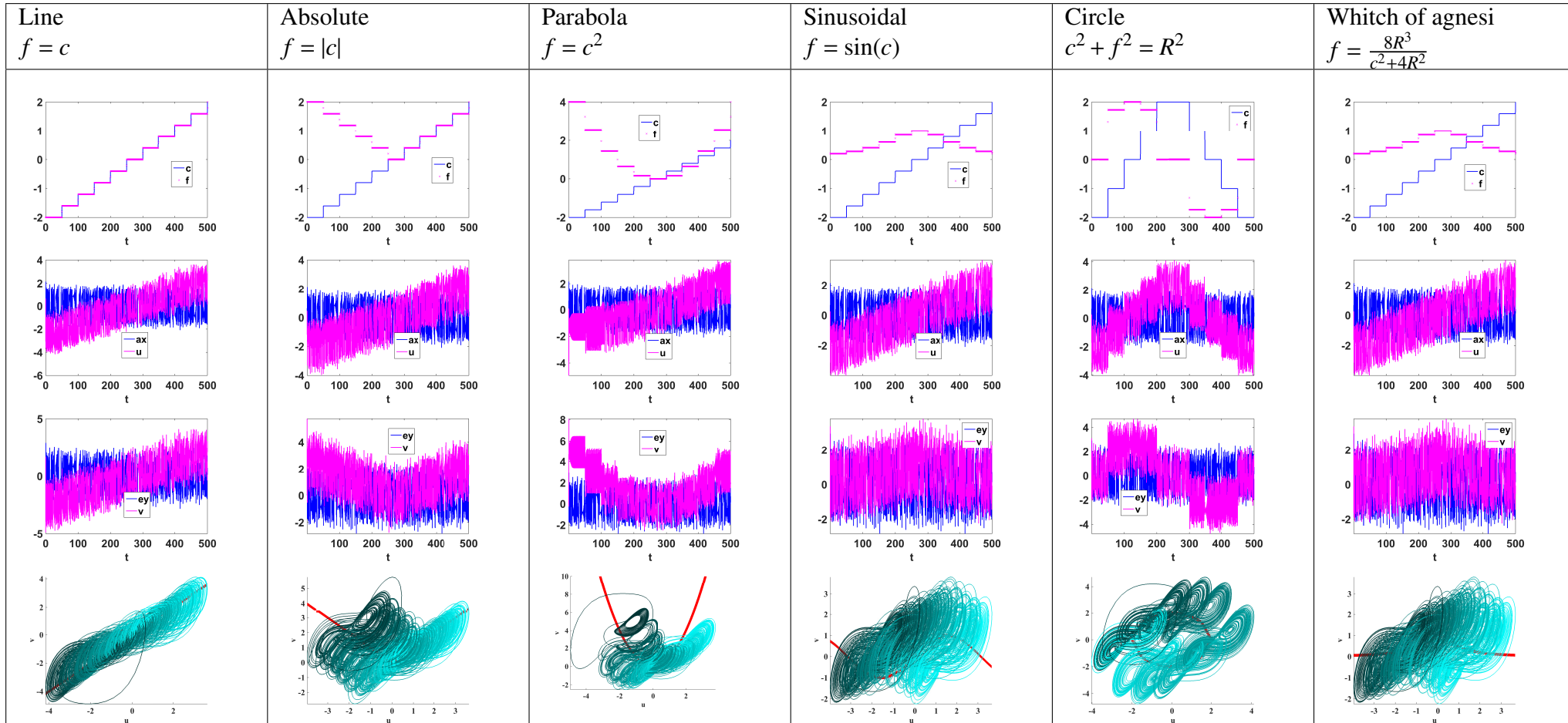
$$H(t) = \begin{cases} 1, & t \geq 0 \\ 0, & t < 0 \end{cases}, \quad (4.11)$$

A and B are vectors that correspond to the gradual amplitudes and stop times of the stairs of the resulting stair case plot. The first and last elements of the vector c equal those of A , respectively. The other translation parameter f is changed accordingly using the prescribed trajectory equation. In the examples of Table 4.4, the amplitudes of c are in the interval $[-2, 2]$ and the step by which they vary equals 50 time units in a total simulation time of 500 time units. The resulting time series of (4.9) are compared to the scaled time series of the conventional Lorenz system. The resulting attractor diagrams follow the prescribed trajectories, which are light/red colored. The intensity of the strange attractor color varies with time, where the darker points are plotted first and becomes brighter as time advances.

4.4 PRNG and Image Encryption Application

This section studies the performance of transformed Lorenz system, compared to Lorenz system, as a PRNG in an image encryption application. Three standard 1024×1024 color

Table 4.4: Trajectory control of (4.9) for $a = e = 0.1$ and different dynamic c and f parameters



images: Lena, mandril and peppers [160] are used for testing the encryption scheme. While Lena image is firstly used in comparing the Lorenz and transformed Lorenz systems performance in the scheme with detailed results, performance metrics are averaged for the three color channels of the two other images.

4.4.1 Encryption and Decryption Schemes

Figure 4.6 shows a simple image encryption scheme with both permutation and substitution phases, which was presented in [11]. Permutation of the original image is performed through generalized Arnold's map [161], where the new pixel location is given by:

$$\begin{bmatrix} \text{row} \\ \text{col} \end{bmatrix}_{\text{new}} = \begin{bmatrix} 1 & \gamma \\ \beta & 1 + \gamma\beta \end{bmatrix} \begin{bmatrix} \text{row} \\ \text{col} \end{bmatrix}_{\text{old}} \text{mod}(N) + \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad (4.12)$$

for an $N \times N$ image. The generalized Arnold's map permutation parameters γ and β are computed as:

$$\begin{aligned} \gamma &= \text{mod}(P_{\text{sum}} + \gamma_{\text{key}}, N - 1) + 1 \\ \beta &= \text{mod}(P_{\text{sum}} + \beta_{\text{key}}, N - 1) + 1 \end{aligned} \quad (4.13)$$

where mod returns the remainder, γ_{key} and β_{key} are the key parts of the permutation parameters and chosen as 73 and 35, respectively and the value P_{sum} is the same input dependent term of Chapter 3, except where stated otherwise.

In the substitution phase, the chaotic generator is either Lorenz or transformed Lorenz with the chaotic time series shown in Fig. 4.7. The correlation coefficients between the u , v and w and the corresponding x , y and z time series are -0.0054 , -0.0051 and 0.0038 . The systems are solved by Euler numerical technique using a time step of 0.01. The outputs x (u), y (v) and z (w) are then scaled, quantized and the LSBs are Xored with the permuted image pixel and the previously encrypted pixel, recalling the multiplexing

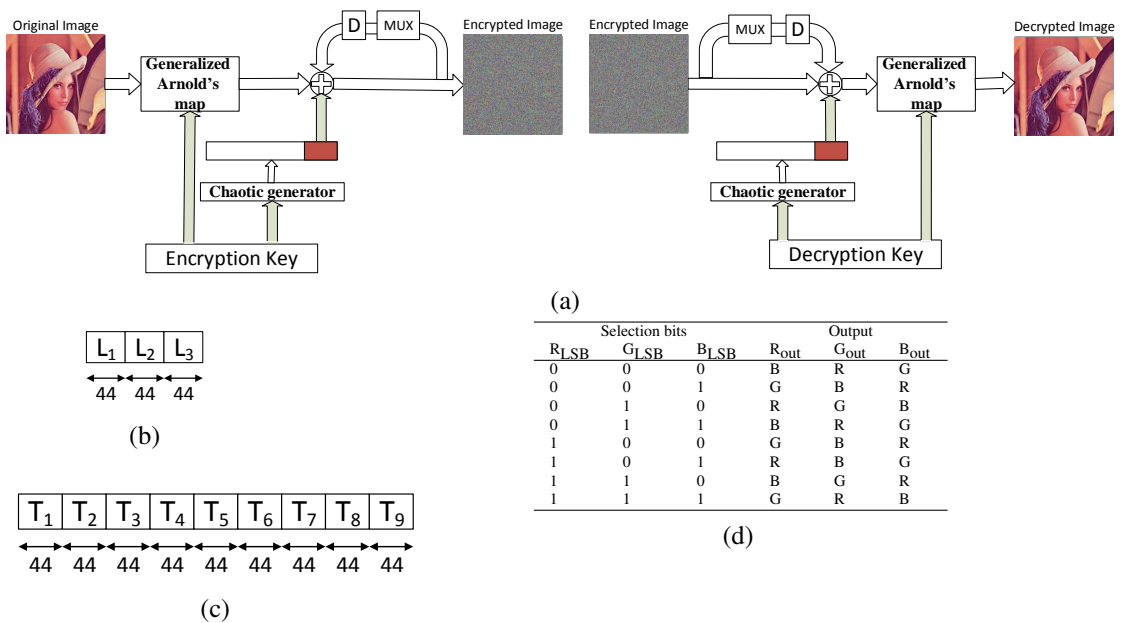


Figure 4.6: (a) Encryption/decryption block diagrams, encryption/decryption key for (b) Lorenz and (c) transformed Lorenz chaotic generators and (d) multiplexing table.

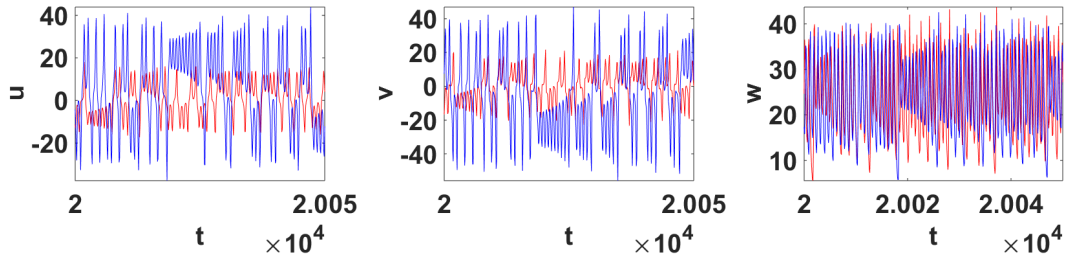


Figure 4.7: Time series of Lorenz, light colored, and transformed Lorenz, dark colored, at $a = 2$, $b = 0.25$, $c = 3$, $d = -0.5$, $e = -2$, $f = -4$, $x_0 = y_0 = z_0 = w_0 = 0.1$ $u_0 = 3.225$ and $v_0 = -0.425$.

technique of Chapter 3. The encryption key determines the parameters of the chaotic generator where it consists of three sub-keys for Lorenz system compared to nine sub-keys using transformed Lorenz system.

Decryption is straightforward as the reverse process shown in Fig. 4.6(a). First, an exact duplicate of the same substitution stage is carried out on the encrypted image. Then, the resulting image is permuted by generalized Arnold's map to return the pixels to their original locations and get the correctly decrypted image.

4.4.2 Performance Evaluation

The performance of the scheme is evaluated through the PRNG properties, encrypted image histogram and its uniformity through chi square test, pixel correlation, MSE, entropy, PSNR, NIST tests, key space, key sensitivity, resistance to differential, ciphertext-only, known plaintext, and chosen plaintext attacks, robustness against noise and computation time comparing Lorenz to transformed Lorenz systems as the chaotic generator. Equations of the performance metrics were given in Table 3.16 of Chapter 3.

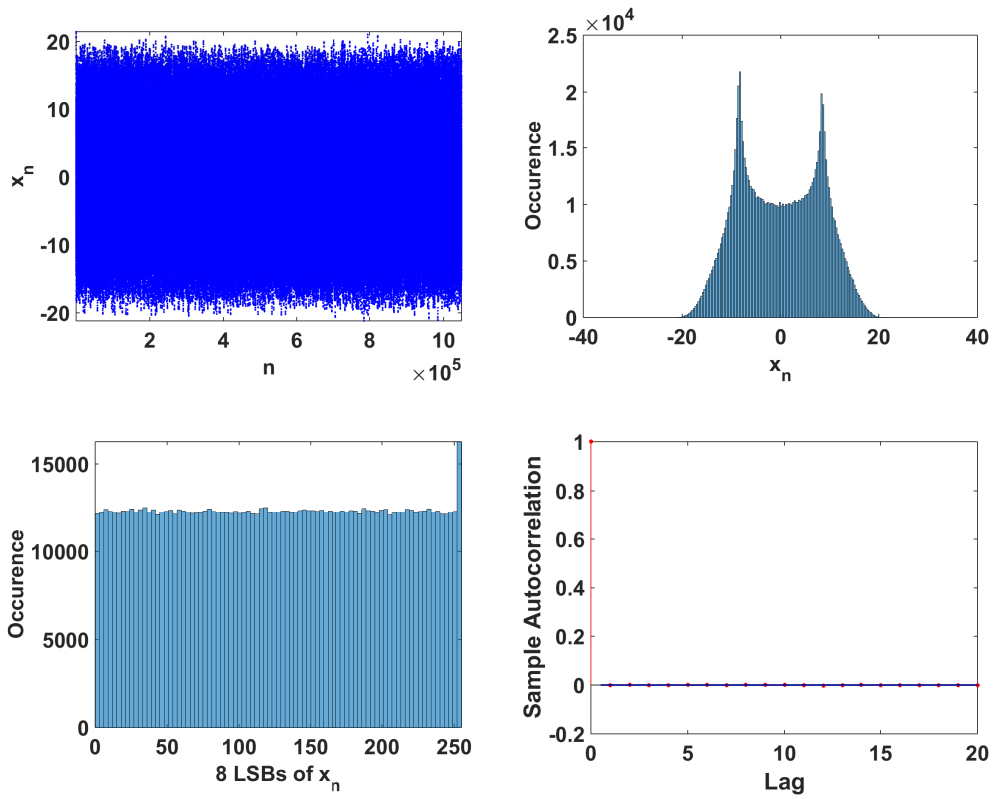
4.4.2.1 PRNG Properties

Figure 4.8 compares the randomness properties of the chaotic sequence generated from Lorenz and transformed Lorenz systems. For a good chaotic sequence, the histogram should be nearly flat or uniform and the adjacent samples should be completely uncorrelated. From Fig. 4.8, it can be inferred that both systems satisfy the requirements, where the nearly aperiodic chaotic sequence has nearly flat frequency distribution. Hence, the transformed Lorenz system provides more control of the Lorenz attractor and is still random and suitable for encryption applications.

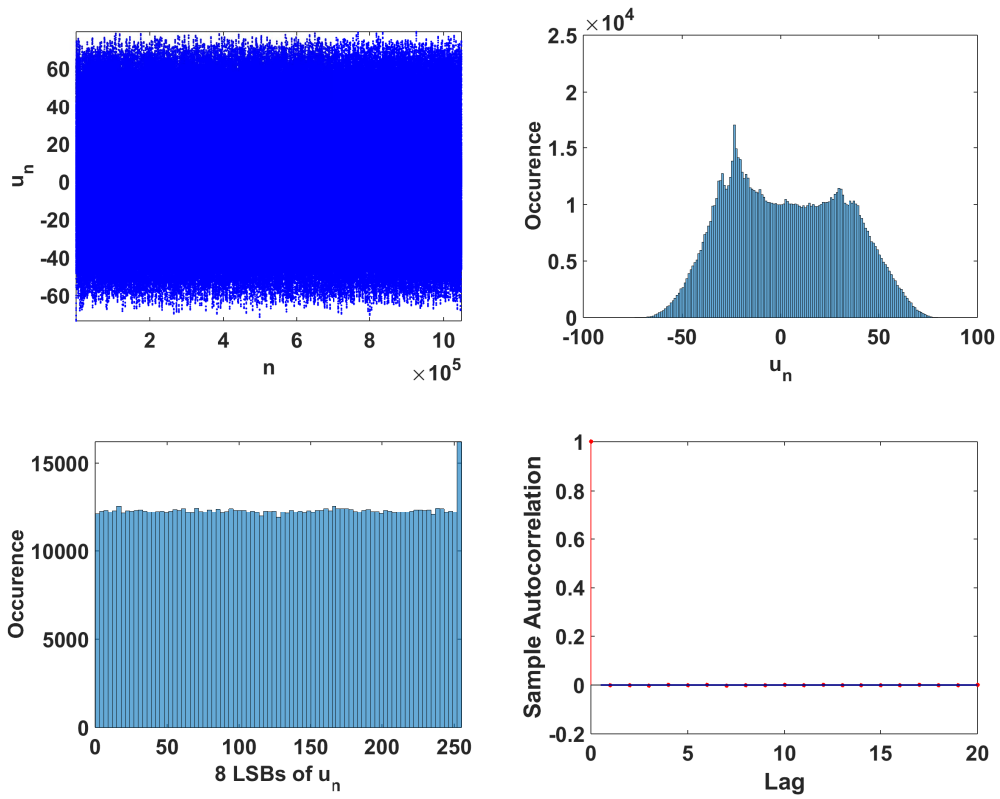
Table 4.5 shows that the PRNGs based on both Lorenz and transformed Lorenz successfully pass NIST tests.

4.4.2.2 Perceptual and Statistical Tests

The encrypted images corresponding to the two chaotic generators are random as shown in Fig. 4.6 as well as Fig. 4.9. In addition, the corresponding histograms reveal a uniform intensity distribution compared to the nonuniform histograms of the original image as shown in Fig. 4.10. To further check the degree of deviation from uniform histogram



(a)



(b)

Figure 4.8: Time series, frequency distribution of the outputs and histogram of the PRNG using (a) Lorenz and (b) transformed Lorenz chaotic generators.

Table 4.5: NIST results for the PRNG and encrypted images

PRNG				Encrypted Lena				Enc. mandril		Enc. peppers	
Lorenz		Transformed		Lorenz		Transformed		Transform.		Transform.	
PV	PP	PV	PP	PV	PP	PV	PP	PV	PP	PV	PP
✓	1	✓	1	✓	0.979	✓	1	✓	0.979	✓	1
✓	0.917	✓	1	✓	1	✓	1	✓	1	✓	0.958
✓	1	✓	0.979	✓	1	✓	1	✓	0.979	✓	0.979
✓	1	✓	1	✓	0.958	✓	1	✓	1	✓	1
✓	0.958	✓	0.958	✓	1	✓	1	✓	1	✓	1
✓	0.958	✓	0.958	✓	1	✓	1	✓	1	✓	1
✓	1	✓	1	✓	1	✓	1	✓	1	✓	1
✓	0.990	✓	0.992	✓	0.989	✓	0.989	✓	0.986	✓	0.989
✓	1	✓	1	✓	1	✓	1	✓	1	✓	0.917
✓	1	✓	1	✓	1	✓	0.958	✓	0.917	✓	1
✓	1	✓	1	✓	1	✓	1	✓	0.958	✓	1
✓	1	✓	1	✓	1	✓	1	✓	0.993	✓	0.979
✓	0.996	✓	0.992	✓	1	✓	0.980	✓	0.977	✓	1
✓	1	✓	1	✓	1	✓	1	✓	1	✓	0.917
✓	1	✓	0.958	✓	1	✓	1	✓	1	✓	1
Passed		Passed		Passed		Passed		Passed		Passed	



Figure 4.9: Original and encrypted (a) mandril and (b) peppers images.

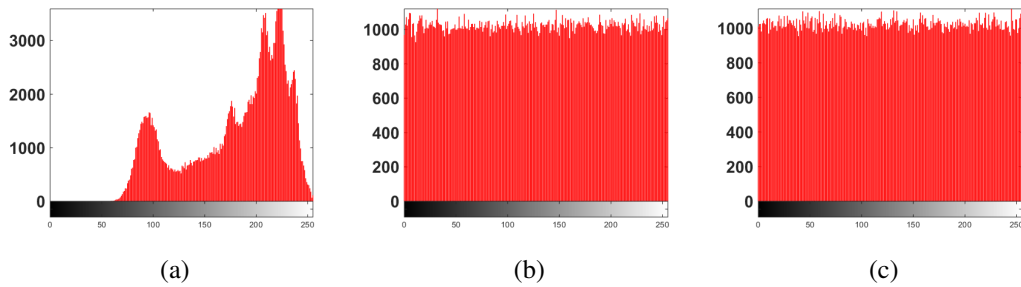


Figure 4.10: Histograms of the red channel of (a) Lena image and the corresponding encrypted images using (b) Lorenz and (c) transformed Lorenz systems.

analysis, chi-square test [162] is used. The less the chi-square value, the better the uniformity. Table 4.6 gives the results for the encrypted image using both Lorenz and transformed Lorenz, where both have relatively low values compared to that of the original image of $O(10^6)$.

Table 4.6 shows the ability of the system to destroy the horizontal, vertical and diagonal correlation between the pixels where the correlation coefficients of the encrypted image approach zero. High MSE, Entropy approaching 8 and low PSNR further indicate the randomness and unpredictability of the encrypted image.

Table 4.5 also examines the randomness of the encrypted images by evaluating the PV and PP of NIST and they successfully pass the tests.

4.4.2.3 Key Space and Key Sensitivity

Key space is defined as the number of encryption keys that are available in the cryptosystem. The maximum key space is determined by sensitivity analysis. Sensitivity of Lorenz system for perturbations in the initial conditions is as follows $\Delta x_0, \Delta y_0 \geq 10^{-17}$ and $\Delta z_0 \geq 10^{-16}$. Sensitivity of transformed Lorenz system for perturbations in the initial conditions and parameters is as follows $\Delta x_0, \Delta y_0 \geq 10^{-15}$, $\Delta z_0 \geq 10^{-17}$, $\Delta a \geq 10^{-15}$, $\Delta b \geq 10^{-16}$, $\Delta c \geq 10^{-15}$, $\Delta d \geq 10^{-16}$ and $\Delta e, \Delta f \geq 10^{-15}$.

The initial conditions and parameters of the chaotic generator consist of a fixed part and a key part, which is determined from the sub-keys denoted by L for Lorenz system and T for transformed Lorenz system as shown in Figs. 4.6(b) and (c). For example, $x_0 = x_{fix} + \Delta x_0$, where Δx_0 equals L_1 multiplied by a scaling factor and similarly for the rest of the parameters. The fixed parts are set to the values of Fig. 4.7. To ensure high key sensitivity, a minimum perturbation of 10^{-14} is specified. Hence, each sub-key is limited to 44 bits using a scaling factor of 10^{-13} . Consequently, the key space of transformed Lorenz system equals 2^{396} compared to 2^{132} of Lorenz system, which is equivalent to 3 times increase in the number of bits.

Table 4.6 gives the values of high MSE and Entropy approaching 8, which indicate the randomness and unpredictability of the wrong decrypted image when the LSB of the sub-key Δx_0 (or Δu_0) is changed. Similar results are obtained for the rest of the sub-keys. An advantage of the encryption system is that perturbation in any parameter affects the three time series and, hence, the three channels unlike encryption systems based on independent discrete maps for each channel [11].

4.4.2.4 Resistance to Differential Attacks

Table 4.6 shows the values of the NPCR and UACI averaged over 20 trials in which one pixel in the original image is changed, which successfully approach 100% and 33.3%, respectively [11].

4.4.2.5 Resistance to Other Cryptanalysis Attacks

Cryptanalysis is the process of studying encryption systems with the intention of revealing their weaknesses and establishing the appropriate attacking schemes [163]. Other famous cryptanalysis techniques, besides brute force and differential attacks, are the ciphertext-only, known plaintext, chosen plaintext and side channel attacks. However, they are

Table 4.6: Performance metrics of the scheme for three encrypted images

Test		Lena (Lorenz)			Lena (Transformed)			Mandril	Peppers
		R	G	B	R	G	B		
$\chi_{\text{test}}^2 (\times 10^2)$		2.4808	2.505	2.6253	3.2239	2.5216	2.8009	2.6778	2.4336
ρ ($\times 10^{-4}$)	Horizontal	-0.0626	-0.0634	0.0227	-6.7144	-20.8894	-19.0264	8.0344	-1.0496
	Vertical	13.7072	-5.8588	0.8549	-8.8684	2.7001	-3.9709	3.2939	-1.1189
	Diagonal	-15.6653	-1.6203	-8.1332	-4.7629	-9.1812	-3.6888	0.3586	0.0903
MSE	($\times 10^3$)	10.6217	9.0629	7.0821	10.6636	9.0617	7.0824	8.7107	8.7984
Entropy		7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
PSNR		7.8689	8.5581	9.6292	7.8517	8.5587	9.6291	8.7537	5.7898
Key Sens. ($\Delta x_0, \Delta u_0$)	MSE($\times 10^3$)	10.6606	9.0569	7.1293	10.6599	9.0727	7.1136	8.7019	8.0343
	Entropy	7.9994	7.9993	7.9993	7.9993	7.9993	7.9992	7.9991	7.9992
DA	NPCR	99.6061	99.6091	99.6104	99.6094	99.6126	99.6121	99.6101	99.6096
	UACI	33.4859	33.4993	33.4859	33.4726	33.4834	33.4571	33.4582	33.4593

Table 4.7: Chosen plaintext attack/known plaintext attack analysis

	1	2	3	4	1	1	1	1	255	255	255	255
$4 \times 4 \times 3$	1	2	3	4	1	1	1	1	255	255	255	255
plainimage	1	2	3	4	1	1	1	1	255	255	255	255
	1	2	3	4	1	1	1	1	255	255	255	255
	2	233	184	203	147	137	125	187	73	33	53	97
$4 \times 4 \times 3$	141	163	166	245	94	238	193	217	169	119	28	163
cipherimage	34	223	68	190	21	69	189	150	222	106	220	184
	239	42	192	231	32	135	236	205	177	36	101	55

less frequently investigated when proposing a new encryption scheme, especially for chaos-based ciphers.

In ciphertext-only attack, the attacker has access only to a ciphertext or a collection of ciphertexts with the objective of finding the plaintext image and/or the secret key. This requires the use of brute force [164], and hence, the large key space and the encryption key design such that it depends on the plaintext image are effective means of enhancing the scheme's resistance to this attack.

In known plain text attack, the attacker has a ciphertext or a set of ciphertexts for which the corresponding plaintext is also known with the objective of finding the secret key. Chosen plaintext attack gives more flexibility to an attacker by allowing plaintext to be selected observing the corresponding ciphertext. To depict the capability of the proposed scheme in eliminating all traces of chosen patterns in a plainimage, a $4 \times 4 \times 3$ image was encrypted similar to [104]. The resulting pixel values after before and after encryption are shown in Table 4.7, where any specific patterns, white or black images are fully randomized after encryption with no observable patterns. This is owed to the presence of both permutation and substitution stages, key sensitivity and plainimage sensitivity properties of the scheme.

4.4.2.6 Robustness Against Noise

The encrypted images may suffer from noise effects during transmission from transmitter to receiver such as: Additive White Gaussian Noise (AWGN) and Salt and Pepper (S & P) noise [165]. To enhance the robustness of the scheme against noise, some input dependent terms in the encryption scheme can be modified. For example, Figs. 4.11(a) and (b) show the decrypted images corresponding to Lena for AWGN of mean 0 and different variances and S & P of different densities, respectively, when $P_{sum} = 0$ and the MUX is removed. The correlation coefficients between the noiseless decrypted image and the noisy one are also given. The robustness against noise can be identified by the capability of perceptually identifying the image content and the correlation coefficient values approaching one.

4.4.2.7 Time Analysis

Our main concern is the time consumed in the solution of the system of differential equations in the substitution phase. Simulations are performed using Matlab 8.4.0.150421 (R2014b) and Windows 8.1 on an Intel(R) Core(TM) i7-4510U CPU @ 2.00 GHz machine. Averaged over 10 trials, around 46.81 % increase in the computation time of transformed



Figure 4.11: Decrypted images and correlation coefficients corresponding to Lena for (a) AWGN of mean 0 and different variances and (b) S & P of different densities when $P_{sum} = 0$ and MUX is removed.

Lorenz than Lorenz system is reported. This is associated with the gain of about 3 times increase in the maximum number of bits of the substitution part in the encryption key with nine sub-keys each with high sensitivity.

4.4.3 Discussion and Comparison Against Other Works

The image encryption scheme utilizing the proposed transformed Lorenz system is compared to other recent image encryption schemes [101–104], which utilized chaotic systems and included separate transformation stages as well. The basic idea and main blocks utilized in each scheme are given in Table 4.8, where only [103] embedded chaotic maps in a cosine transformation to generate equation of a new chaotic map. All the utilized chaotic generators were simple low-dimensional chaotic maps. On the other hand, the proposed transformed Lorenz system is based on differential equations allowing increased complexity, sensitivity and further enhanced chaotic properties. The capability of generating three chaotic outputs simultaneously makes it more suitable for color image encryption applications. Table 4.8 also compares the schemes from the viewpoint of the performance metrics evaluated in each paper. While both [103, 104] gave a clear description of the

Table 4.8: Comparison of the ideas and evaluation of different image encryption schemes

Ref.	Main Blocks	Statistical				Key		DA	Other attacks	Time Analysis
		Corr.	Hist.	χ_{test}^2	NIST	Space	Sens.			
This work	Transformed Lorenz and Arnold map	✓	✓	✓	✓	✓	✓	✓	✓	
[101]	Affine Hill cipher and Arnold transform	✓	✓	—	—	from parameters		—	—	
[102]	Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS), skew tent map and affine transform	✓	✓	—	—	from parameters		✓	—	
[103]	Cosine-Transform-Based Chaotic System (CTBCS)	✓	✓	—	—	✓	✓	✓	—	
[104]	A chaotic map perturbed by another using either logistic, sine or tent maps	✓	✓	—	—	✓	✓	✓	known-plaintext/ chosen-plaintext	

key design, space and sensitivity analysis, [101, 102] only mentioned the parameters from which the key can be composed and assessed sensitivity by slightly modifying the parameter value. Such preliminary analysis neglects that the effective key space is governed by the basin of attraction and parameter basin of attraction which correspond to chaotic behavior [140] and the remarkable importance of Least Significant Bit (LSB) sensitivity. While none of the compared works performed chi-square or NIST tests, all of them presented differential attack and time analyses except [101]. None of the other cryptanalysis attacks or robustness against noise were analyzed except in [104], which discussed known- and chosen-plaintext attacks.

As for the papers reviewed in Chapter 2 on generalization and control of chaotic systems, only three of them presented grayscale image encryption applications. The scheme presented in [23] was evaluated using encrypted image, histogram, entropy and parameter sensitivity. The same performance metrics were used to evaluate the scheme presented in [56] except that entropy was replaced by correlation. Histogram, correlation and entropy metrics were included in [58].

4.5 Extension to 3D and Fractional Systems with Hidden Attractors

This section extends the affine transformations-based control technique to three-dimensional space and to be applicable for hidden attractors in fractional-order systems. The proposed transformation framework overcomes the limitations imposed by the unique properties of hidden attractors. Generally, an appropriate controlling scheme must be cautious with the increased sensitivity of the dynamical behavior of hidden attractors if the chaotic dynamics are required to be maintained.

The first addressed limitation is that some analog circuit implementations require specific voltage level and/or polarity of the chaotic signals. The proposed transformation framework enables such control by time series scaling, reflection and offset, which correspond to attractor size, polarity, and position control. In previous researches on amplitude control and offset boosting, multiplicative and additive parameters, respectively, were inserted selectively in terms of the governing equations. On the other hand, the proposed systematic coordinate transformation provides a more generic control technique, which is applicable to any system. Phase and shape of the attractor are also shown to be controllable through rotation and skewing. Few recent researches employed rotation, yet, for self-excited attractors instead. Orientation control through skewing/shearing was not employed before in the field of chaotic attractor control. All these transformations are shown not to endanger the chaotic dynamics of the original systems by means of strange attractors, spectral entropy and bifurcation diagrams. The unpredictability of time series is enhanced due to the mutual coupling between state variables and that one of them undergoing transformation affects the rest when solving the governing equations.

The second addressed limitation is the unsuitability of the conventional multi-wing generation techniques, which extend the equilibrium points, for hidden attractors with no equilibria. Non-autonomous parameter approaches are utilized to generate multiple wings around the same center point using multi-level pulse signals as scaling, reflection, rotation and skewing parameters. In addition, non-autonomous translation parameters are used to

generate distributed self-reproduced attractors along an arbitrary line, curve or surface.

The third addressed limitation is that hidden attractors have very narrow, mostly specific single value, basin of attraction, parameter basin of attraction and fractional-orders. The newly introduced parameters enable quite wide ranges and are suitable for constructing the encryption key in digital chaos-based encryption systems. Having up to twelve degrees of freedom provided by the extra parameters enables enlarging the key space and enhancing resistance to brute force attacks.

The works reviewed in Chapter 2 barely focused on hidden attractors control, but all of them were limited to integer-order chaotic systems. For example, static offset boosting was presented in [45, 166, 167] for systems with the specific conditions on offset boostable variables, but with hidden attractors. While dynamic offset boosting of hidden attractors was presented in [26], dynamic amplitude control was presented in [23, 43]. Systems with open curves, closed curves and surfaces of equilibria theoretically possess an infinite number of equilibrium points. Yet, being hidden attractors, the number of equilibrium points does not directly affect the number of scrolls. Hence, this technique is not generally considered as a method of attractor control or multi-wing generation.

4.5.1 Hidden Chaotic Attractors in Fractional-Order Systems

Table 4.9 provides a summary of researches on fractional-order systems with hidden attractors, which are noticeably fewer than fractional-order extensions of the conventional well-established systems with self-excited attractors. They are almost evenly distributed between systems of 3 and 4 differential equations. The proposed fractional-order systems cover different types of hidden attractors such as: no equilibria (the majority), one or more stable equilibria, a line or infinite number of equilibria, where one of the recent papers proposed three different types [168]. Table 4.9 also gives the minimum fractional-orders that were reported to generate chaos for the reviewed systems, with single value for systems with commensurate orders and all fractional-orders when incommensurate cases were given. Around half of these researches reported chaotic behavior only for fractional-orders close to the integer case, i.e., $q > 0.98$. Some of the systems exhibit unique interesting properties such as no reporting of chaotic behavior for the equivalent integer-order system in [169] and complicated nonlinear terms, e.g., cubic [170] and exponential [45].

Two systems were selected to validate the transformation framework proposed in this paper. The first system from [176] is given by:

$$\begin{aligned} D^{q_1} x &= y, \\ D^{q_2} y &= -x - yz, \\ D^{q_3} z &= xy + 2.5|x| - 1.35, \end{aligned} \tag{4.14}$$

which yields low frequency chaotic time series and a familiar double-scroll-shaped attractor when starting from initial values (0, 0.1, 0) and the second system from [178] is given by:

$$\begin{aligned} D^{q_1} x &= yz + x(y - 0.35), \\ D^{q_2} y &= 1 - |x|, \\ D^{q_3} z &= -xy - z, \end{aligned} \tag{4.15}$$

with higher frequency chaotic time series and an irregular-shaped attractor when starting from initial values (1, 1, 1). The constants 2.5 and 1.35 in (4.14) and 0.35 in (4.15)

Table 4.9: Summary of Hidden Chaotic Attractors in Fractional-Order Systems

Ref.	Dim.	Equilibria	Fractional-Orders
[171]	4	none	(0.80,0.85,0.88,0.81)
[172]	3	none	0.98
[169]	4	none	0.8
[173]	4	none	0.96
[174]	3	none	0.992
[45]	4	none	0.95
[170]	4	none	0.91
[78]	3	infinite number	0.98
[175]	3	none	0.9
[176]	3	none	0.9
[177]	3	two stable	(0.98,0.99,0.99)
[178]	3	none	0.97
[179]	3	none	0.982
[180]	3	two stable	0.988
[166]	4	none	0.98
[167]	4	none	0.9
[181]	4	none	0.985
[168]	4	a line of unstable none single stable	0.82 0.9 0.99

are the values of the main system parameters corresponding to chaotic behavior [176, 178]. Fractional-order chaotic systems are solved numerically using GL method [31] as previously explained in Section 3.2.4 of Chapter 3.

4.5.2 3D Affine Transformations in Fractional Systems

Consider the three-dimensional fractional-order chaotic system given by:

$$D^q X = F(X), \quad (4.16)$$

where q is the fractional-order in case of commensurate order or vector of fractional-orders $[q_1 \ q_2 \ q_3]$ in case of incommensurate orders, $X = [x \ y \ z]^T$ is the vector of the original state variables, and $F(X) = [f_1(x, y, z) \ f_2(x, y, z) \ f_3(x, y, z)]^T$ are the functions on the right hand side.

A three-dimensional affine transformation of the form $U = AX + b$ is performed, where A is a non-singular matrix and $U = [u \ v \ w]^T$ is the transformed vector of state variables. Hence, the new transformed system is given by:

$$D^q U = A \left(F \left(A^{-1} (U - b) \right) \right),$$

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \quad b = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}, \quad (4.17)$$

For an identity A matrix and zero b vector, the transformed system (4.17) reduces to the original system (4.16). The transformation considers the attractor diagram as a geometric shape and applies the well-established affine transformations to it. However, this does not take place as a post-processing technique for the chaotic time series. The transformation is embedded into the dynamic equations instead and is performed within the solution procedure. This guarantees mutual coupling between the different state variables and maintaining the sensitivity and unpredictability properties of chaotic generators on the long term evolution. That is, a transformation that relates u time series to x time series also affects v and w time series implicitly through (4.17) even if this does not appear in $U = AX + b$.

Using GL method of (3.9), the transformed system can be expressed by:

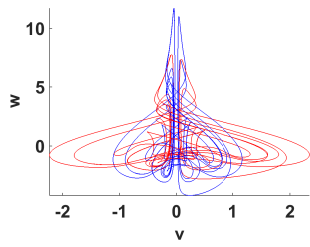
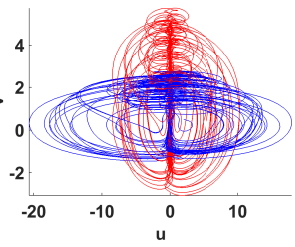
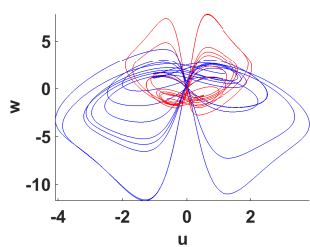
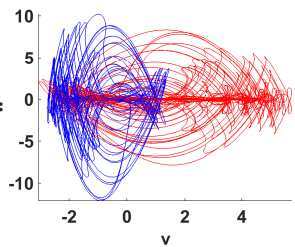
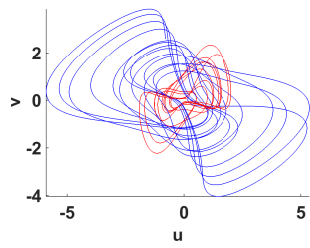
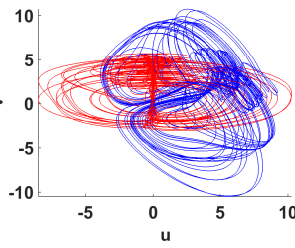
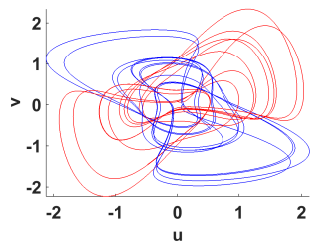
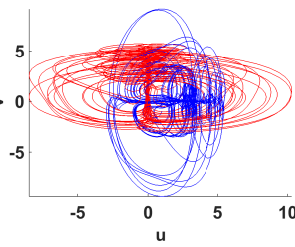
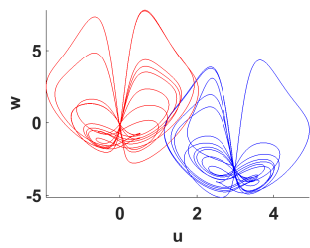
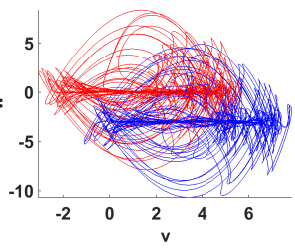
$$\begin{bmatrix} u_{i+1} \\ v_{i+1} \\ w_{i+1} \end{bmatrix} = \left(A \left(F \left(A^{-1} \left(\begin{bmatrix} u_i \\ v_i \\ w_i \end{bmatrix} - b \right) \right) \right) \right) \odot \begin{bmatrix} h^{q_1} \\ h^{q_2} \\ h^{q_3} \end{bmatrix} - \begin{bmatrix} \sum_{j=1}^i c_j^{(q_1)} u_{i-j+1} \\ \sum_{j=1}^i c_j^{(q_2)} v_{i-j+1} \\ \sum_{j=1}^i c_j^{(q_3)} w_{i-j+1} \end{bmatrix}, \quad (4.18)$$

where \odot represents the Hadamard (element-wise) multiplication of vectors. The twelve parameters in the matrix A and vector b provide controllability and degrees of freedom in the three spatial coordinates as detailed in the next section. The transformation treats the attractor as a shape that is almost trapped inside a cuboid with dimensions corresponding to the state space volume of the attractor. The diagonal elements of A provide scaling and reflection transformations and, together with the off-diagonal elements, they control skewing and reflection. The vector b provides translation transformation. Two-dimensional transformations can be achieved using (4.17) in two-dimensional planes controlling the shape of the attractor projection trapped in the rectangular projection of the cuboid. Furthermore, the procedure can be generalized to n -dimensional chaotic systems.

4.5.3 Autonomous Parameters

This section presents the special cases that can be achieved through (4.17) when A and b are constants or static parameters. These cases are summarized using the examples shown in Table 4.10 for autonomous time-invariant parameters, where the original and transformed attractor diagrams are light/red and dark/blue colored, respectively (see the online colored version). For scaling, both systems exhibit v time series and phase space dimension that is roughly an attenuated version of y multiplied by 0.5. However, this does not mean $v_i = 2y_i$, where more unpredictability is involved using the embedded transformation, but the effect appears in the range and attractor size. Similarly, u and w are roughly amplified versions of x and z by 2 and 1.5, respectively. Reflection acts similarly but results in a time series with inverted sign and mirror image of the phase space dimension about its corresponding axis. In skewing and rotation, u and v are affected by both x and y simultaneously. Skewing distorts the geometric shape, where the rectangle that encloses the attractor projection becomes a parallelogram. In the rotation example, this rectangle and the attractor are rotated by $\pi/2$ clockwise in the two-dimensional u - v plane considering the same placement of coordinate axes. Finally, translation shifts the

Table 4.10: Transformed Systems Special Cases Using Autonomous Parameters

Parameters A, b	Transformed system 1 ($q = 0.9$)	Transformed system 2 ($q = 0.97$)
<p>Scaling</p> $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 0.5 & 0 \\ 0 & 0 & 1.5 \end{bmatrix},$ $\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$		
SE_u	0.4064	0.4892
<p>Reflection</p> $\begin{bmatrix} -2 & 0 & 0 \\ 0 & -0.5 & 0 \\ 0 & 0 & -1.5 \end{bmatrix},$ $\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$		
SE_u	0.4064	0.4892
<p>Skewing</p> $\begin{bmatrix} 1 & 2 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$ $\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$		
SE_u	0.4516	0.3495
SE_v	0.4019	0.4911
<p>Rotation</p> $\begin{bmatrix} a_{11} & a_{12} & 0 \\ -a_{12} & a_{11} & 0 \\ 0 & 0 & 1 \end{bmatrix},$ $a_{11} = \cos(\pi/2), \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$ $a_{12} = \sin(\pi/2),$		
SE_u	0.4550	0.2847
SE_v	0.4047	0.5214
<p>Translation</p> $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$ $\begin{bmatrix} 3 \\ 2 \\ -3 \end{bmatrix}$		
SE_u	0.3832	0.5180

attractor diagram along the positive direction of the corresponding axis when the parameter is positive and vice versa.

4.5.3.1 Time Series Complexity Estimation

To evaluate the effect of transformations on the complexity and randomness of the chaotic signals, a complexity measure is needed. It is generally harder to evaluate such metrics for fractional-order chaotic systems, yet Spectral Entropy (SE) was used [182], especially for those with hidden attractors [167, 180]. SE represents an accurate and rapid method of chaos quantification from time series without much preprocessing. The normalized power spectrum is considered a probability distribution computing its entropy [182]. Larger SE values indicate a flatter power spectrum, which shows high complexity of the time series and its effectiveness when used in information security applications. First, the mean is subtracted from the time series using $x(n) = x(n) - \bar{x}$. Then, Discrete Fourier Transformation (DFT) is computed using:

$$X(k) = \sum_{n=0}^{N-1} x(n)e^{-j2\pi nk/N}, \quad (4.19)$$

where N is the length of the time series, $k = 0, 1, \dots, N-1$ and $j = \sqrt{-1}$. The probability of power spectrum $|X(k)|^2$ at frequency k is given by:

$$P_k = \frac{|X(k)|^2}{\sum_{k=0}^{N/2-1} |X(k)|^2}, \quad (4.20)$$

SE is given by:

$$SE = \frac{\sum_{k=0}^{N/2-1} |P_k \ln(P_k)|}{\ln(N/2)} \quad (4.21)$$

where the denominator term corresponds to random signal entropy. In this section, SE is computed using $N = 4 \times 10^4$ after discarding the first 10^4 iterations.

While SE values for stable and periodic signals are $\mathcal{O}(10^{-4})$, the values increase for random and chaotic signals. The spectral entropies of the x (y) time series of the original systems SE_x (SE_y) are 0.4020 (0.4564) and 0.4980 (0.1931) for systems 1 and 2, respectively. The SE values of the transformed systems are also given in Table 4.10. It is usually enough to compute SE for one of the time series [167, 180, 182]. Considering SE of u time series S_u , we find its value close to that of x time series in the cases of scaling, reflection and translation transformations in which u roughly follows an amplified/reflected/shifted version of x . This indicates the topological equivalence and maintaining complexity properties of the chaotic dynamics. For skewing and rotation, each of u and v depends on both x and y simultaneously and, yet, SE_u and SE_v preserve positive values and maintain complexity properties of the chaotic dynamics. For example, in rotation by $\pi/2$, where the transformation reduces to $u = y$ and $v = -x$, SE_u and SE_v exhibit values close to those of SE_y and SE_x , respectively.

4.5.3.2 Generic Parameters and Bifurcation Diagrams

The presented special cases can be applied in any of the three coordinate planes formed by the principal axes. Moreover, generic parameter values in the three dimensional space can be applied as shown in Fig. 4.12, which corresponds to $A = [2 \ 0.5 \ 1; -2 \ 4 \ 1; 2 \ -0.5 \ -3]$ and $b = [3 \ -3 \ 1.5]^T$. Such transformations reinforces the mutual effects between time series and unpredictability while preserving the chaotic dynamics. While transformed system 1 exhibit $SE_u = 0.3724$, $SE_v = 0.3949$ and $SE_w = 0.3304$, while transformed system 2 exhibit $SE_u = 0.5025$, $SE_v = 0.3215$ and $SE_w = 0.5380$. These SE values further indicate the time series complexity, randomness and chaotic behavior.

The bifurcation diagram plots the post-transient system's output against its parameters. Plotting bifurcation diagrams is one of the approaches towards identifying the effective range of parameters through which the system exhibits bounded responses. In addition, it is used to classify the corresponding qualitative type of the post-transient solution into stable, periodic or chaotic. To further indicate the wide ranges of affine transformations parameters, bifurcation diagrams are generated through plotting the value of u time series when it reaches a local maximum. Bifurcation diagrams are plotted against example scaling a_{11} , skewing a_{32} and translation b_3 parameters as shown in Fig. 4.13. The chaotic behavior extends beyond this interval to the right and left directions of the horizontal axes. While studying each parameter, the rest are fixed to the values corresponding to Fig. 4.12. The effect of the scaling parameter a_{11} on u_{max} range can be observed. The two other parameters do not clearly affect the range of values of u_{max} , but they result in a different time series due to the dependency between the three state variables in the governing equations. Their effect can be alternatively noticed in a bifurcation diagram of w_{max} since they correspond to the third state variable. Figure 4.13 also validates these bifurcation diagrams by the corresponding SE plots. It can be inferred from Fig. 4.13 that the transformed fractional-order systems with hidden attractors yield chaotic responses for a wide range of the introduced affine transformation parameters, which is an advantage not offered by the rest of the system parameters and initial conditions setting.

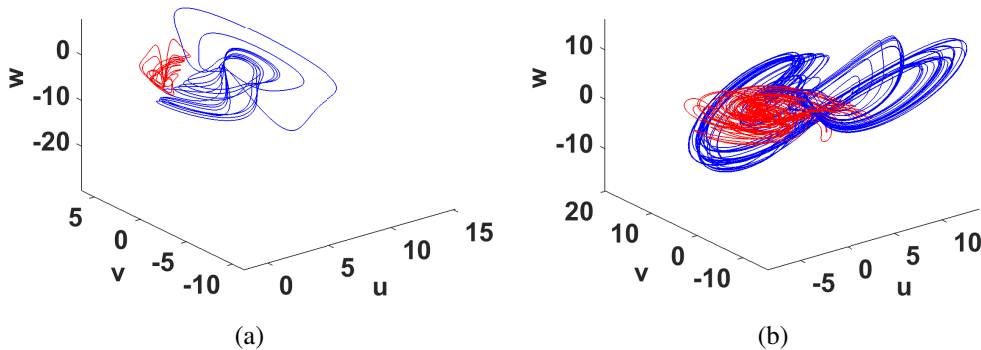


Figure 4.12: Generic case of transformed (a) system 1 and (b) system 2.

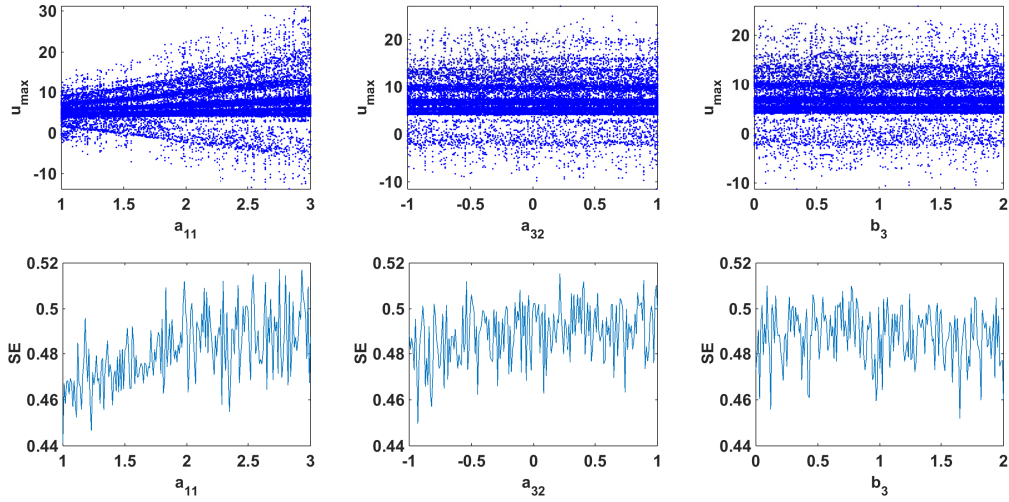


Figure 4.13: Bifurcation diagrams and SE plots of transformed system 2 against affine transformation parameters.

4.5.4 Non-Autonomous Parameters

4.5.4.1 Multiple Wings Generated by Multi-Level Pulse Signals

When the parameters become time variant or non-autonomous, they take dynamic values that change throughout the simulation time. These values can be represented as a multilevel pulse signal, which is constant in each time period apart from breakpoints. The derivative of such non-autonomous parameters can be considered zero, since the angular frequency of the multi-level pulse signals is sufficiently small compared with the chaotic oscillator, even the low frequency transformed system 1. Figure 4.14 shows the resulting strange attractors when the parameters are the multi-level pulse signals given in Table 4.11 with 4, 3 and 5 wings. The total simulation time is T_f and $H(t)$ is the Heaviside function.

With each different combination of parameter values, the attractor reproduces another form of it. This results in multiple wings whose number can be specified by the number of different levels when designing the non-autonomous parameters.

4.5.4.2 Multiple Wings Distributed on a Predefined or Arbitrary Line, Curve or Surface

Translation transformation has the advantage of displacement of the center of the geometric shape. Hence, the self-reproduced attractors can be distributed in space in any predefined form. Figure 4.15(a) shows 5 self-reproductions of the attractor of transformed system 1 along the u -axis using a translation parameter $b_1 = -2H(t) + \sum_{i=1}^4 H\left(t - i\frac{T_f}{5}\right)$. The parameters b_2 and b_3 can be used similarly to generate self-reproduced attractors along v and w axes, respectively. Combinations of two non-autonomous translation parameters can move the attractor along any line or curve equation. For example, Fig. 4.15(b) moves them on a circle of radius R with equation $b_1^2 + b_2^2 = R^2$ and $R = 2$ as an example. One of the two parameters takes values in $[-2, 2]$, e.g., b_1 and the other is computed using $b_2 = \sqrt{R^2 - b_1^2}$. An alternate method sets $b_1 = R \cos(\theta)$ and $b_2 = R \sin(\theta)$, where $0 \leq \theta < 2\pi$.

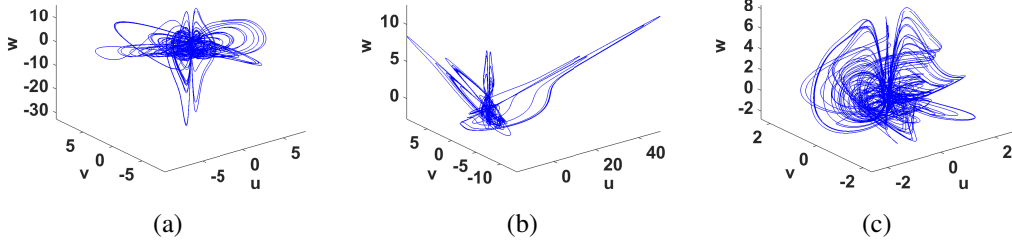


Figure 4.14: Multi-wing attractors by transformed system 1 and multi-level pulse signals as (a) scaling (b) skewing parameters and (c) rotation angle.

Table 4.11: Multi-level pulse signals used in Fig. 4.14

(a)	$a_{11} = -H(t) + 3H\left(t - \frac{T_f}{4}\right) - H\left(t - 2\frac{T_f}{4}\right) - 5H\left(t - 3\frac{T_f}{4}\right)$ $a_{22} = H(t) - 5H\left(t - \frac{T_f}{4}\right) + 3H\left(t - 2\frac{T_f}{4}\right) + 3H\left(t - 3\frac{T_f}{4}\right)$ $a_{33} = 2H(t) - 3H\left(t - \frac{T_f}{4}\right) - 3H\left(t - 2\frac{T_f}{4}\right) + 3H\left(t - 3\frac{T_f}{4}\right)$
(b)	$a_{12} = 2H\left(t - \frac{T_f}{4}\right) - H\left(t - 2\frac{T_f}{4}\right) - 5H\left(t - 3\frac{T_f}{4}\right)$ $a_{21} = -H\left(t - \frac{T_f}{4}\right) - 0.5H\left(t - 2\frac{T_f}{4}\right) + 2.5H\left(t - 3\frac{T_f}{4}\right)$ $a_{13} = -2H\left(t - \frac{T_f}{4}\right) + H\left(t - 2\frac{T_f}{4}\right) - 5H\left(t - 3\frac{T_f}{4}\right)$ $a_{31} = H\left(t - \frac{T_f}{4}\right) + 0.5H\left(t - 2\frac{T_f}{4}\right) - 2.5H\left(t - 3\frac{T_f}{4}\right)$
(c)	$\theta = -\pi H(t) + \frac{\pi}{3} \sum_{i=1}^4 H\left(t - i\frac{T_f}{5}\right)$

The values of b_1 (or θ) can also be represented as a multi-level pulse signal and are assigned uniformly or randomly. A gallery of distributed self-reproduced attractors along a linear segment, piecewise linear (absolute or triangular), exponential, hyperbolic tangent and sine, oval-shaped (ellipse) or heart-shaped (two ellipses) can be produced simply by knowing their equation. Moreover, the attractor can be moved on a three-dimensional surface governed by the equation relating the three translation parameters. Figure 4.15(c) validates this proposal for a sphere $b_1^2 + b_2^2 + b_3^2 = R^2$, where b_1 , b_2 and b_3 are generated based on the sphere point picking algorithm and spherical coordinates [183]. That is, $b_1 = R \cos(\theta) \sin(\phi)$, $b_2 = R \sin(\theta) \sin(\phi)$ and $b_3 = R \cos(\phi)$, where $0 \leq \theta < 2\pi$ and $0 \leq \phi \leq \pi$ are assigned randomly or uniformly. Distributed self-reproduced attractors on a sphere with shifted center, cube, cylinder, ellipsoid or any other surface with predefined equation can be designed similarly.

Similar multiple wing attractors can be formed by employing non-autonomous parameters in transformed system 2 using the proposed transformation framework. A mix of autonomous and non-autonomous parameters can also be used depending on the requirements. For example, the distributed attractors formed by non-autonomous translation parameters can themselves be scaled, reflected, skewed or rotated versions of the original attractor and vice versa.

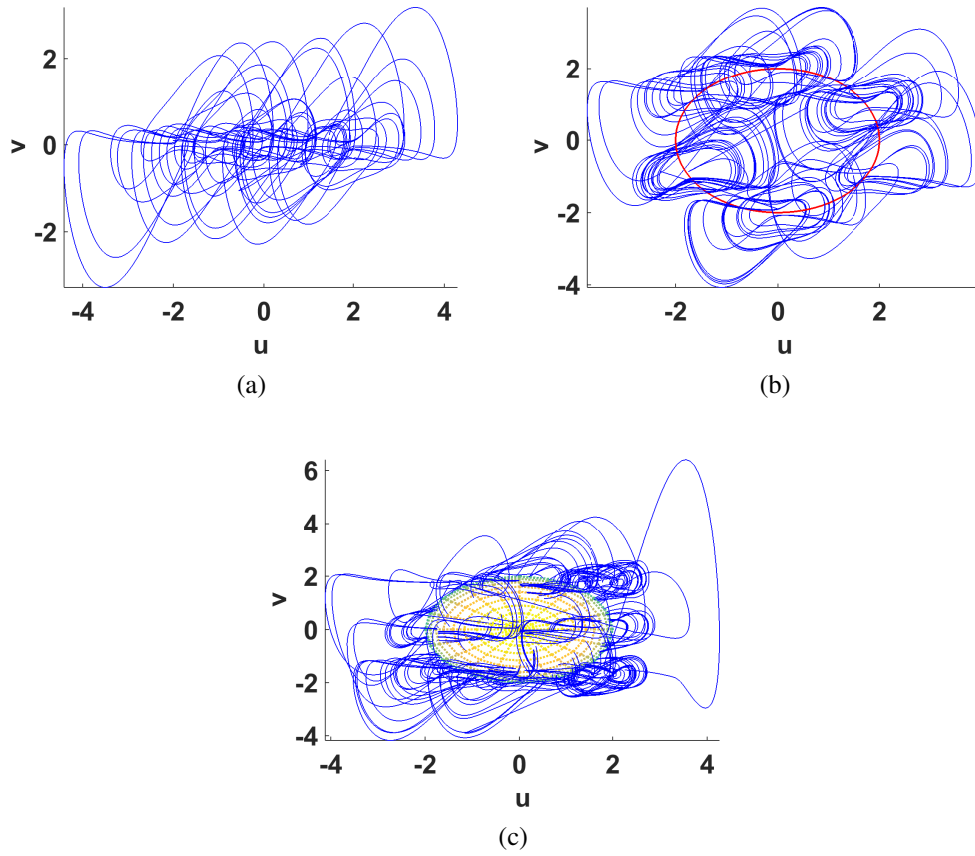


Figure 4.15: Self-reproduced attractors by transformed system 1 along (a) a line, (b) a circle and (c) a sphere.

4.5.5 Impact on Potential Encryption Applications

Figure 4.16 shows a simple chaos-based symmetric encryption scheme with a substitution phase, multiplexer and feedback similar to ones proposed in [11] (a simpler form of the scheme of 4.6). Either of the transformed systems can be used as the chaotic generator, which is iterated using the parameters setting corresponding to the encryption key. Each parameter is computed as the sum of two components: a predefined fixed value such as those given in A and b of Fig. 4.12 and a perturbation value computed from sub-key. That is, if the predefined values are called A_{fix} and b_{fix} then the utilized values are $A = A_{fix} + \Delta A$ and $b = b_{fix} + \Delta b$. For example, $a_{11} = a_{11,fix} + \Delta a_{11}$, where $\Delta a_{11} = K_1 \times 2^{-p}$ with p bits for each sub-key, and so on for the rest of the parameters.

As previously indicated by strange attractors, SE values and bifurcation diagrams, the transformed systems are suitable for encryption applications. Making use of all twelve parameters, an encryption key of length up to $12p$ can be designed, without endangering the chaotic dynamics. This is opposed to designing the encryption key to provide perturbations of the main system parameters, initial conditions and fractional-orders, which may lead to unexpected results if the system is drifted from chaotic dynamics. For instance, $p = 11$ corresponds to a key space of 2^{132} , which is robust against brute force attacks in which the hacker attempts all key combinations [11].

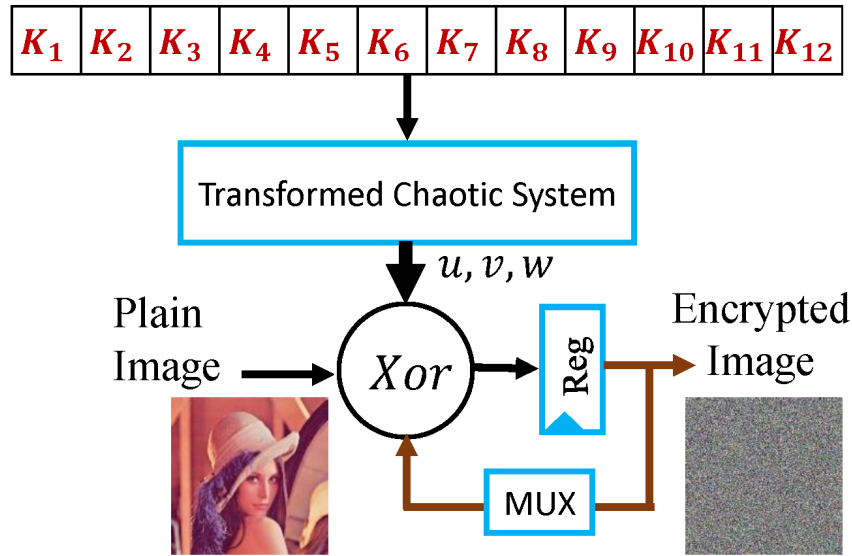


Figure 4.16: Simple example substitution cipher based on the proposed transformed system(s) and encryption key design.

The proposed transformation can also improve the unpredictability of the fractional-order chaotic system and enhance its robustness against synchronization attacks. This advantage can be further enhanced by modifying the definition of perturbation values (ΔA , Δb) such that it has a plain image-dependent component added to the component computed from sub-key similar to the scheme proposed in [4] and Chapter 5.

An analog/digital or mixed circuit realization of the proposed transformed fractional-order chaotic systems can be presented in future work based on (4.18) or simplified forms of it. This can be performed by combining similar previous designs of GL-based fractional-order systems [32] and rotated chaotic systems [7] realizations.

This section proposed a unified control approach for hidden attractors, which exhibit small basins of attractions and extra sensitivity to initial conditions and parameters. A systematic coordinate affine transformation framework was utilized to construct transformed systems with self-reproducing attractors. Simulation results of two systems validate that the proposed framework supports attractors geometric structure design and multi-wing generation. Hidden attractor size, polarity, phase, shape and position control while preserving the chaotic dynamics was indicated by strange attractors, spectral entropy and bifurcation diagrams. Simulations demonstrated the capability of multi-wing generation from fractional-order hidden attractors with no equilibria using non-autonomous parameters as opposed to the classical equilibria extension techniques suitable only for self-excited attractors. The self-reproduced multiple wings can share the same center point or be distributed along an arbitrary line, curve or surface thanks to the non-autonomous translation parameters. Multi-wing attractors widen the basin of attraction and enlarge the state space volume. For practical applications, the proposed technique makes fractional-order systems with hidden attractors suitable for circuit implementations that require specific signal level and polarity conditions. In addition, for digital encryption applications, the relatively wide range of the extra parameters enhances the key space and hence the robustness against brute force attacks.

From all the special cases of transformations presented in this chapter, rotation deserves

an attentive study. The rotation angle can take any value, which will eventually be mapped to the interval $[0, 2\pi)$, and corresponds to continuous chaotic behavior of the rotated system against this parameter. The rotation matrix is orthogonal, i.e., R^{-1} can be replaced by R^T resulting in easier computations. For instance, Fig. 4.17 shows the continuous chaotic behavior of the rotating Lorenz system against θ . Further applications of the rotation transformation along with translation and scaling of specific state variables according to the target will be studied in the next chapter.

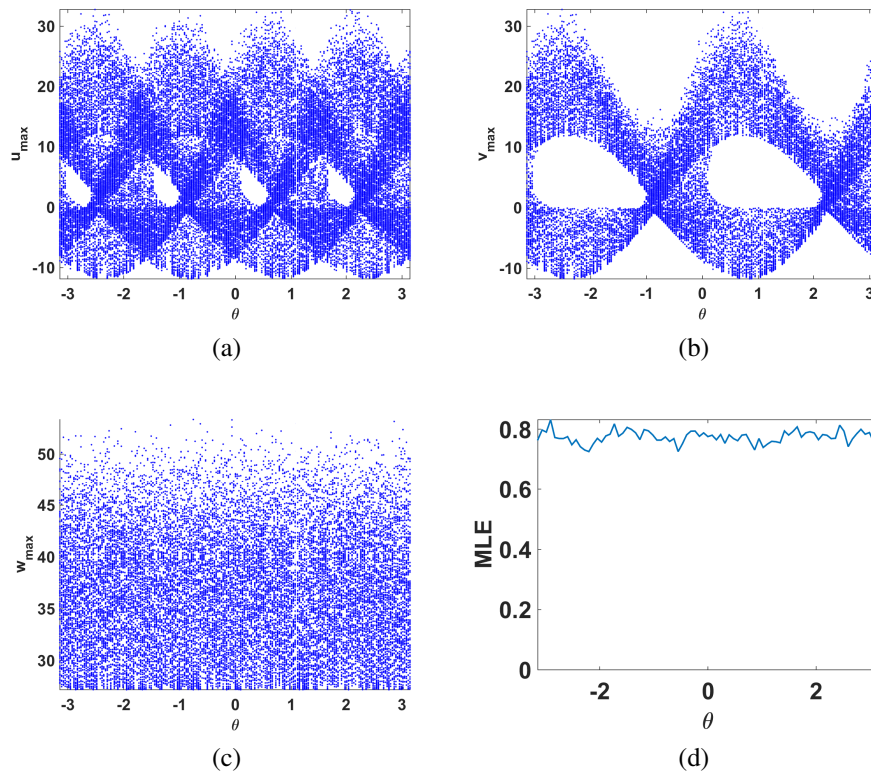


Figure 4.17: (a) u , (b) v and (c) w bifurcation diagrams and (d) MLE against the rotation angle θ of rotating Lorenz system.

Chapter 5: Planar and Spatial Rotation with a Synchronization-Dependent Encryption Application

This chapter focuses on a modification in the second proposed generalization and control approach, which focuses on a combination of rotation, scaling and translation among the other affine transformations [7].

5.1 Rotation with Offset Boosting and Amplitude Control

This section provides examples on multi-scroll rotating chaotic systems, which already have wide enough basin of attraction to enable full utilization of rotation combined with translation (offset boosting) and scaling (amplitude control). In addition, it demonstrates their applications in attractor control and encryption schemes. Moreover, experimental validation on FPGA is presented. The rotation angle is sometimes mentioned in degrees because that's how it is used in the Coordinate Rotation Digital Computer (CORDIC) employed in digital design and FPGA realization.

5.1.1 Multi-Character Chaotic Attractor

Recalling Table 2.1 from Chapter 2, V-shape is a modification of Lorenz system by including a staircase function as a constituent for creating multi-scroll system attractor as in [184]. The system is given by:

$$\dot{x} = y - x, \quad (5.1a)$$

$$\dot{y} = \text{sgn}(x)[1 - mz + G(z)], \quad (5.1b)$$

$$\dot{z} = |x| - rz, \quad (5.1c)$$

$$G(z) = \begin{cases} 0 & z < s_0 \\ d_1 & s_0 < z < s_1 \\ \vdots & \\ d_{N-1} & z < s_{N-1} \end{cases} \quad (5.1d)$$

where m , r and b are parameters and $G(Z)$ is the staircase function, which generates the scrolls of the system. The parameters d and s are responsible for controlling the diameter and the height of the scrolls, where the number of scrolls is equal to $2N$.

A Λ -shape or turned V-shape was presented in [185] by inverting the signs of the initial values and a substitution for z by $-z$. In addition, an X-shape multi-scroll attractor was constructed via switching between the Λ and V-shape. These capabilities inspired us to generate different letters of the English alphabet and, furthermore, use it to write words and statements in a nontraditional way. A generalized form of (5.1) is proposed, through which the multi-scrolls can be manipulated to “write”.

We apply rotation in the plane of the two phase space dimensions x and z , to get the corresponding rotated axes u and w , respectively. Consequently, the governing differential equations of the variables u and w in terms of x and z are given by:

$$\begin{aligned}\dot{u} &= \cos\theta \dot{x} + \sin\theta \dot{z}, \\ \dot{v} &= \dot{y}, \\ \dot{w} &= -\sin\theta \dot{x} + \cos\theta \dot{z},\end{aligned}\tag{5.2}$$

where θ is the rotation angle in the $x - z$ plane, or the rotation angle about the y -axis. To apply rotation to a chaotic system, \dot{x} , \dot{y} and \dot{z} in (5.2) are replaced by the functions on the right hand side of the chaotic equations (5.1). The equations are completely represented in terms of the new variables u and w through the inverse transformation:

$$\begin{aligned}x &= \cos\theta u - \sin\theta w, \\ z &= \sin\theta u + \cos\theta w.\end{aligned}\tag{5.3}$$

To enable offset boosting of both axes, two offset parameters t_u and t_w are subtracted from the inverse transformation equations. Furthermore, to enable amplitude control of the vertical axis, an amplitude parameter s_w is introduced through replacing each $w \rightarrow w/s_w$ and modifying all equations accordingly. This results in planarly rotating, translational (offset boostable) and scalable (amplitude controllable) attractors. In order to realize this system later on FPGA Euler method is used for discretization, where the discretized system is given by:

$$t_{1i} = \cos(\theta)u_i - \sin(\theta)\frac{w_i}{s_w} - t_u,\tag{5.4a}$$

$$t_{2i} = \sin(\theta)u_i + \cos(\theta)\frac{w_i}{s_w} - t_w,\tag{5.4b}$$

$$u_{i+1} = u_i + h(\cos(\theta)(v_i - t_{1i}) + \sin(\theta)(|t_{1i}| - r t_{2i})),\tag{5.4c}$$

$$v_{i+1} = v_i + h(\text{sgn}(t_{1i})[1 - m t_{2i} + G(t_{2i})]),\tag{5.4d}$$

$$w_{i+1} = w_i + h s_w (-\sin(\theta)(v_i - t_{1i}) + \cos(\theta)(|t_{1i}| - r t_{2i})),\tag{5.4e}$$

$$G(t_{2i}) = \begin{cases} 0 & t_{2i} < s_0 \\ d_1 & s_0 < t_{2i} < s_1 \\ \vdots & \\ d_{N-1} & t_{2i} < s_{N-1} \end{cases}\tag{5.4f}$$

where h is the step size, t_{1i} and t_{2i} are defined for simplicity. The proposed generalization is capable of generating various shapes from the simple cases shown in Fig. 5.1 to the more complex ones shown in Fig. 5.2. Yet, we focus on its application in a nontraditional type of “writing” English characters as follows. We demonstrate the words “WELCOME” and “WORLD” for example; yet, we start with single characters writing.

5.1.1.1 V-like Characters

Characters such as “W” and “M” are so much like “V”, where “W” is composed of two joined versions of the 4-scrolls V-shape one in its original position and the other is shifted/translated/offset using t_u as given in Table 5.1. T_f is the total simulation time and $H(t)$ is the Heaviside function. “M” can be similarly generated after rotation by π .

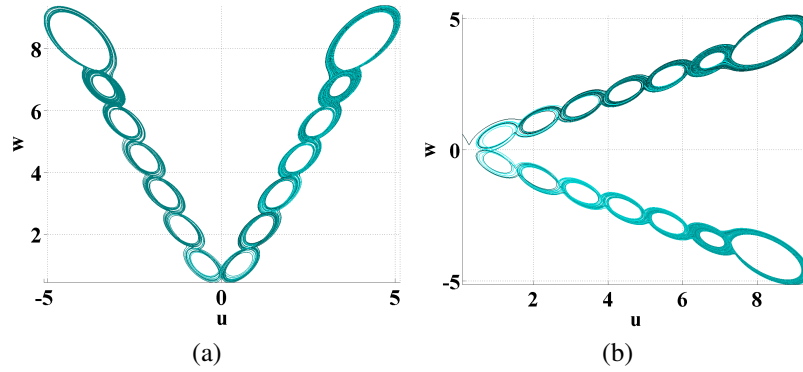


Figure 5.1: Rotating multi-scroll system at (a) $\theta = 0$ and (b) $\theta = \pi/2$.

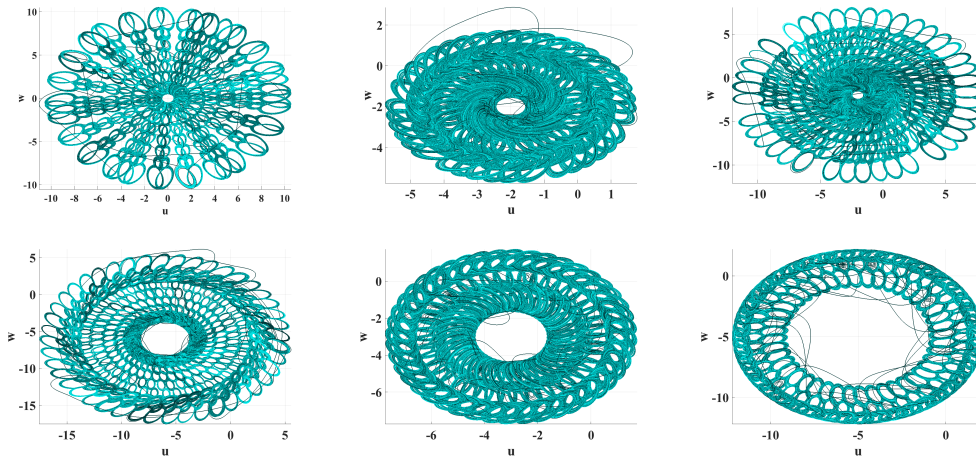


Figure 5.2: Rotating V-shape for dynamic values of θ and different number of scrolls.

5.1.1.2 Straight Characters

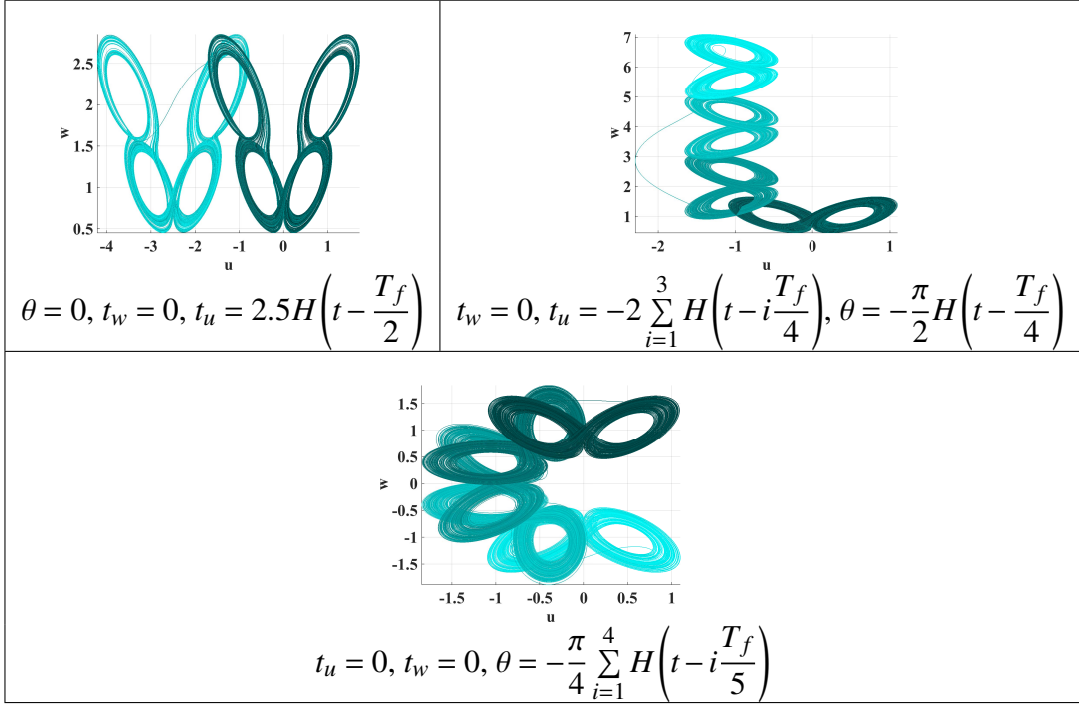
Characters such as “L” and “E” are composed of straight line segments, which can be produced by several joined 2-scrolls V-shape with different orientations and offsets. For example, “L” shown in Table 5.1 is composed of the original 2-scroll V-shape in its conventional position and three versions rotated by $-\pi/2$ and gradual shifts in the direction of the attractor’s base (u -axis).

5.1.1.3 Curved Characters

Characters such as “C”, “O” are circular and, hence, produced by successive gradual rotations. For example “C” shown in Table 5.1 is composed of 5 versions of the 2-scroll V-shape, where the rotation angle starts from 0 and reduces by $\pi/4$ every one fifth of the simulation time. On the other hand, for “O”, this reduction takes place every one eighth of the simulation time to draw a complete circle. Characters combining both straight and curved parts such as “R” and “D” are generated similarly by switching between the corresponding parameters values. Scaling is also employed when required, e.g., to control the size of the semicircle and quadrant needed to generate the curved parts of “R”.

Furthermore, the same chaotic equations can generate multi-characters to compose

Table 5.1: Single character generation



words and statements. The simulation time is subdivided to write characters successively similar to how it was divided to draw different parts of a single character. As previously explained in Chapter 4, the proposed transformation treats the attractor as a shape that is almost trapped inside a rectangle with base width and height corresponding to the two-dimensional projection of the state space volume of the attractor in the $u - w$ plane. To align characters as a word or statement, the location and size of each single character can be further manipulated by t_u , t_w and s_w modifying them the values corresponding to the single character generation previously explained. To offset curved characters and characters with curved parts, the offset parameters are computed from the vector sum of the displacements along the base width and height and are given by:

$$\begin{aligned} t_u &= -t_{w_{fix}} \sin(\theta) + t_{u_{fix}} \cos(\theta), \\ t_w &= t_{w_{fix}} \cos(\theta) + t_{u_{fix}} \sin(\theta), \end{aligned} \quad (5.5)$$

where $t_{w_{fix}}$ and $t_{u_{fix}}$ are the corresponding values of the offset parameters if the character was V-like or straight. Examples on multi-character attractors writing are shown in Fig. 5.3.

It should not necessarily be written successively and the parameters settings can be adjusted to generate multiple-rounds of motion between the characters. In this work, the parameter manipulation is achieved manually through piecewise definitions and Heaviside function. In future work, all letters of the alphabet can be generated and the width and height of each character as well as its position can be reported. An automated design for writing words and statements with chaotic attractors can be presented, which may utilize pattern recognition techniques to generate the parameters setup corresponding to an input word or statement.

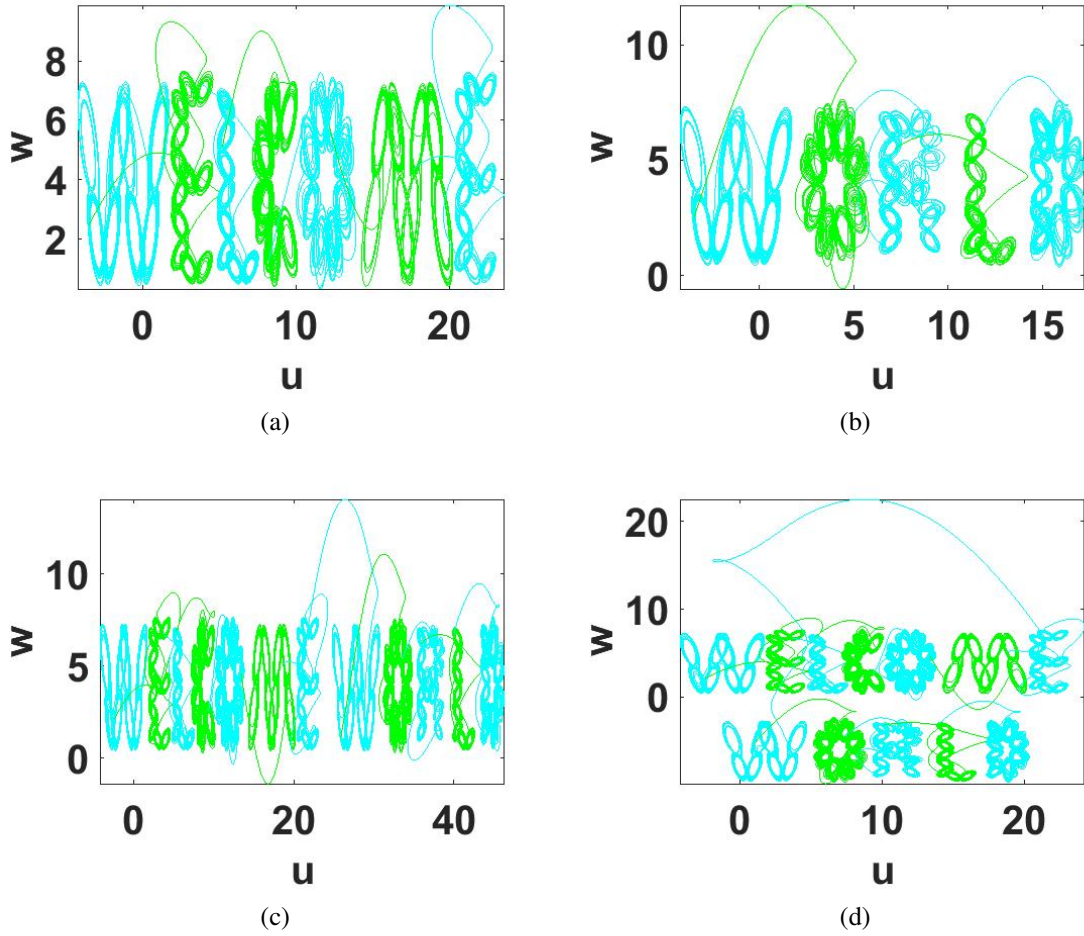


Figure 5.3: Multi-character attractors writing (a) “WELCOME”, (b) “WORLD”, “WELCOME WORLD” on (c) a single line and (d) two lines.

5.1.2 Planarly Rotating Translational Fractional-Order Multi-Scroll Grid Chaotic System

An integer-order multi-scroll 2×2 grid chaotic system was presented in [186]. Its fractional-order counterpart is given by:

$$D^\alpha X = AX + B\Phi(X), \quad (5.6a)$$

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a & -a & -a \end{bmatrix}, \quad B = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & a \end{bmatrix}, \quad \Phi = \begin{bmatrix} f_1(y) \\ 0 \\ f_2(x) \end{bmatrix}, \quad (5.6b)$$

$$f_1(y) = g(y), \quad f_2(x) = 2g(x), \quad g(\tau) = \begin{cases} 0 & \tau \geq 0.5 \\ -1 & \tau < 0.5 \end{cases} \quad (5.6c)$$

Hence, the final system equations are given by:

$$\begin{aligned} D^{\alpha_1} x &= y - g(y), \\ D^{\alpha_2} y &= z, \\ D^{\alpha_3} z &= -a(x + y + z - 2g(x)), \end{aligned} \quad (5.7)$$

and it is solved using (3.9) from Chapter 3 as follows:

$$\begin{aligned}
x_{i+1} &= (y_i - g(y_i))h^{\alpha_1} - \sum_{j=1}^i c_j^{\alpha_1} x_{i-j+1}, \\
y_{i+1} &= z_i h^{\alpha_2} - \sum_{j=1}^i c_j^{\alpha_2} y_{i-j+1}, \\
z_{i+1} &= (-a(x_i + y_i + z_i - 2g(x_i)))h^{\alpha_3} - \sum_{j=1}^i c_j^{\alpha_3} z_{i-j+1}.
\end{aligned} \tag{5.8}$$

The projections of the strange attractors and bifurcation diagrams shown in Table 5.2 show that the system exhibit chaotic behavior at different combinations and against ranges of the fractional orders at $a = 0.81$.

Similar to the integer-order case, the new governing differential equations are constructed using:

$$\begin{aligned}
D^{\alpha_1} u &= \cos \theta D^{\alpha_1} x + \sin \theta D^{\alpha_1} y, \\
D^{\alpha_2} v &= -\sin \theta D^{\alpha_2} x + \cos \theta D^{\alpha_2} y, \\
D^{\alpha_3} w &= D^{\alpha_3} z,
\end{aligned} \tag{5.9}$$

where the x , y and z fractional derivatives in (5.9) are replaced by the functions on the right hand side of the chaotic equations. The equations are completely represented in terms of the new variables u , v and w through the inverse transformation. The resulting discretized system by (3.9) is given by:

$$\begin{aligned}
t_{1i} &= \cos(\theta)u_i - \sin(\theta)v_i - t_u, \\
t_{2i} &= \sin(\theta)u_i + \cos(\theta)v_i - t_v, \\
u_{i+1} &= (\cos(\theta)(t_{2i} - g(t_{2i})) + \sin(\theta)(w_i))h^{\alpha_1} - \sum_{j=1}^i c_j^{\alpha_1} u_{i-j+1}, \\
v_{i+1} &= (-\sin(\theta)(t_{2i} - g(t_{2i})) + \cos(\theta)(w_i))h^{\alpha_2} - \sum_{j=1}^i c_j^{\alpha_2} v_{i-j+1}, \\
w_{i+1} &= (-a(t_{1i} + t_{2i} + w_i - 2g(x_i)))h^{\alpha_3} - \sum_{j=1}^i c_j^{\alpha_3} w_{i-j+1},
\end{aligned} \tag{5.10}$$

The terms t_u and t_v are translational parameters that translate or shift the attractor along the u and v axes, respectively. The system achieves rotation only when $t_u = t_v = 0$. Two-dimensional rotation about y or x axes can be achieved similarly. Figure 5.4 shows examples of the two dimensional rotating translational system with generally dynamic parameters at $(\alpha_1, \alpha_2, \alpha_3) = (1, 0.95, 1)$. From Fig. 5.4(a), it can be inferred that the translation parameters t_u and t_v perform their role in comparison with the original strange attractor in Table 5.2. Figure 5.4(b) uses dynamic translation parameters which change values after a specific duration. Figure 5.4(c) shows the generation of more multi-scrolls using dynamic rotation angle generated via the same procedure.

5.1.2.1 Encryption Applications

Rotated chaotic systems were shown to theoretically preserve the chaotic dynamics adding extra controllability and sensitivity through stability analysis, bifurcations and MLE [6, 7]. This section shows that the same result is valid for practical applications by presenting both an image and a speech encryption applications using the rotated fractional-order

Table 5.2: x - y projections and bifurcation diagrams of the solution of (5.8)

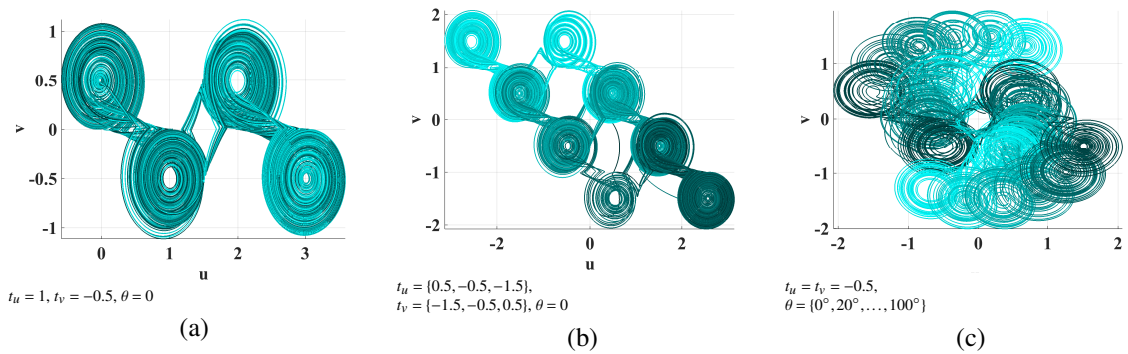
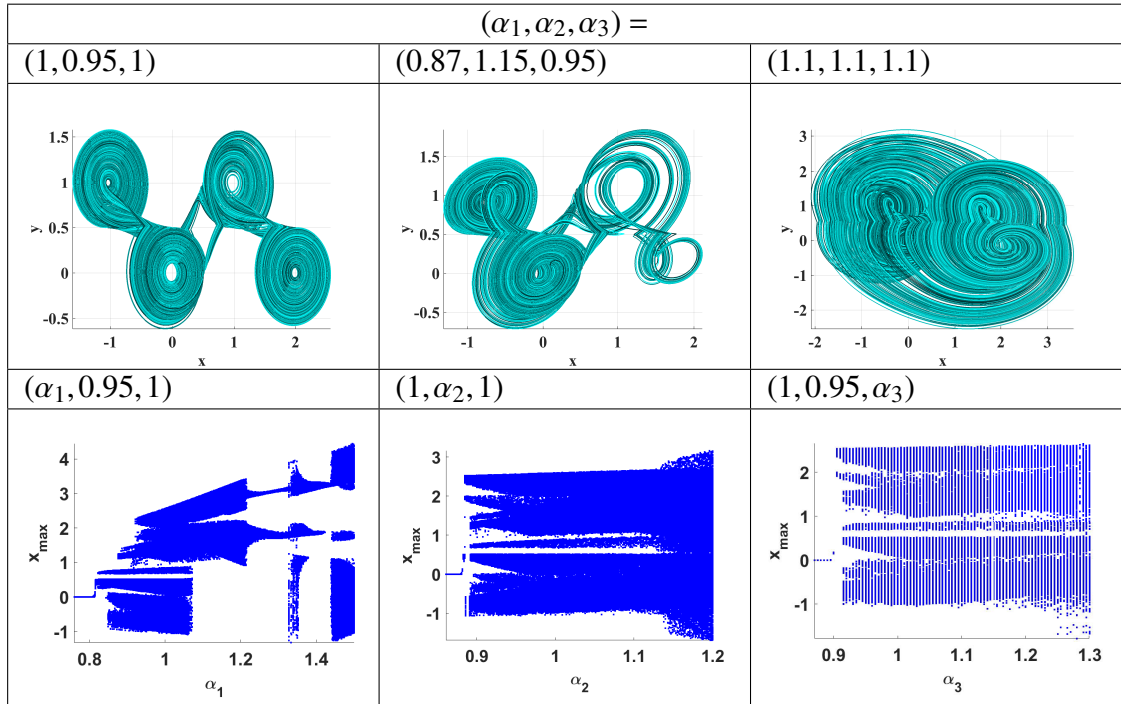


Figure 5.4: Two-dimensional (a) static translation, (b) dynamic translation and (c) dynamic rotation.

multi-scroll grid chaotic system. The advantage provided by the rotation angle as a system parameter is that, unlike the case for chaotic system parameters, the system remains chaotic and does not drift to stable, periodic or divergent responses outside a specific range.

The proposed rotating system is suitable for encryption scheme design with a large enough key space thanks to the fractional-order parameters. The scheme is similar to the substitution phase of the encryption schemes of Chapter 4 and is shown in Table 5.3. The encryption key is composed of seven sub-keys (18, 18, 18, 18, 18, 19, 19 bits) with a total number of 128 bits. The system initial values, rotation angle and fractional-orders are

Table 5.3: The proposed image encryption scheme and its performance analysis

Encryption scheme		Histograms	NIST		
			Test	PV	PP
			1	✓	0.979
			2	✓	0.958
			3	✓	1
			4	✓	0.917
			5	✓	1
			6	✓	1
			7	✓	1
			8	✓	0.989
			9	✓	1
Horz. corr.	Vert. corr.	Diag. corr.	10	✓	1
5.5465×10^{-4}	2.4273×10^{-4}	3.8249×10^{-5}	11	✓	1
Key Sens. (ΔK_4)	MSE ($\times 10^3$)	Entropy	12	✓	0.969
	8.9265	7.9998	13	✓	0.99
DA	NPCR (%)	UACI (%)	14	✓	1
	99.5607	33.4624	15	✓	0.958

computed from the key and P_{sum} , for example:

$$\begin{aligned}
 u_0 &= u_{fix} + K_1 \times 2^{-24} + \text{mod}(P_{sum}, 10)/1000, \\
 \theta &= \theta_{fix} + K_4 \times 2^{-24} + \text{mod}(P_{sum}, 10)/1000, \\
 \alpha &= \alpha_{fix} + K_5 \times 2^{-24} + \text{mod}(P_{sum}, 10)/1000,
 \end{aligned} \tag{5.11}$$

where the fixed parts are set to values within the ranges corresponding to chaotic behavior.

The encrypted image shown in Table 5.3 is completely random and noisy. Table 5.3 validates the good performance of the encryption scheme using various perceptual and statistical evaluation criteria. The histogram reveal a uniform intensity distribution compared to the original nonuniform distribution of the plain image. Close to zero correlation coefficients are reported between the encrypted image pixels. The encrypted image successfully passes NIST tests. The wrong decrypted image is very far from the plain image as indicated by high MSE value. The entropy value approach 8 indicating the randomness and unpredictability of the encrypted image samples. An advantage of the encryption system is that perturbation in any parameter affects the three time series and, hence, the three channels unlike encryption systems based on independent discrete maps for each channel, which require special key design to overcome their limitation [11]. The values of the NPCR and UACI of the three channels are averaged over 20 trials in which one pixel in the original image is changed and found to approach the ideal values 100% and 33.3%, respectively [187].

Furthermore, Table 5.4 hows the capability of constructing a speech encryption scheme base on the proposed system. For speech encryption, the outputs u , v and w of the chaotic generator are multiplied by a scaling factor of 10^{16} to be suitable for conversion to an integer value represented in 64 bits. Each original speech sample is xored with the least significant 16 bits of one of the outputs of the chaotic generator u or w , based on the least significant bit of z , xored together with a feedback element from the previously encrypted

Table 5.4: The proposed speech encryption scheme and its performance analysis

Encryption scheme		Spect. & hist.	NIST		
			Test	PV	PP
			1	✓	1
			2	✓	1
			3	✓	1
			4	✓	1
			5	✓	1
			6	✓	1
			7	✓	1
			8	✓	0.992
			9	✓	0.938
ρ	MSE ($\times 10^4$)	Entropy	10	✓	0.938
-0.0017	3.2649	15.9696	11	✓	1
Key Sens. (ΔK_4)	MSE ($\times 10^4$)	Entropy	12	✓	1
	3.2648	15.9546	13	✓	0.986
DA	NSCR (%)	UACI (%)	14	✓	0.969
	99.9980	33.3564	15	✓	1

sample.

The test speech file obtained from [188] yields a completely random and noisy corresponding encrypted signal as shown in Table 5.4. Good performance is validated similar to image encryption. The spectrogram plots the magnitude squared of the spectrum, which is indicated by the color, in a logarithmic scale against time and frequency. Both the spectrogram and histogram are uniform as opposed to comprehensible speech characteristics. The rest of the successful performance metrics can be described similar to image encryption, where NPCR is replaced by Number of Sample Change Rate (NSCR) [140] and the ideal entropy value is 16 because each speech sample is represented in 16 bits.

5.1.2.2 Experimental FPGA Realization

CORDIC is an iterative method to calculate elementary functions such as trigonometric and hyperbolic using add and shift operations. It overpasses other methods, including multiplication and division, such as Taylor Series and Lookup Table, which suffer from increased hardware resources and memory requirements, respectively. To the best of our knowledge, only [189] was found to use CORDIC in an Artificial Neural Network (ANN)-based chaotic generator to approximate sigmoid activation function using exponent calculator.

Using a setup similar to Chapter 3, Fig. 5.5 shows the experimental results of Section 5.1.1 on the oscilloscope switching between rotation angles 0° and 90° . Table 5.5 shows the experimental results of Section 5.1.2 on the oscilloscope, where the 2D rotation is performed in $x-z$ plane with angle equals to 90° . Table 5.5 also gives the hardware resources utilization for system parameters $u_1 = 0.1$, $v_1 = 0.1$, $w_1 = 0.1$ step size $h = 0.0625$, $\alpha_1 = 1$, $\alpha_2 = 0.9$, $\alpha_3 = 1$, $a = 0.81$, $\theta = 0.5$ and window size=20.

The planarly rotating translational fractional-order multi-scroll grid chaotic system and

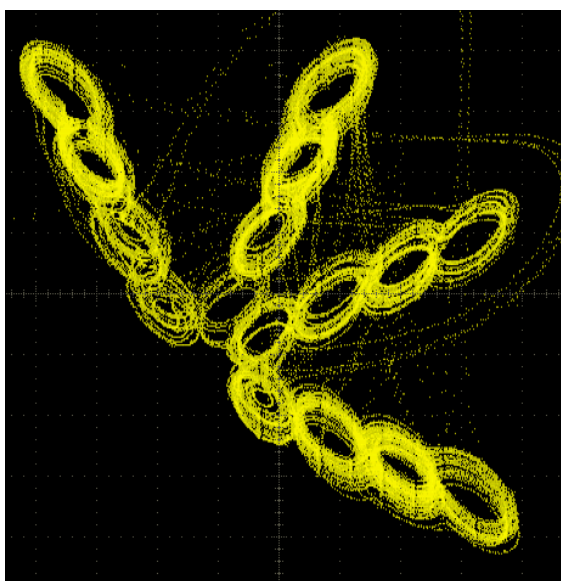


Figure 5.5: Experimental results for rotating integer-order V-shape multi-scroll attractor

Table 5.5: FPGA summary and experimental results for rotating fractional-order multi-scroll attractor

Logic Utilization	2D Rotation
No of LUT	1833 out of 63400 (2%)
No of slice registers	1091 out of 126800 (0%)
Clock speed (MHz)	25.685
Throughput (Mbit/sec)	821.92
Oscilloscope results	

its implementation based on compact GL and CORDIC algorithm can enrich the fields of fractional chaotic dynamics and their applications. It is advantageous compared to previous related works, which proposed multi-scroll chaotic systems and their hardware realizations. The rotation angle had a static value in [89], so a cascade of transformations was applied to achieve a circular grid. That is, the angle variable (register) is set to a specific value during simulation (run) time and is not allowed to vary as time progresses. A dynamic rotation angle was employed in [7] to obtain increased number of scrolls with a single transformation. However, both works did not really implement the sine and cosine functions and only considered the conventional integer-order domain. The compact GL-based digital design of a fractional-order multi-scroll attractor presented in [32] was automated

in [185], yet, the parameter values were still static. None of [7, 89, 185] assessed the performance of their proposed systems in PRNG or encryption applications. The proposed work combines fractional-order domain, multi-scroll grid attractors, two-dimensional rotation and translation transformations to get a chaotic system with controllable complex behavior. The proposed system is employed in an image and a speech encryption applications that successfully pass performance tests. To enable complete control and dynamic planar rotation, it was necessary to have real-time computation of the sine and cosine functions. A CORDIC-based algorithm was designed and implemented successfully in association with compact GL yielding an FPGA realization that balances between accuracy and efficiency. The proposed design is generic for rotating any other chaotic system. The algorithm will be extended to three-dimensional rotation in Section 5.3.

5.2 Synchronization-Dependent Image Encryption Application

The capability of dynamically rotating chaotic systems presented in the previous section enables data embedding in the dynamic rotation angle. For encryption applications, this provides a chance for having more input (plaintext) dependent terms in the utilized chaotic PRNG, which enhances the cryptographic properties and resistance to the different attacks. However, in this case, the symmetric decryption key is not enough to perform correct decryption and chaotic synchronization must be employed.

Chaotic synchronization has been utilized in data encryption and secure communication applications in different forms. For secure communication applications, the message or information signal is embedded in a carrier signal (one or more of the chaotic outputs) through modulation. Embedding is either performed in the dynamical equations [105–110] or applied as a post processing through addition [111–118] or multiplication [119]. The former method imposes conditions on the amplitudes of the message and hence not always suitable, especially for digital encoded signals such as images. Integer-order chaotic systems synchronization has been applied for image encryption [70, 120–124, 124–127]. Although fewer works utilized fractional-order chaotic systems, they have flourished recently and more papers appeared presenting fractional-order chaotic systems synchronization-dependent encryption. Secure communication of simple signals [128] and voice signals [129, 130] were presented based on fractional-order chaotic systems synchronization. Furthermore, researches in image encryption field include [131–137].

Based on dynamically rotating fractional-order systems, this section presents a synchronization-dependent secure communication and image encryption application. The encryption scheme modulates the rotation angle of a fractional-order chaotic system using the plaintext image. Then, it uses this system as a PRNG in data substitution for image encryption, which introduces double-layered security [4, 6].

5.2.1 Dynamic Rotation of Three Fractional-Order Chaotic Systems

Three chaotic systems were selected from [31] as they were successfully extended to fractional-order. In addition, their common fractional orders and output ranges make it easier to visualize the synchronization results. The systems' equations and attractor

diagrams at the used fractional-orders are given in Table 5.6. Only in this section, we refer to the original coordinates by capital letters X , Y , and Z and the transformed coordinates by small letters x , y and z to be capable of following the same notations of the generalized switched synchronization scheme [190].

The rotation transformation yields systems 1, 2 and 3 from those of Table 5.6, respectively. To simplify the equations of the rotating systems, $X(x, y, \theta) = \cos \theta x - \sin \theta y$ and $Y(x, y, \theta) = \sin \theta x + \cos \theta y$ are defined. For instance, system 2 is given by:

$$\begin{aligned} D^\alpha x_2 &= \cos \theta_2 \left(-X(x_2, y_2, \theta_2) + Y^2(x_2, y_2, \theta_2) \right) + \sin \theta_2 (2.5Y(x_2, y_2, \theta_2) - 4z_2 X(x_2, y_2, \theta_2)) \underline{+S_2 u_{2x}}, \\ D^\beta y_2 &= -\sin \theta_2 \left(-X(x_2, y_2, \theta_2) + Y^2(x_2, y_2, \theta_2) \right) + \cos \theta_2 (2.5Y(x_2, y_2, \theta_2) - 4z_2 X(x_2, y_2, \theta_2)) \underline{+S_2 u_{2y}}, \\ D^\gamma z_2 &= -5z_2 + 4X(x_2, y_2, \theta_2) Y(x_2, y_2, \theta_2) \underline{+S_2 u_{2z}}, \end{aligned} \quad (5.12)$$

and equations of systems 1 and 3 can be obtained similarly. The underlined terms $S_i u_{ix}$, $S_i u_{iy}$ and $S_i u_{iz}$ only appear in the synchronization scheme as explained in Section 5.2.2. While Fig. 5.6 shows examples of clockwise and anti-clockwise static rotation, Table 5.7 shows dynamic rotation in which θ is set to four alternatives of dynamic signals. Figure 5.7 further indicates the capability of increasing the number of scrolls. The same color code is fixed in the rest of the section for systems 1, 2 and 3 (see the online colored version). The rotating systems exhibit continuous chaotic behavior against all values of rotation angle, enabling its dynamic change.

Table 5.6: Systems equations and attractor diagrams at $(\alpha, \beta, \gamma) = (0.99, 0.96, 0.95)$

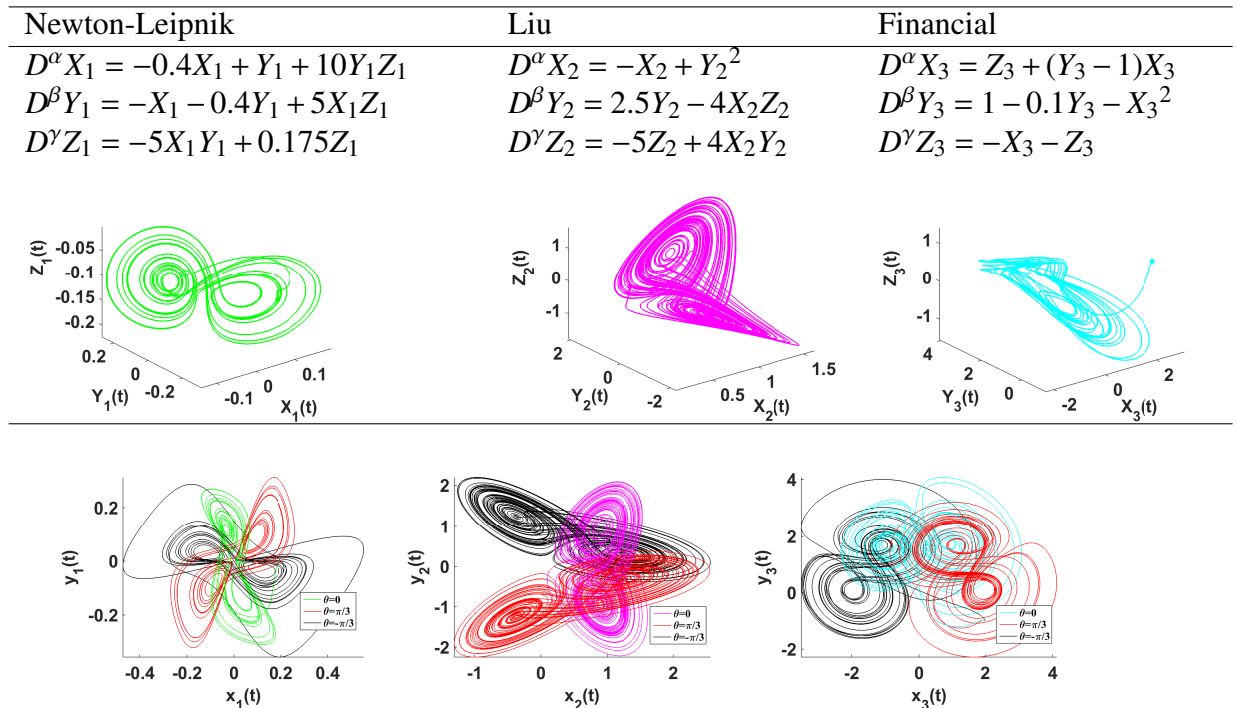


Figure 5.6: Static rotation of the three fractional-order chaotic systems.

Table 5.7: Dynamic rotation examples for the three systems and four dynamic signals, where $A = 5$ and $T = 50$

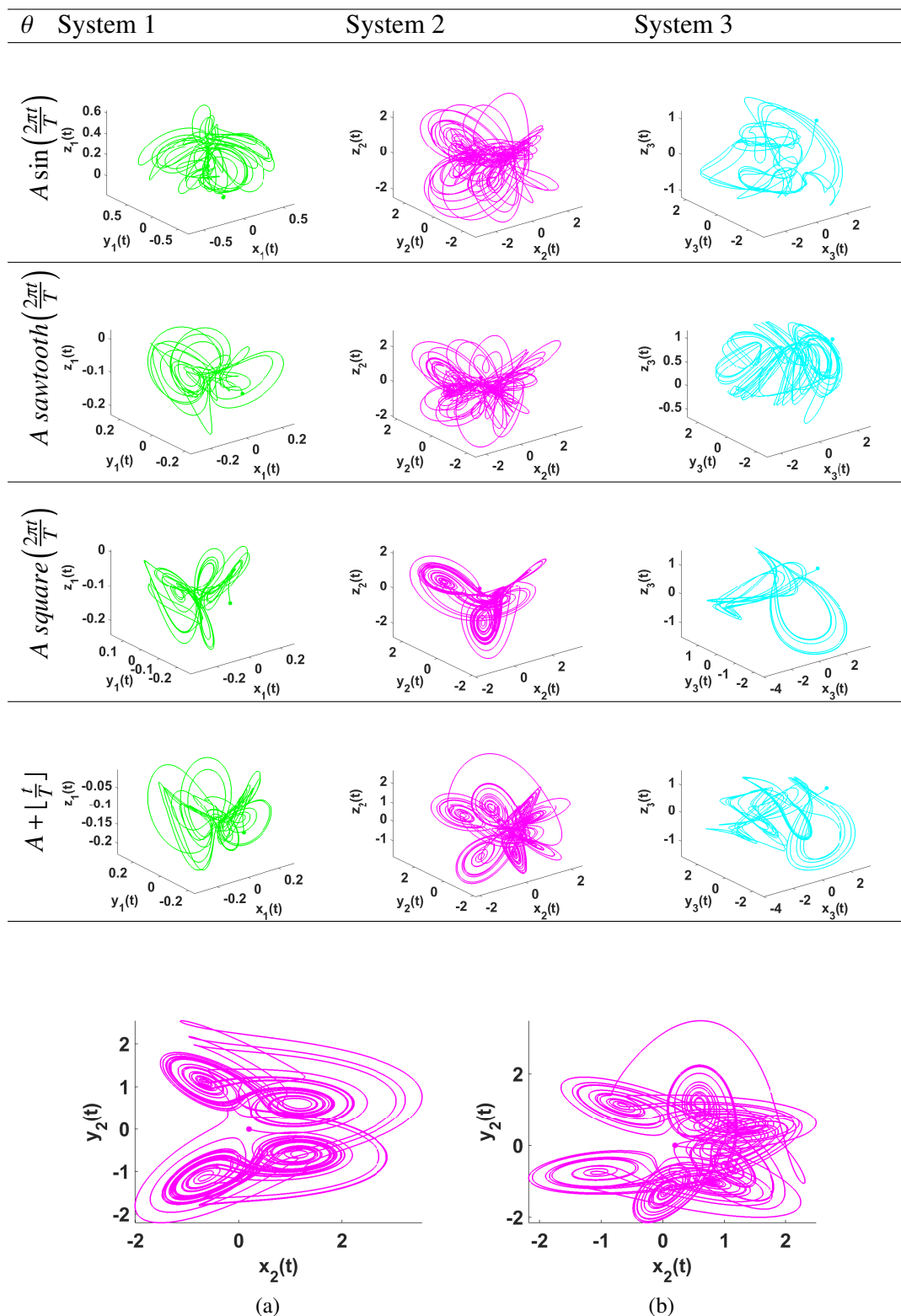


Figure 5.7: Multi-scroll attractors generated by dynamic rotation of system 2 using (a) $\theta = 5 \text{ square}\left(\frac{2\pi t}{50}\right)$ and (b) $\theta = 5 + \lfloor \frac{t}{50} \rfloor$.

5.2.2 Generalized Switched Synchronization Scheme

In this section, the rotating fractional-order chaotic systems are integrated in the generalized dynamic switched synchronization scheme of n systems [190]. The block diagram is shown in Fig. 5.8 for three systems, where $S_i \in \{0, 1\}$ is the control switch of system i , where “0” and “1” correspond to master and slave roles, respectively, k_{jx} , k_{jy} and k_{jz} are scaling factors for the state variables of the master system j , $i, j \in \{1, 2, 3\}$. For an idle system, switches and scaling factors are set to zero. The control functions u_{ix} , u_{iy} and u_{iz} affect the response of slave systems only and are derived using superposition, active nonlinear control and Lyapunov stability theorem [190].

For each slave system i given by:

$$\begin{aligned} D^\alpha x_i &= f_i(x_i, y_i, z_i) + S_i u_{ix}, \\ D^\beta y_i &= g_i(x_i, y_i, z_i) + S_i u_{iy}, \\ D^\gamma z_i &= h_i(x_i, y_i, z_i) + S_i u_{iz}, \end{aligned} \quad (5.13)$$

the corresponding master system/combination is given by:

$$\begin{aligned} x_m &= \sum_{j=1, j \neq i}^n k_{jx}(1 - S_j)x_j, \\ y_m &= \sum_{j=1, j \neq i}^n k_{jy}(1 - S_j)y_j, \\ z_m &= \sum_{j=1, j \neq i}^n k_{jz}(1 - S_j)z_j, \end{aligned} \quad (5.14)$$

where the scaling factors k_{jx} , k_{jy} and k_{jz} control the time series of the slave system i according to those of the master system(s). The error vector e_i is the difference between the master and slave systems. The error derivatives are given by:

$$\begin{bmatrix} D^\alpha e_{ix} \\ D^\beta e_{iy} \\ D^\gamma e_{iz} \end{bmatrix} = \begin{bmatrix} f_i(x_i, y_i, z_i) + S_i u_{ix} - \sum_{j=1, j \neq i}^n (k_{jx}(1 - S_j)f_j(x_j, y_j, z_j)) \\ g_i(x_i, y_i, z_i) + S_i u_{iy} - \sum_{j=1, j \neq i}^n (k_{jy}(1 - S_j)g_j(x_j, y_j, z_j)) \\ h_i(x_i, y_i, z_i) + S_i u_{iz} - \sum_{j=1, j \neq i}^n (k_{jz}(1 - S_j)h_j(x_j, y_j, z_j)) \end{bmatrix} \quad (5.15)$$

According to the nonlinear control and Lyapunov stability theorems, these error derivatives should force negative eigenvalues to ensure stability and zero steady state [191, 192]. Hence, they are given by:

$$\begin{bmatrix} D^\alpha e_{ix} \\ D^\beta e_{iy} \\ D^\gamma e_{iz} \end{bmatrix} = \begin{bmatrix} V_{ix}(e_{ix}) \\ V_{iy}(e_{iy}) \\ V_{iz}(e_{iz}) \end{bmatrix} = \begin{bmatrix} -k_{ux} & 0 & 0 \\ 0 & -k_{uy} & 0 \\ 0 & 0 & -k_{uz} \end{bmatrix} \begin{bmatrix} e_{ix} \\ e_{iy} \\ e_{iz} \end{bmatrix} \quad (5.16)$$

which makes the derivatives decaying functions of the errors controlled by the tuning parameters k_{ux} , k_{uy} , $k_{uz} \geq 1$, such that $e_i \rightarrow 0$ as $i \rightarrow \infty$. Consequently, substitution from (5.16) into (5.15), setting $S_i = 1$ for each slave system i , $i = \{1, 2, \dots, n\}$, yields:

$$\begin{aligned} u_{ix} &= V_{ix}(e_{ix}) + \sum_{j=1, j \neq i}^n k_{jx}(1 - S_j)f_j(x_j, y_j, z_j) - f_i(x_i, y_i, z_i), \\ u_{iy} &= V_{iy}(e_{iy}) + \sum_{j=1, j \neq i}^n k_{jy}(1 - S_j)g_j(x_j, y_j, z_j) - g_i(x_i, y_i, z_i), \\ u_{iz} &= V_{iz}(e_{iz}) + \sum_{j=1, j \neq i}^n k_{jz}(1 - S_j)h_j(x_j, y_j, z_j) - h_i(x_i, y_i, z_i). \end{aligned} \quad (5.17)$$

The obtained active control functions (5.17) are substituted in the equations of the systems, e.g. (5.12).

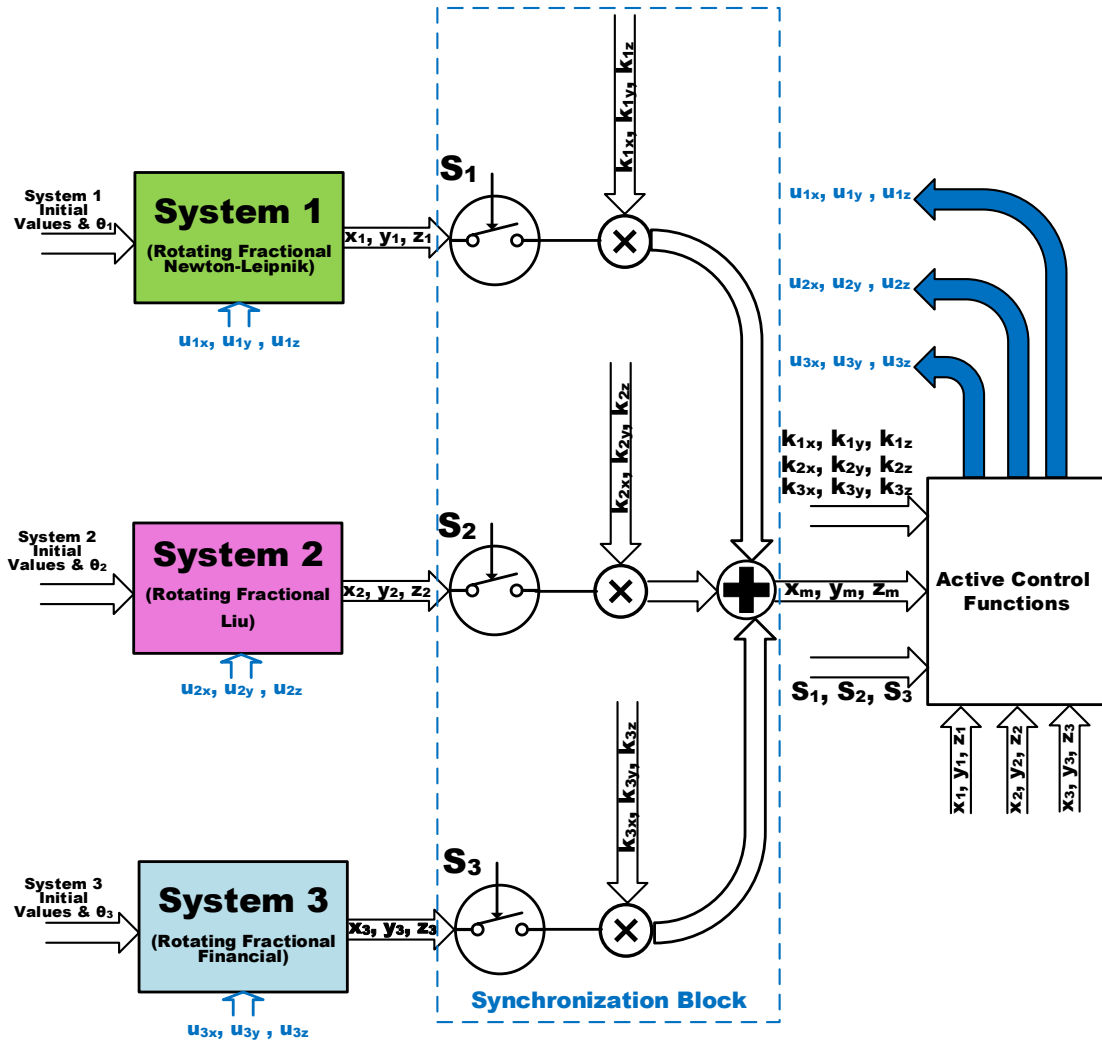


Figure 5.8: Generalized dynamic switched synchronization scheme of rotating fractional-order chaotic systems.

5.2.3 Simulation Results for the Synchronization Scheme

This section demonstrates the suitability of rotating fractional-order chaotic systems for synchronization applications preserving same capabilities of [190] as well as static and dynamic rotation. Figure 5.9 summarizes the available alternatives provided by the generalized synchronization scheme from different viewpoints. Various cases are validated to achieve the targeted synchronization even in the complicated case with various dynamic signals. Simulation results are obtained using $h = 0.005$ as a step size, 40 000 iterations (i.e., total duration of 200 time units) and $k_{ux} = k_{uy} = k_{uz} = 50$ [31, 190]. The three rotating systems have $\theta_1 = 5 \sin\left(\frac{2\pi t}{50}\right)$, $\theta_2 = 5 + \lfloor \frac{t}{50} \rfloor$ and $\theta_3 = 5 \text{ sawtooth}\left(\frac{2\pi t}{50}\right)$.

Table 5.8 shows the simulation results for three selected cases. First, for single master, the slave systems are synchronized with the master (system 1). The beginning of both x and y time series shows that they successfully follow the master time series and the error approaches 0 in around 30 iterations. Second, for master combination, the slave (system 2) is synchronized with the master combination (systems 1 and 3, dark, blue, colored). Third, a case with several dynamic signals is shown, where the master is system 2 followed by

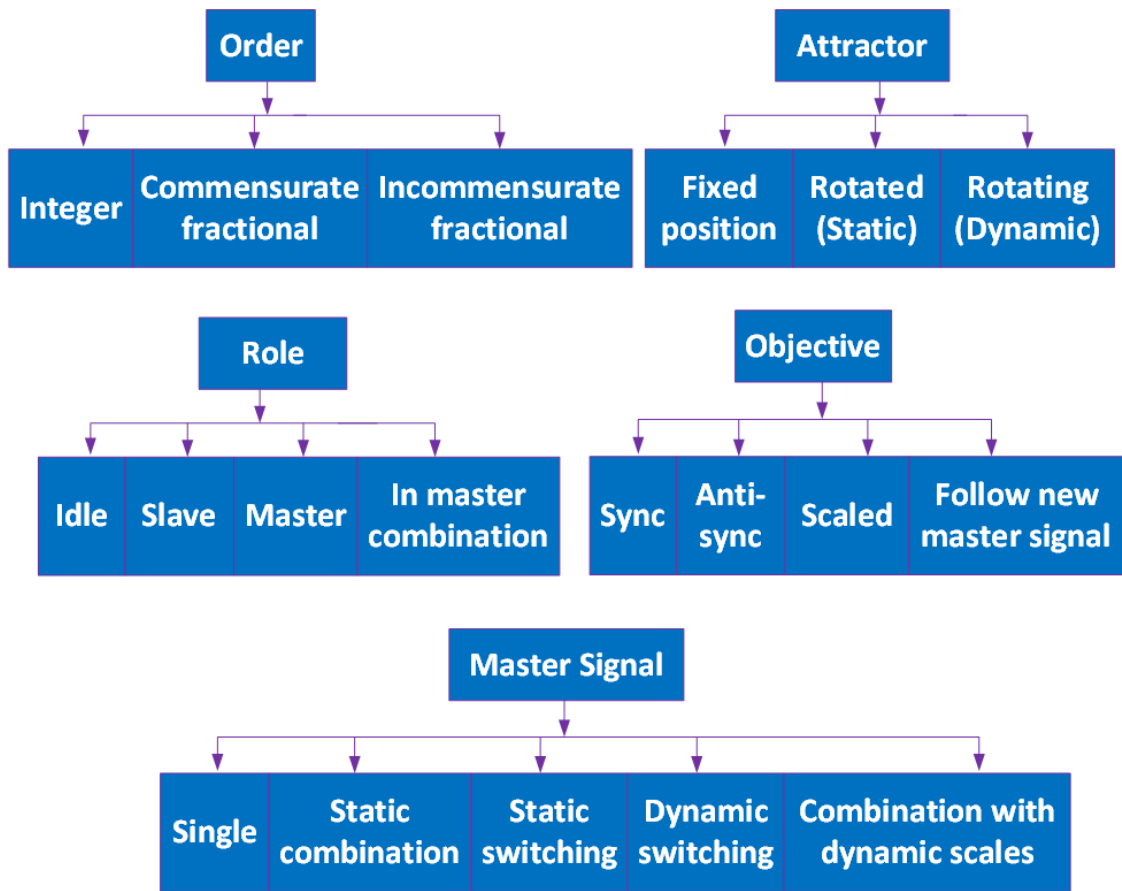


Figure 5.9: Generalized dynamic switched synchronization applications on rotating chaotic systems.

system 3, each for half the simulation time. The time series of both systems are scaled by $k_{2x} = k_{3x} = k_x = \text{square}\left(\frac{2\pi t}{50}\right)$ and $k_{2y} = k_{3y} = k_y = 1 + \lfloor \frac{t}{50} \rfloor$. The resulting time series and attractor diagram indicate that the slave (system 1) follows the switched master.

5.2.4 Proposed Encryption/Decryption Scheme

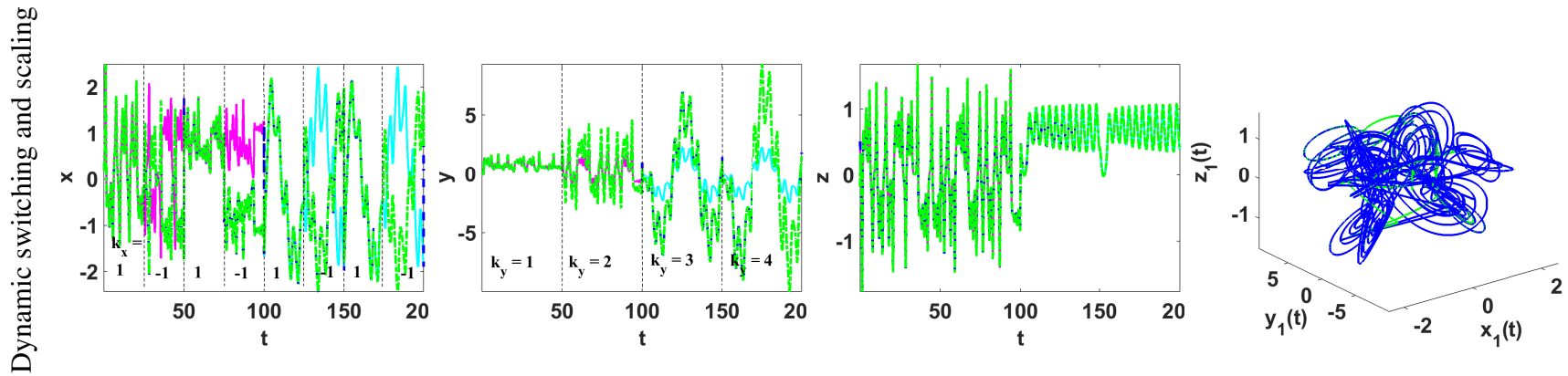
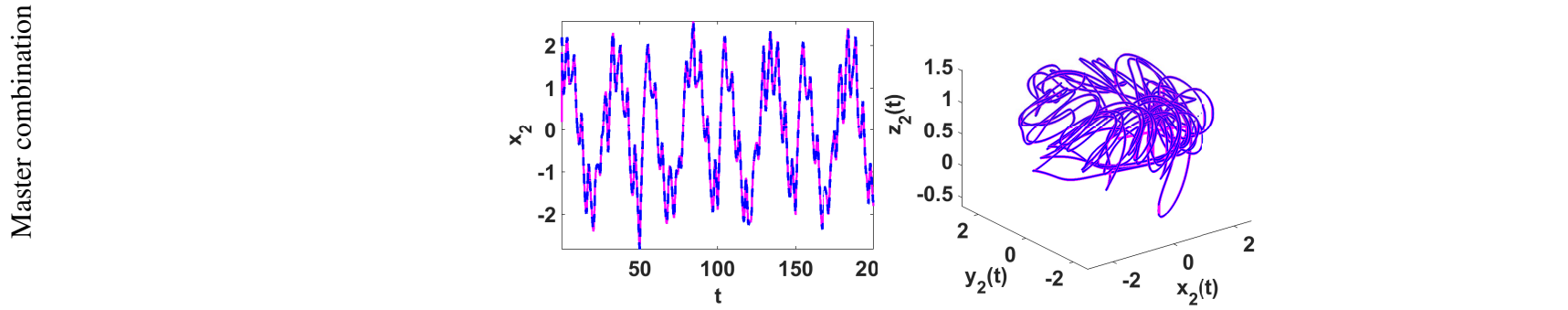
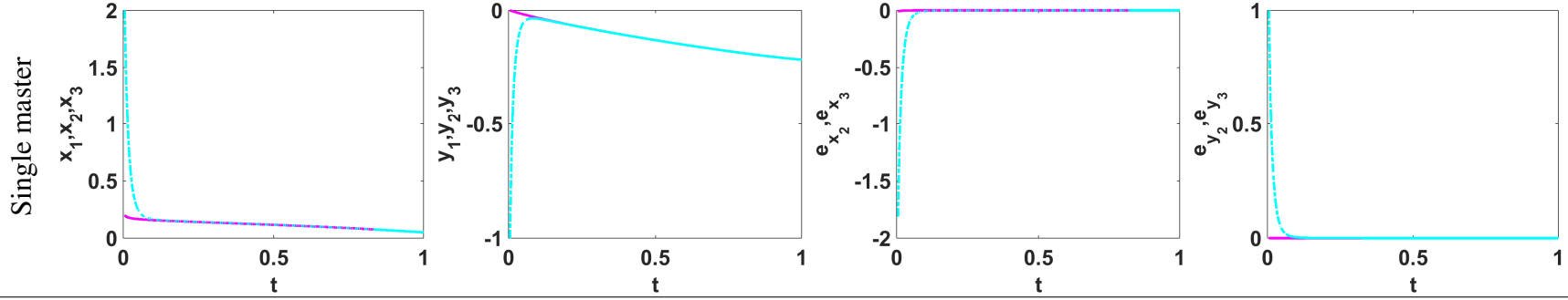
This section presents an image encryption scheme that utilizes rotating fractional-order chaotic systems for plaintext image pixels substitution using the logical XOR operation. At the same time, the dynamic rotation angle is modulated using the input image pixels. Hence, synchronization is required to generate the same chaotic time series needed for decryption as the decrypter has no access to the plaintext image. The proposed generalized switched synchronization scheme offers multiple alternatives of master system construction and synchronization types as previously summarized in Fig. 5.9.

Figure 5.10 shows the synchronization-dependent encryption and decryption scheme. The encryption key consists of six sub-keys and determines the fractional-orders and initial values of the chaotic systems as follows:

$$\alpha = \alpha_{fix} + K_1 \times 2^{-26}, \quad (5.18)$$

where α_{fix} is a fixed part set to a value that generates chaotic behavior, e.g., the values given in Table 5.6, and similarly for the rest of the sub-keys.

Table 5.8: Successful synchronization simulation results



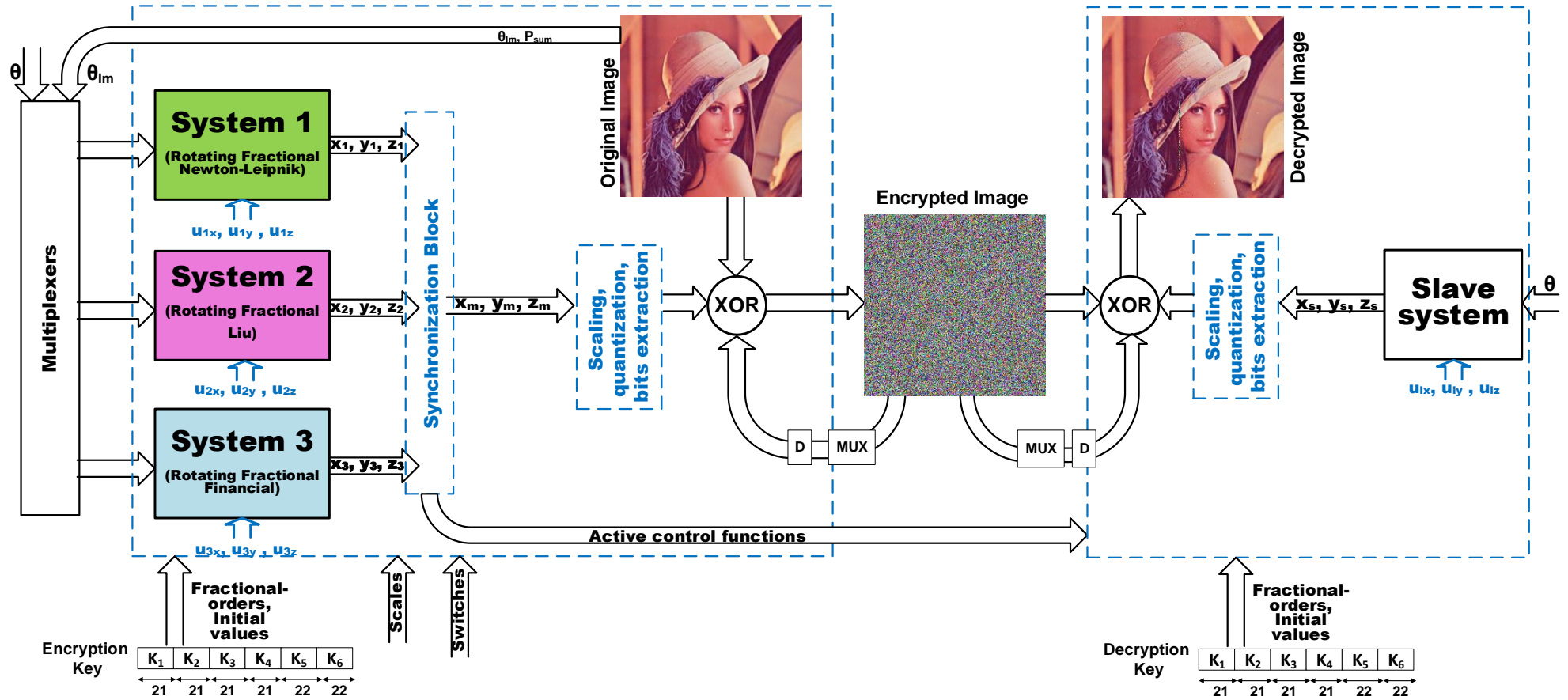


Figure 5.10: Synchronization-Dependent Image Encryption/Decryption Scheme.

For the master system(s), the dynamic rotation angle θ is given by:

$$\theta = \frac{\text{double}(R \oplus G \oplus B) \lfloor \frac{P_{sum}}{255} \rfloor}{P_{sum}}, \quad (5.19)$$

and is evaluated for each iteration i and denoted by θ_{Im} in Fig. 5.10. For the slave system(s), θ can be set to any static or dynamic value(s). The chaotic outputs of the master system or master combination are scaled, quantized and 8 bits are extracted from each of them to act as PRNG (usually the LSBs, except where stated otherwise). Substitution by logical XOR with feedback and multiplexer are then applied similar to Chapter 3. For decryption, all operations are reversed, using the slave system to generate the PRNG. The switch and scaling factors of the slave system i are set to one, i.e., $S_i = k_{ix} = k_{iy} = k_{iz} = 1$.

5.2.5 Simulation Results and Performance Evaluation

NIST tests are carried out on each chaotic output in the same manner in which they are used in encryption and using the input dependent rotation angle given by (5.19). Table 5.9 shows that the three chaotic PRNGs pass the tests. Three synchronization scenarios are tested using the colored 256×256 Lena image [160]. In scenario 1, system 2 is the single master and system 1 is used as a slave in the decryption side. In scenario 2, a master combination of both systems 1 and 3 is used. In scenario 3, dynamic switching between systems 2 and 3 as master systems is employed. The performance of the scheme is evaluated through the encrypted image, histogram and its uniformity through chi square test, pixel correlation, MSE, entropy, PSNR, key sensitivity, resistance to brute force, differential and other security attacks. Equations of the performance metrics were given in Table 3.16 of Chapter 3.

The encrypted images corresponding to the three scenarios are random similar to the example shown in Fig. 5.10. In addition, the corresponding histograms reveal a uniform intensity distribution compared to the nonuniform histograms of the original image as shown in Fig. 5.11. To further check the degree of deviation from uniform histogram, chi-square test [162] is used. The less the chi-square value, the better the uniformity. Table 5.10 gives the results for the encrypted images, which have relatively low values compared to that of the original image of $\mathcal{O}(10^4)$.

Table 5.10 shows the ability of the system to destroy the horizontal, vertical and diagonal correlation between the pixels where the correlation coefficients of the encrypted image approach zero. High MSE, Entropy approaching 8 and low PSNR further indicate the randomness and unpredictability of the encrypted image.

The 128 encryption key designed as shown in Fig. 5.10 has a key space of 2^{128} , which is large enough to resist brute force attacks in which the hacker attempts all key combinations [187] and make them impractical. When the LSB of the sub-key ΔK_1 is changed, high MSE values and Entropy approaching 8 are reported as given in Table 5.10, which indicate the randomness and unpredictability of the wrong decrypted image. Similar results are obtained for the rest of the sub-keys. In the proposed scheme, perturbation in any parameter affects the three time series and, hence, the three channels. This is an advantage of encryption systems based on higher-order differential equations unlike those based on independent discrete maps for each channel [11].

Table 5.9: NIST results for the PRNG from the three chaotic systems

Test	System 1		System 2		System 3	
	PV	PP	PV	PP	PV	PP
Frequency	✓	1	✓	1	✓	1
Block Frequency	✓	1	✓	1	✓	0.958
Cumulative Sums	✓	1	✓	1	✓	1
Runs	✓	1	✓	0.958	✓	1
Longest Run	✓	0.917	✓	1	✓	1
Rank	✓	0.958	✓	1	✓	1
FFT	✓	1	✓	0.958	✓	0.958
Non-overlapping Template	✓	0.99	✓	0.992	✓	0.995
Overlapping Template	✓	1	✓	0.958	✓	1
Universal	✓	1	✓	0.958	✓	1
Approximate Entropy	✓	0.958	✓	1	✓	1
Random Excursions	✓	1	✓	1	✓	0.992
Random Excursions Variant	✓	1	✓	0.992	✓	0.948
Serial	✓	1	✓	1	✓	1
Linear Complexity	✓	0.958	✓	1	✓	1
Final result	Passed		Passed		Passed	

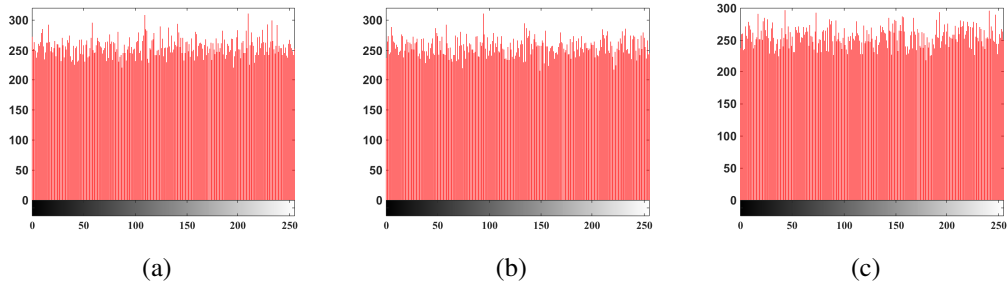


Figure 5.11: Histograms of the encrypted red channel for (a) scenario 1 (b) scenario 2 and (c) scenario 3.

Table 5.10 shows the values of the NPCR and UACI averaged over 10 trials in which one pixel in the original image is changed, which successfully approach 100% and 33.33%, respectively [187].

The system can resist other cryptanalysis techniques, besides brute force and differential attacks. In ciphertext-only attack, the attacker has access only to a ciphertext or a collection of ciphertexts with the objective of finding the plaintext image and/or the secret key. This requires the use of brute force [164], and hence, the large key space and the dependence of the PRNG on the plaintext image are effective means of enhancing the scheme's resistance to this attack.

Embedding the plaintext image in the dynamic rotation angle of the chaotic time series almost eliminates the chances of its discovery, unlike post-processing rotation. In the latter case, given the rotated and original coordinates, (x, y) and (X, Y) , respectively, the rotation

Table 5.10: Performance evaluation of the image encryption scheme for three synchronization scenarios

Test		Scenario 1	Scenario 2	Scenario 3
$\chi_{\text{test}}^2 (\times 10^2)$		2.3345	2.4158	2.5528
ρ ($\times 10^{-3}$)	Horizontal	-1.8985	0.8363	0.7832
	Vertical	-0.2458	0.6062	-1.8442
	Diagonal	0.6054	-6.0965	-2.8532
MSE ($\times 10^3$)		8.8586	8.8623	8.8684
Entropy		7.9974	7.9973	7.9972
PSNR		8.7189	8.7135	8.7117
Key Sens. (ΔK_1)	MSE ($\times 10^3$)	8.8640	8.8701	8.8838
	Entropy	7.9973	7.9969	7.9971
DA	NPCR	99.6272	99.5941	99.6216
	UACI	33.5249	33.4539	33.5218

angle can be computed from:

$$\theta = \tan^{-1} \frac{y X - x Y}{X x + Y y}. \quad (5.20)$$

Yet, the proposed method embed the plaintext image in the chaotic dynamics and, on the long term evolution, it is totally different from the post-processing time series due to chaotic sensitivity properties. That is, trajectories that start out very close to each other, with extremely slight differences in initial values, parameters or implementations, separate with time. Ultimately, this makes information retrieval or message extraction only possible through synchronization and having access to the decryption scheme. To further illustrate this advantage, (5.19) is simplified to $\theta = \frac{G \lfloor \frac{P_{sum}}{255} \rfloor}{P_{sum}}$ and an attempt of its retrieval from the chaotic time series is implemented. Figure 5.12 shows that although post-processing enables image restoration from the chaotic time series using (5.20), the proposed rotating chaotic systems do not allow this to happen. This result suggests that the scheme with angle modulation only can be suitable for secure data transmission of any type whether it is digital encoded in a fixed point representation and suitable for logic XOR operation or not. In our scheme, the process is even more complicated due to XORing the three components in (5.19) to modulate the rotation angle of the chaotic system. In addition, the transmitted encrypted image is produced by XORing with the PRNG formed by the bit sequence extracted from this modulated chaotic output, as well as a multiplexed previous encrypted pixel.

In order to achieve correct decryption as shown in Fig. 5.10, different settings are needed for the different complexities of synchronization scenarios. For example, the tuning factors k_u range between 50 and 300, the discarded simulation time ranges from 20 to 50 time units. Finally, the selection of bits that form the PRNG extracted after scaling and quantization of the chaotic output differ among scenarios. Specifically when dynamic switches or scaling factors are employed, the LSBs become sensitive to the slight synchronization error, which is bounded close to zero. Hence, intermediate significant bits are used, where they are less subject to synchronization error and achieve both good encryption performance (Table 5.10) and correct decryption. Similar limitations

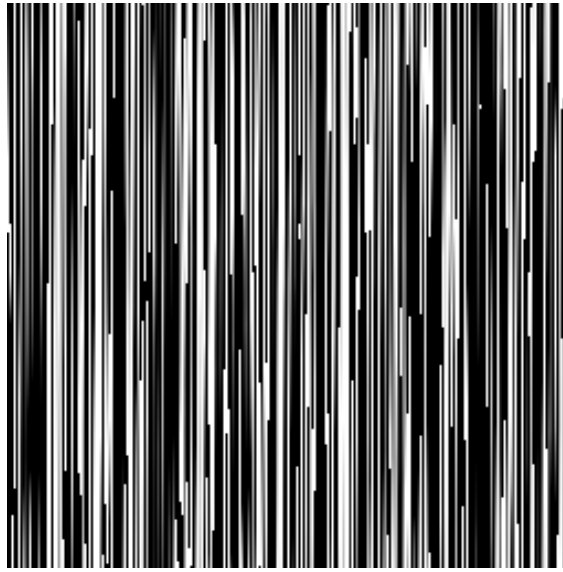


Figure 5.12: Failed attack of image green channel restoration from the proposed rotating chaotic time series.

and precautions were reported in previous related works, even for simple single master synchronization, e.g., [110, 126, 127, 131, 132, 137].

5.2.6 Discussion and Comparison

The proposed synchronization-dependent secure communication setup is suitable for one-to-one, one-to-many, mutual interconnection and role switching. The transmitter and receiver of Fig. 5.10 can exchange roles in the presence of a dual channel. Synchronization can be performed with the transmitter chaotic system as it is or a dynamic scaled version of it. It can employ dynamic switching between multiple transmitters or a combination of them with dynamic scaling parameters. Static switching and/or scaling are also feasible as special cases. Moreover, synchronization can be achieved for one state variable or all of them according to the application. Most of the papers on the topic, e.g., the ones briefly reviewed in the beginning of this section, only focused on one type of synchronization and one-way communication with fixed single transmitter and receiver. Only [135] discussed anti-synchronization, which is a special case of our generalized synchronization with a scaling factor of -1 .

In the designed scheme, synchronization is employed for a purpose and correct decryption can not properly take place without it. The plaintext image itself is used to determine the dynamic rotation angle every single iteration. Consequently, such a design for the master system requires synchronization because the master signals are irreproducible at the receiver side with no access to the plaintext image. In most of the reviewed papers, their PRNGs were independent on the plaintext with the exception of [132], in which key and input dependent parameters are utilized in the chaotic PRNG. In addition, the utilization of synchronization was only owed to external disturbances and design mismatches [116, 117, 130]. In our proposed work, synchronization is a must and design dictated and PRNG dependence on plaintext image increases robustness against different cryptanalysis attacks.

A novel dynamically rotating fractional-order system is utilized, rather than integer-order systems or fractional-order systems with static attractors. Fractional-orders and dynamic parameters enhance the chaotic properties and encryption performance. The fractional-orders enable reaching a large key space and the dynamic rotation angle enable input dependence. The synchronization-dependent encryption scheme makes use of two ideas: angle modulation using the plaintext and XOR logic operation for plaintext image substitution. Almost all reviewed papers applied only one approach; either embedding the information/message/plaintext in the chaotic equations through amplitude modulation or performing an arithmetic or logic operation between it and the independent chaotic output. Only in [132], the data is converted to a data carrier signal by logic XOR with the PRNG, added to one chaotic output then transmitted. Adopting both approaches in our scheme adds a double-layered security. One of the advantages of angle modulation is that it has no conditions on the amplitudes/values of the message as it will be eventually mapped to $[0, 2\pi)$.

The reviewed works depended on the arithmetic data masking through addition in most papers [109–118, 126], permutation before arithmetic substitution [127, 134, 137], and/or performing the logic XOR operation, whether preceded by complicated arithmetic operations on the resulting chaotic signals or not [127, 131, 132, 134, 137], which represents extra overhead besides the chaotic systems solution. Our scheme depends on rotation angle modulation by the plaintext image, followed by data substitution based on simple XOR logic operation. The rotating chaotic systems can be realized in digital hardware using methods of implementing the trigonometric functions [193]. Hardware realization methods were presented for fractional-order chaotic systems and can be also employed [32–34, 194]. However, hardware realization of chaotic systems and encryption schemes was more frequently presented than synchronization schemes [126]. Hence, hardware realization of the proposed synchronization-dependent encryption scheme can be considered in a future research that combines fractional-order chaotic systems, with trigonometric functions, synchronization and encryption digital realization. The scheme is also suitable for various types of data transmission: text, simple signals, speech whether applying both phases or the rotation angle modulation only as shown in Fig. 5.12. Moreover, it is tested for RGB images with the challenges: bulk data size, the correlations between adjacent pixels and high redundancy among the raw pixel, unlike the papers that used simple one dimensional signals [109, 110, 116, 128–130].

The encryption scheme was evaluated using more performance metrics than the reviewed papers and give a more precise key design than theirs. Focusing on fractional-order chaotic systems synchronization-dependent image encryption schemes [131–137], their security analyses included one or more of the following metrics: histograms, correlation, entropy and preliminary parameter space and sensitivity analysis. While [136] additionally included MSE and PSNR, [134] included DA analysis. In these works, only a preliminary analysis of key space and key sensitivity was presented through listing the parameters of the chaotic systems. However, the encryption key design, effective key space and precise sensitivity analysis were not given.

To avoid negative effects of the slight bounded, yet, nonzero synchronization error on decryption, some precautions should be considered in choosing the parameters settings. This can be overcome by using intermediate significant bits for PRNG or utilizing other PRNG methods different from extracting LSBs directly, such as permutation prior to bits

extraction [140]. For systems with uncertain parameters in the presence of unknown internal and external disturbances, a controller-observer approach can be adopted [116].

In the next sections, a preliminary discussion and proof of concept of more chaotic systems generalization methods are presented. These further methods include three-dimensional rotation and novel chaotic equations constructed in other coordinate systems.

5.3 Three-Dimensional Rotating Chaotic Systems

Chapter 4 presented three-dimensional affine transformations. This section extends the rotation approach of the previous two sections and focuses on three-dimensional rotation and its implementations. Recalling the transformation from $\underline{X} = [x \ y \ z]^T$ to $\underline{U} = [u \ v \ w]^T$ through rotation, a transformation of $\dot{\underline{X}} = f(\underline{X})$ to the rotated coordinates \underline{U} and its inverse can be applied to get a system with rotating solution. Such transformation can be expressed as a rotation matrix, quaternion or successive shearing as explained in this section. The same simple jerk-based system with piecewise nonlinearity (4.3) of Chapter 4 is used for validation.

5.3.1 Implementation I: Matrix-Based Rotation

5.3.1.1 Mathematical Analysis

Two-dimensional rotations can be extended to three-dimensional rotations by constructing elementary three-dimensional rotation matrices, which perform rotations individually about the three coordinate axes z , y , and x by angles θ_1 , θ_2 and θ_3 , respectively. The rotations about the three axes (R_{θ_1} , R_{θ_2} and R_{θ_3}) can be derived similar to the previous sections and applied to create general composite three-dimensional rotation with matrix R as follows:

$$\begin{bmatrix} u \\ v \\ w \end{bmatrix} = R \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \quad (5.21a)$$

$$R = \begin{bmatrix} \cos \theta_1 \cos \theta_2 & \cos \theta_3 \sin \theta_1 + \cos \theta_1 \sin \theta_3 \sin \theta_2 & \sin \theta_1 \sin \theta_3 - \cos \theta_1 \cos \theta_3 \sin \theta_2 \\ -\cos \theta_2 \sin \theta_1 & \cos \theta_1 \cos \theta_3 - \sin \theta_1 \sin \theta_3 \sin \theta_2 & \cos \theta_1 \sin \theta_3 + \cos \theta_3 \sin \theta_1 \sin \theta_2 \\ \sin \theta_2 & -\cos \theta_2 \sin \theta_3 & \cos \theta_3 \cos \theta_2 \end{bmatrix} \quad (5.21b)$$

5.3.1.2 Matrix-Based Rotating Chaotic System

This procedure is used to obtain the equations of the rotating simplest chaotic system through the algorithm:

Algorithm 1: Matrix-Based Rotation Algorithm

Generate the rotation matrices about the three axes.

Construct the final rotation matrix R and R^T .

Find $\underline{X}_i = R^T \underline{U}_i$.

Apply Euler numerical solution of (4.3) to find \underline{X}_{i+1} .

Find $\underline{U}_{i+1} = R \underline{X}_{i+1}$.

which can be rewritten in a single vector equation as:

$$\begin{aligned}\underline{U}_{i+1} &= R\underline{X}_{i+1} = R(\underline{X}_i + h\underline{f}(\underline{X}_i)) \\ &= R(R^T\underline{U}_i + h\underline{f}(R^T\underline{U}_i))\end{aligned}\quad (5.22)$$

where R^{-1} is replaced by R^T since rotation matrices are orthogonal. Figure 5.13 shows the projections of the attractor diagrams of both the original system (4.3), in light color (red), and the rotating system (5.22), in dark color (blue), at different values of the rotation angles (see the online colored version).

5.3.2 Implementation II: Quaternions-Based Rotation

Seeking a more compact formulation or implementation for the three-dimensional rotation, this section explores quaternion-rotation.

5.3.2.1 Mathematical Analysis

The quaternion group has 8 members:

$$\pm i, \pm j, \pm k, \pm 1, \quad (5.23)$$

where i , j and k are the orthonormal basis vectors, whose products are defined by:

$$i^2 = j^2 = k^2 = ijk = -1. \quad (5.24)$$

The linear combination of the real numbers a, b, c and s

$$q = s + ia + jb + kc \quad (5.25)$$

is a quaternion, which can also be rewritten as:

$$q = (s, a, b, c). \quad (5.26)$$

The set of all the combinations of q is called the quaternion algebra [195].

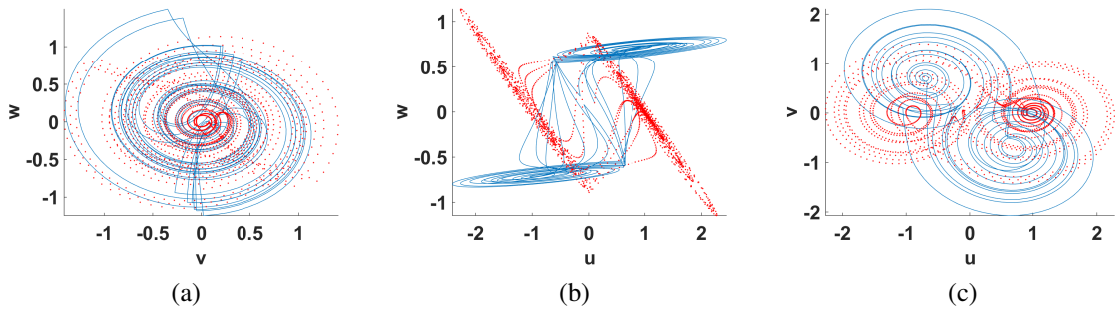


Figure 5.13: Projections of the attractor diagrams of (5.22) at (a) $\theta_1 = \theta_2 = 0$ and $\theta_3 = \pi/4$, (b) $\theta_1 = \theta_3 = 0$ and $\theta_2 = \pi/4$ and (c) $\theta_2 = \theta_3 = 0$ and $\theta_1 = \pi/4$.

By Euler's theorem, every rotation can be represented as a rotation around some axis \hat{k} with angle θ . In quaternion terms:

$$q = Rot(\hat{k}, \theta) = \left(\cos\left(\frac{\theta}{2}\right) + \sin\left(\frac{\theta}{2}\right)\hat{k} \right) = (\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4) \quad (5.27)$$

The operation qXq^{-1} rotates the 3D vector \underline{X} about the axis of q (\hat{k}) with an angle twice that of q (θ), according to the right hand rule. Composition of rotations is equivalent to quaternion multiplication, which is supposed to provide a more compact form of implementation.

5.3.2.2 Quaternion-Based Rotating Chaotic System

The quaternion-based rotating simplest chaotic system is given by the following algorithm.

<p>Algorithm 2: Quaternion-Based Rotation Algorithm</p> <p>Define three quaternions corresponding to the three axes each with a specific angle. Construct the final quaternion q from their product.</p> <p>For each iteration:</p> <p>Find $\underline{X}_i = q^{-1}\underline{U}_i q$. Apply Euler numerical solution of (4.3) to find \underline{X}_{i+1}. Find $\underline{U}_{i+1} = q\underline{X}_{i+1}q^{-1}$.</p>

The algorithm can be rewritten in the form of a single vector equation as follows.

$$\begin{aligned} \underline{U}_{i+1} &= q\underline{X}_{i+1}q^{-1} = q\left(\underline{X}_i + hf(\underline{X}_i)\right)q^{-1} \\ &= q\left(q^{-1}\underline{U}_i q + hf\left(q^{-1}\underline{U}_i q\right)\right)q^{-1} \end{aligned} \quad (5.28)$$

The results from the two implementations, matrix-based and quaternion-based, are roughly identical/coinciding as shown in Fig. 5.14.

5.3.3 Implementation III: Shearing-Based Rotation

In this section, 3D rotation is implemented using matrix multiplication as well. Yet, each matrix represents a 2D skewing, which is alternatively called non-symmetrical rotation. It is another workaround that may provide a more compact or simpler implementation of 3D rotation. However, in order to perform rotation through shearing, the shearing parameters need to be first computed from the rotation angle θ [196]

5.3.3.1 Mathematical Analysis of 2D Skewing

A two-dimensional shear operation has the following matrix representations:

$$Shear - X(\alpha) = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}, \quad Shear - Y(\beta) = \begin{bmatrix} 1 & 0 \\ \beta & 1 \end{bmatrix}, \quad (5.29)$$

where $Shear - X(\alpha)$ and $Shear - Y(\beta)$ matrices represent shears parallel to the x and y -axis, respectively. For instance, $Shear - X(\alpha)$ results in $x' = x + \alpha y$, while $y' = y$ is unchanged.

Two-dimensional rotation can be implemented by the following steps:

1. a shear along one axis,

2. a shear along the second axis,
3. another shear along the first axis,

which can be formulated as follows:

$$ShearX(\alpha)ShearY(\beta)ShearX(\gamma) = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \beta & 1 \end{bmatrix} \begin{bmatrix} 1 & \gamma \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1+\alpha\beta & \alpha+\gamma+\alpha\beta\gamma \\ \beta & 1+\beta\gamma \end{bmatrix} \quad (5.30)$$

Equating the familiar rotation matrix to (5.30) and solving for α, β and γ as follows:

$$\begin{aligned} \beta &= -\sin\theta, \\ 1+\alpha\beta &= \cos\theta, \\ 1-\alpha\sin\theta &= \cos\theta, \\ \alpha &= \frac{1-\cos\theta}{\sin\theta}, \\ \alpha &= \tan\frac{\theta}{2}, \\ 1+\alpha\beta &= 1+\beta\gamma, \\ \gamma &= \alpha \end{aligned} \quad (5.31)$$

yields $\alpha = \gamma = \tan\frac{\theta}{2}$ and $\beta = -\sin\theta$, which are totally represented in terms of θ .

Therefore, to obtain the skewed system in two-dimensional plane we define

$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} 1+\alpha\beta & \alpha+\gamma+\alpha\beta\gamma \\ \beta & 1+\beta\gamma \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}, \quad (5.32)$$

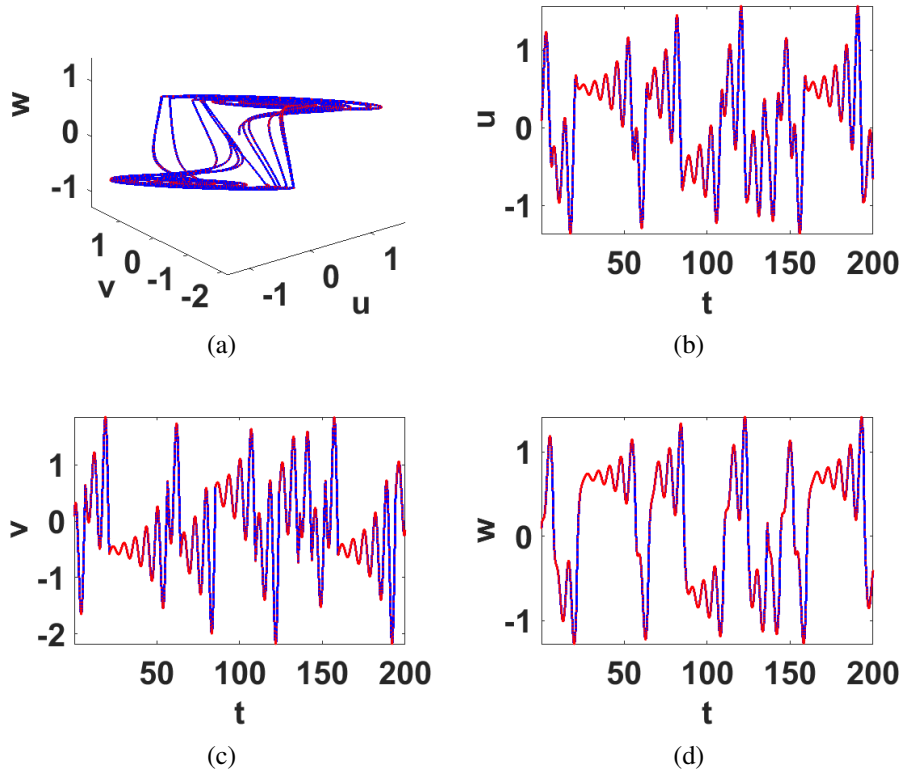


Figure 5.14: Attractor diagram and time series from the rotation-matrix and quaternion-based implementations.

and its inverse

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 + \gamma\beta & -\alpha - \gamma - \alpha\beta\gamma \\ -\beta & 1 + \beta\alpha \end{bmatrix} \begin{bmatrix} u \\ v \end{bmatrix}, \quad (5.33)$$

Hence, the skewed simplest system rotating about z axis is given by:

$$\begin{aligned} \dot{u} &= (1 + \alpha\beta)(-\beta u + (1 + \beta\alpha)v) + (\alpha + \gamma + \alpha\beta\gamma)w, \\ \dot{v} &= \beta(-\beta u + (1 + \beta\alpha)v) + (1 + \beta\gamma)w, \\ \dot{w} &= -a(w - \beta u + (1 + \beta\alpha)v + (1 + \gamma\beta)u + (-\alpha - \gamma - \alpha\beta\gamma)v - \text{sgn}((1 + \gamma\beta)u + (-\alpha - \gamma - \alpha\beta\gamma)v)). \end{aligned} \quad (5.34)$$

To cancel any of the shearing effects, the corresponding parameter is set to zero.

5.3.3.2 Shearing-Based Rotating Chaotic System

Shearing-Based Rotation is applied to the simplest chaotic system in a similar manner to Algorithm 1 and (5.22) of Section 5.3.1, except for computing R_{θ_1} by replacing $\begin{bmatrix} \cos \theta_1 & \sin \theta_1 \\ -\sin \theta_1 & \cos \theta_1 \end{bmatrix}$ by $\begin{bmatrix} 1 & \alpha_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \beta_1 & 1 \end{bmatrix} \begin{bmatrix} 1 & \gamma_1 \\ 0 & 1 \end{bmatrix}$ and similarly for $R_{\theta_2}(\alpha_2, \beta_2, \gamma_2)$ and $R_{\theta_3}(\alpha_3, \beta_3, \gamma_3)$.

Figure 5.15 validates the achievement of rotation by -20° using three successive shears. The results shown in Fig. 5.16 are roughly identical to/coinciding with those obtained from the two previous implementations, matrix-based and quaternion-based. Hence, the three implementations are roughly equivalent.

For future work, digital design of the three proposed implementations will be proposed and compared regarding both accuracy and efficiency.

5.3.4 Spatially Rotating Fractional-Order System Realization

This section applies Implementation I to (5.8). This results in a spatially rather than only planarly rotating attractor. In case of fractional-order systems, Algorithm 1 is modified as follows.

Algorithm 3: Matrix-Based Rotation Algorithm for Fractional-Order Systems

Construct the rotation matrix R and R^T .
Find $X_i = R^T U_i$.
Apply GL method to solve (5.8) and find X_{i+1} .
Find $U_{i+1} = R X_{i+1}$.

Figure 5.17 shows an example of the spatially rotating system at rotation angles $(\theta_1, \theta_2, \theta_3) = (90^\circ, 90^\circ, 45^\circ)$.

Table 5.11 shows the experimental results on the oscilloscope. The 3D rotation is performed in $x - y$ plane with angles $\theta_1 = \theta_2 = \theta_3 = 90^\circ$. Table 5.11 also gives the hardware resources of the proposed algorithm for the same system parameters and window size of Table 5.5. The 2D rotation can also be realized using the 3D algorithm. However, from the hardware resources comparison, the 3D algorithm needs more resources than the 2D algorithm.

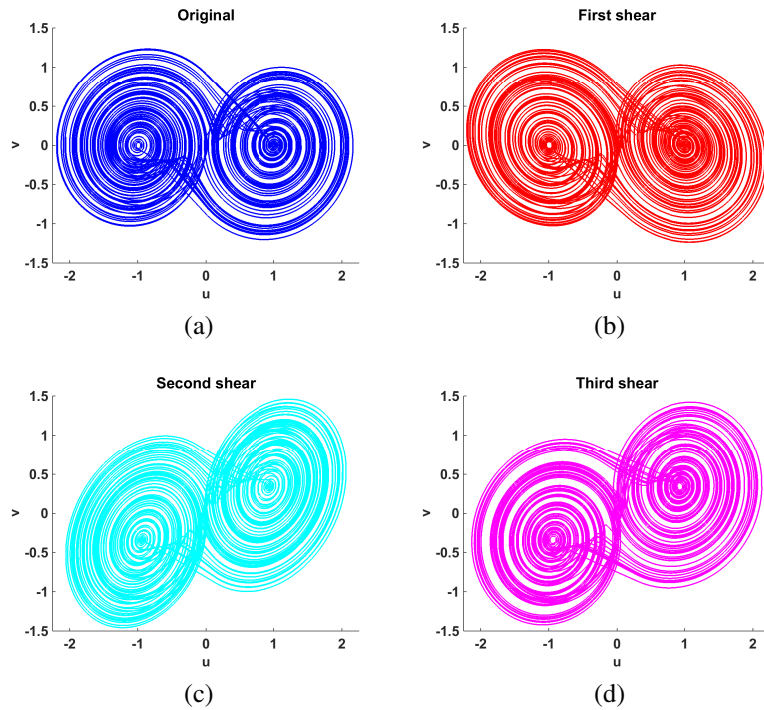


Figure 5.15: Rotation by -20° using three successive shears for the simplest chaotic system.

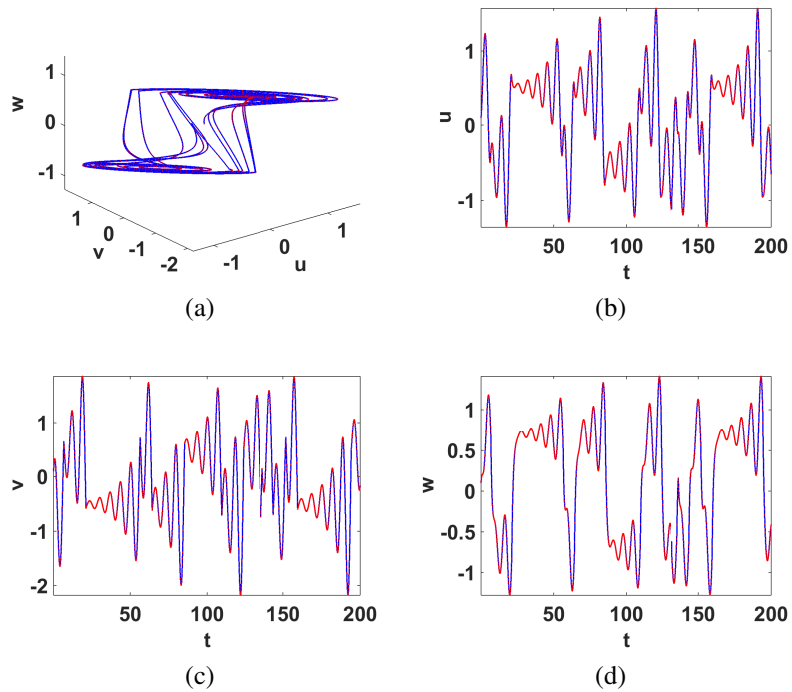


Figure 5.16: Attractor diagram and time series from the rotation-matrix and shearing-based implementations.

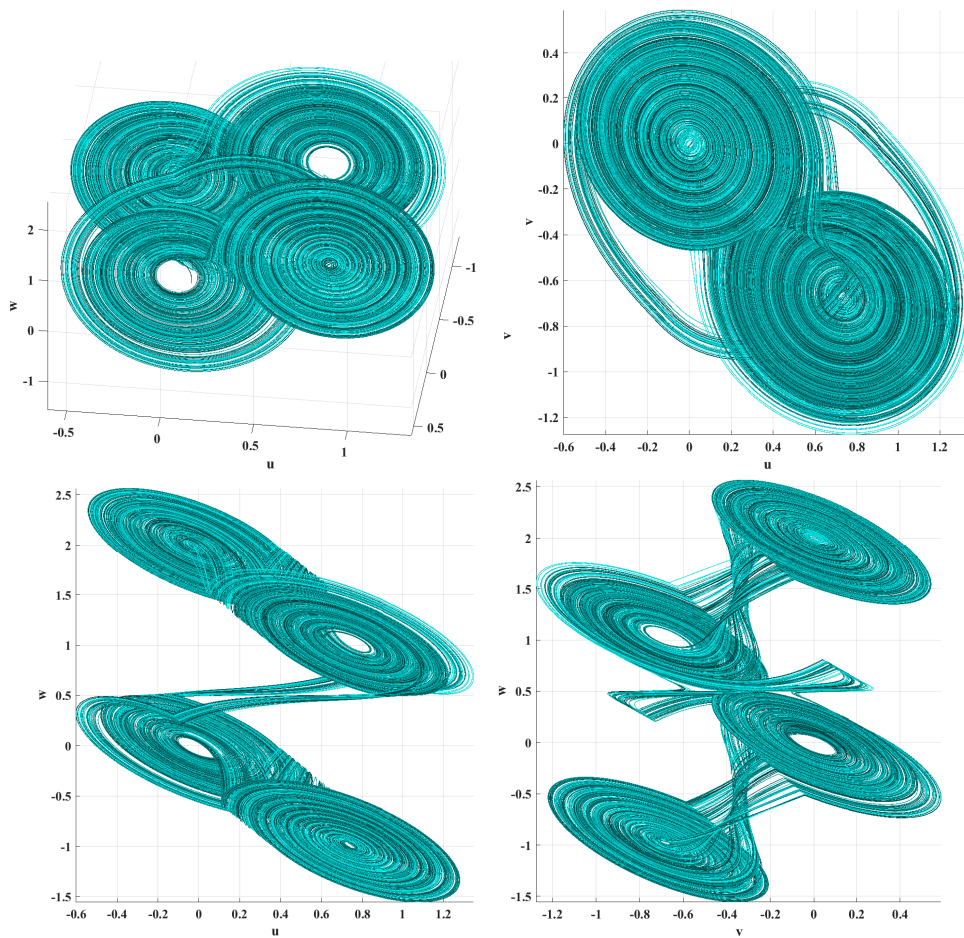
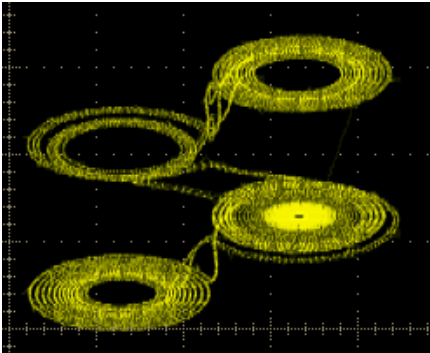


Figure 5.17: Spatially rotating fractional-order multi-scroll grid attractor at $(\theta_1, \theta_2, \theta_3) = (90^\circ, 90^\circ, 45^\circ)$.

Table 5.11: 3D rotation FPGA summary and experimental results for the fractional-order multi-scroll grid attractor

Logic Utilization	3D Rotation
No of LUT	5636 out of 63400 (8%)
No of slice registers	1106 out of 126800 (0%)
Clock speed (MHz)	16.274
Throughput (Mbit/sec)	520.768
Oscilloscope results	

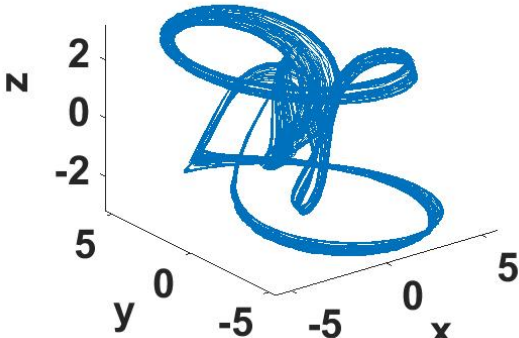
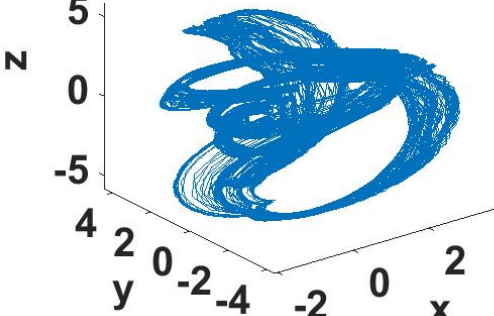
5.4 Preliminary Insights on Jerk-Analogues in Other Coordinates

Analogous to the jerk-based systems in the Cartesian coordinates, where \dot{x} , \ddot{x} and \dddot{x} appear, we attempt to construct similar systems in polar and spherical coordinates. Table 5.12 provides some preliminary examples and their attractor diagrams plotted using the transforms $x = \rho \cos \theta$, $y = \rho \sin \theta$ and $x = \rho \cos \theta \sin \phi$, $y = \rho \sin \theta \sin \phi$, $z = \rho \cos \phi$ for polar and spherical examples, respectively.

Compared to [98–100], these previous works focused on spherical coordinates only and included larger number of terms and nonlinearities. For example, the system proposed in [98] has 8 terms with 2 quadratic terms. The system proposed in [99] has 11 terms with 5 quadratic terms. The system proposed in [100] has 14 terms with 7 quadratic terms. Each of our proposed systems in Table 5.12 consists of 5 terms with a single nonlinear term, where the challenge is the type of nonlinearity.

For future work, analysis of the characteristics and behaviors of the proposed chaotic equation such as equilibria, stability, bifurcations, MLE can be studied for the different ranges of initial conditions and parameters. In addition, the nonlinear function can take other forms than the provided example. Moreover, it may be extended to a function of two variables $f(\rho, \theta)$ or more.

Table 5.12: Proposed chaotic equations in other coordinate systems

Polar	Spherical
$\dot{\rho} = \theta$ $\dot{\theta} = z$ $\dot{z} = -\theta - a z + f(\rho)$ $a = 0.6 \quad f(\rho) = 2.7 \sin(\rho)$	$\dot{\rho} = \theta$ $\dot{\theta} = \phi$ $\dot{\phi} = -\theta - a \phi + f(\rho)$ $a = 0.6 \quad f(\rho) = 2.7 \sin(\rho)$
	

Chapter 6: Conclusions and Future Work

Generalization of chaotic systems is highly required to enhance their controllability, sensitivity, randomness and unpredictability properties. Generating chaotic signals and attractors with controllable amplitude/size, polarity, offset/location, phase/orientation, and number of scrolls has recently flourished. This thesis presented several incremental generalization and control approaches towards achieving this controllability, which were successfully validated through numerical simulations. In addition, the proposed approaches were successfully utilized in several chaotic trajectory control, synchronization, PRNG, image and speech encryption applications. Moreover, digital hardware realization on FPGA was verified experimentally. Recalling the literature review from Chapter 2, non-autonomous control of chaotic systems through dynamic parameters is a hot research topic and it has just recently started to be employed in applications.

The first generalization approach proposed the controllable jerk-based chaotic systems with extra parameters of Chapter 3. The systems utilized generalized forms of well-known discrete time chaotic maps as the nonlinear function of the jerk equation. While the piecewise nonlinearity system employs the scaled tent map, the quadratic nonlinearity system employs the scaled logistic map. An analogy exists between the effects of the scaling parameters a and b in simple one-dimensional discrete chaotic maps and their effects in continuous jerk-based chaotic systems with more complicated dynamics. The impacts of these scaling parameters appear on the effective ranges of the parameter μ and the ranges of the obtained solution. However, the approach was only suitable for jerk-based systems and only limited attractor size and location control and limited multiplication of scrolls were allowed.

Numerical simulation and digital hardware realization were usually proposed as evidence of the parameter and initial conditions sensitivity and randomness properties of the proposed systems in digital applications. However, before proceeding to such steps, Chapter 3 focuses on the implementation sensitivity property and its conscious utilization in enhancing randomness. The algebraic associativity property of digitally implemented chaotic systems was assessed in software double-precision, single-precision floating-point and hardware fixed-point implementations on changing the order of terms addition and multiplication. Three implementation cases of each of three discretized chaotic systems were presented considering the order of additions. In addition, two more cases for one of these systems and four cases of the discrete logistic map were presented considering the order of multiplications. Despite sharing the common chaotic properties such as: strange attractor shape, bifurcations and MLE values, mismatches between time series of all the different cases were uncovered in floating-point implementations. On the other hand, fixed-point implementations exhibited mismatches only when changing order of multiplications. The mismatch or error increases gradually, but remains bounded and its three components form a strange attractor. The effect of this mismatch in a software image encryption application was demonstrated, where using an implementation with different order of execution results in wrong decryption. As an attempt to make use of this implementation sensitivity as an alternative randomness source, the resulting mismatch signals between various implementations were used as PRNG in an image encryption

application, which successfully passes the standard performance tests. Chapter 3 sets the reproducibility rules to be followed in the next chapters.

The second generalization approach proposed two-dimensional affine transformations: scaling, reflection, rotation, translation and/or shearing of chaotic systems and validated them for the simplest and Lorenz systems in Chapter 4. The effects on the time series, equilibrium points, attractor diagrams, bifurcations and MLE were demonstrated. This approach overpasses post-processing by applying transformations on the resulting time series. The six parameters, which are embedded in the differential equations of the chaotic system, control the system response and enhance its randomness and sensitivity. Trajectory control of the dynamic motion of the attractor was also presented exploring different trajectories. An image encryption system was proposed, which successfully passes the standard performance tests: PRNG NIST tests, encrypted image, histogram and its uniformity through chi square test, pixel correlation, MSE, entropy, PSNR, key sensitivity, resistance to brute force, differential and other security attacks. Transformed Lorenz system increases the key space and, hence, security in comparison to Lorenz system with an acceptable increase in the computation time as well as overpassing other recent related works.

This approach was further extended to three-dimensional affine transformations in Chapter 4, which were applied to control hidden attractors in fractional-order systems. Generally, an appropriate controlling scheme must be cautious with the increased sensitivity of the dynamical behavior of hidden attractors if the chaotic dynamics are required to be maintained. The proposed transformation framework overcomes the limitations imposed by the unique properties of hidden attractors. The proposed transformations were shown to preserve the chaotic dynamics of the original systems by means of strange attractors, spectral entropy and bifurcation diagrams. Non-autonomous parameter approaches were utilized to generate multiple wings around the same center point using multi-level pulse signals. In addition, non-autonomous translation parameters were used to generate distributed self-reproduced attractors along an arbitrary line, curve or surface. Compared to the very narrow, mostly specific single value, basin of attraction, parameter basin of attraction and fractional-orders of hidden attractors, the newly introduced parameters enable quite wide ranges. Hence, they are suitable for constructing the encryption key in digital chaos-based encryption systems. Having up to twelve degrees of freedom provided by the extra parameters enlarges key space and enhances resistance to brute force attacks.

A modification on affine transformations approach was presented in Chapter 5, where two-dimensional rotation, translation and scaling transformations were applied to two multi-scroll chaotic systems. These systems are characterized by wide basin of attraction and, hence, using the proposed transformations, they can span the whole space. The transformations enhance complex multi-scroll attractor structures and controllability through static and dynamic parameters. First, the transformed integer-order V-shape multi-scroll system was proposed and used to write letters, words and sentences. Second, a transformed fractional-order multi-scroll 2×2 grid chaotic system was proposed, utilized successfully in speech and image encryption applications and verified experimentally on FPGA using GL technique and CORDIC algorithm.

Dynamic rotation of fractional-order chaotic systems was further utilized successfully in a novel synchronization-dependent RGB image encryption application in Chapter 5. The

generalized synchronization scheme also includes dynamic scaling factors and dynamic switches. Moreover, it enables several systems participation in the constructed master. Various synchronization cases were validated in spite of how difficult the master response tracking is when all these dynamic signals are present. The synchronization-dependent encryption scheme employs angle modulation using the plaintext and XOR logic operation for plaintext image substitution. The performance of the scheme was evaluated for three synchronization scenarios through the standard tests, where it successfully passed them.

As an extension of 2D planar rotation, three different implementations of spatially rotating simplest chaotic system: matrix-based, quaternions-based and shearing-based were presented and validated in Chapter 5. The rotation matrix-based implementation was experimentally verified for the fractional-order multi-scroll 2×2 grid chaotic system of Chapter 5. Preliminary results on generalized chaotic systems in polar and spherical coordinate systems were also presented with fewer number of terms than recent related works.

For future work, the following items can be considered:

- Research ideas similar to the generalized maps utilized in Chapter 3 can be extended from the discrete domain to the continuous domain and combined to produce new systems. Increased nonlinearity and extra degrees of freedom can be added to the systems through using more complicated maps with extra parameters such as the generalized transition and generalized modified transition maps [197].
- Besides the affine transformations utilized in Chapter 4, nonlinear transformations can be applied to obtain more random and sensitive time series. In addition, they can be utilized in robotic applications for random motion planning along a prescribed trajectory.
- The multi-characters of Chapter 5 should not necessarily be written successively and the parameters settings can be adjusted to generate multiple-rounds of motion between the characters. Instead of manual parameter manipulation through piecewise definitions and Heaviside function, all letters of the alphabet can be generated and the width and height of each character as well as its position can be reported. An automated design for writing words and statements with chaotic attractors can be presented, which may utilize pattern recognition techniques to generate the parameters setup corresponding to an input word or statement.
- Regarding the synchronization-dependent image encryption system of Chapter 5, a controller-observer approach can be adopted to be suitable for synchronizing systems with uncertain parameters in the presence of unknown internal and external disturbances.
- Digital design of the three implementations of spatially rotating chaotic systems in Chapter 5 can be proposed and compared regarding both accuracy and efficiency.
- The chaotic equations in polar and spherical coordinates proposed in Chapter 5 can be mathematically analyzed considering equilibria, stability, bifurcations, MLE can be studied for the different ranges of initial conditions and parameters. In addition, the nonlinear function can take other forms than the provided example. Moreover, it may be extended to a function of two variables $f(\rho, \theta)$ or more.

References

- [1] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the atmospheric sciences*, vol. 20, no. 2, pp. 130–141, 1963.
- [2] S. H. Strogatz, *Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering*. Westview press, 2014.
- [3] W. S. Sayed, A. G. Radwan, H. A. Fahmy, and A. Elsedeeq, "Trajectory control and image encryption using affine transformation of Lorenz system," *Egyptian Informatics Journal*, 2020.
- [4] W. S. Sayed and A. G. Radwan, "Generalized switched synchronization and dependent image encryption using dynamically rotating fractional-order chaotic systems," *AEU-International Journal of Electronics and Communications*, p. 153268, 2020.
- [5] W. S. Sayed, A. G. Radwan, H. A. Fahmy, and A. El-Sedeek, "Software and hardware implementation sensitivity of chaotic systems and impact on encryption applications," *Circuits, Systems, and Signal Processing*, vol. 39, no. 11, pp. 5638–5655, 2020.
- [6] W. S. Sayed, A. G. Radwan, H. A. Fahmy, and A. Elsedeeq, "All-dynamic synchronization of rotating fractional-order chaotic systems," in *2019 Novel Intelligent and Leading Emerging Sciences Conference (NILES)*, vol. 1, pp. 226–229, IEEE, 2019.
- [7] W. S. Sayed, A. G. Radwan, M. Elnawawy, H. Orabi, A. Sagahyoon, F. Aloul, A. S. Elwakil, H. Fahmy, and A. El-Sedeek, "Two-dimensional rotation of chaotic attractors: Demonstrative examples and FPGA realization," *Circuits, Systems, and Signal Processing*, vol. 38, no. 10, pp. 4890–4903, 2019.
- [8] W. S. Sayed, A. G. Radwan, and H. A. Fahmy, "Chaos and bifurcation in controllable jerk-based self-excited attractors," in *Nonlinear Dynamical Systems with Self-Excited and Hidden Attractors*, pp. 45–70, Springer, 2018.
- [9] W. S. Sayed, A. G. Radwan, and H. A. Fahmy, "Chaotic systems based on jerk equation and discrete maps with scaling parameters," in *2017 6th International Conference on Modern Circuits and Systems Technologies (MOCASST)*, pp. 1–4, IEEE, 2017.
- [10] P. S. Gohari, H. Mohammadi, and S. Taghvaei, "Using chaotic maps for 3D boundary surveillance by quadrotor robot," *Applied Soft Computing*, vol. 76, pp. 68–77, 2019.

- [11] A. G. Radwan, S. H. AbdElHaleem, and S. K. Abd-El-Hafiz, “Symmetric encryption algorithms using chaotic and non-chaotic generators: A review,” *Journal of advanced research*, vol. 7, no. 2, pp. 193–208, 2016.
- [12] W. S. Sayed, M. F. Tolba, A. G. Radwan, S. K. Abd-El-Hafiz, and A. M. Soliman, “A switched chaotic encryption scheme using multi-mode generalized modified transition map,” *Multimedia Tools and Applications*, pp. 1–30, 2020.
- [13] H. Wang, H.-F. Liang, and Z.-H. Miao, “A new color image encryption scheme based on chaos synchronization of time-delay Lorenz system,” *Advances in Manufacturing*, vol. 4, no. 4, pp. 348–354, 2016.
- [14] C. Li, J. C. Sprott, Z. Yuan, and H. Li, “Constructing chaotic systems with total amplitude control,” *International Journal of Bifurcation and Chaos*, vol. 25, no. 10, p. 1530025, 2015.
- [15] B. M. Steinhaus, “Estimating cardiac transmembrane activation and recovery times from unipolar and bipolar extracellular electrograms: a simulation study,” *Circulation research*, vol. 64, no. 3, pp. 449–462, 1989.
- [16] I. Obeid, J. C. Morizio, K. A. Moxon, M. A. Nicolelis, and P. D. Wolf, “Two multichannel integrated circuits for neural recording and signal processing,” *IEEE transactions on biomedical engineering*, vol. 50, no. 2, pp. 255–258, 2003.
- [17] K. T. Alligood, T. D. Sauer, and J. A. Yorke, *Chaos*. Springer, 1996.
- [18] G. Leonov, N. Kuznetsov, and V. Vagitsev, “Hidden attractor in smooth Chua systems,” *Physica D: Nonlinear Phenomena*, vol. 241, no. 18, pp. 1482–1486, 2012.
- [19] T. Lu, C. Li, S. Jafari, and F. Min, “Controlling coexisting attractors of conditional symmetry,” *International Journal of Bifurcation and Chaos*, vol. 29, no. 14, p. 1950207, 2019.
- [20] J. Lü and G. Chen, “Generating multiscroll chaotic attractors: theories, methods and applications,” *International Journal of Bifurcation and Chaos*, vol. 16, no. 04, pp. 775–858, 2006.
- [21] B. Yu and G. Hu, “Constructing multiwing hyperchaotic attractors,” *International Journal of Bifurcation and Chaos*, vol. 20, no. 03, pp. 727–734, 2010.
- [22] N. Yu, Y.-W. Wang, X.-K. Liu, and J.-W. Xiao, “3D grid multi-wing chaotic attractors,” *International Journal of Bifurcation and Chaos*, vol. 28, no. 04, p. 1850045, 2018.
- [23] Q. Wu, Q. Hong, X. Liu, X. Wang, and Z. Zeng, “A novel amplitude control method for constructing nested hidden multi-butterfly and multiscroll chaotic attractors,” *Chaos, Solitons & Fractals*, vol. 134, p. 109727, 2020.

- [24] A. S. Elwakil, S. Ozoguz, and M. P. Kennedy, "Creation of a complex butterfly attractor using a novel lorenz-type system," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 49, no. 4, pp. 527–530, 2002.
- [25] A. S. Elwakil and S. Ozoguz, "Multiscroll chaotic oscillators: The nonautonomous approach," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 53, no. 9, pp. 862–866, 2006.
- [26] Q. Xie and Y. Zeng, "Generating different types of multi-double-scroll and multi-double-wing hidden attractors," *The European Physical Journal Special Topics*, vol. 229, pp. 1361–1371, 2020.
- [27] I. Petráš, *Fractional-order nonlinear systems: modeling, analysis and simulation*. Springer Science & Business Media, 2011.
- [28] W. S. Sayed, S. M. Ismail, L. A. Said, and A. G. Radwan, "On the fractional order generalized discrete maps," in *Mathematical Techniques of Fractional Order Systems*, pp. 375–408, Elsevier, 2018.
- [29] J. Sabatier, O. P. Agrawal, and J. T. Machado, *Advances in fractional calculus*, vol. 4. Springer, 2007.
- [30] D. Yousri, A. M. AbdelAty, L. A. Said, A. Elwakil, B. Maundy, and A. G. Radwan, "Parameter identification of fractional-order chaotic systems using different meta-heuristic optimization algorithms," *Nonlinear Dynamics*, vol. 95, no. 3, pp. 2491–2542, 2019.
- [31] I. Petras, *Fractional-order nonlinear systems: modeling, analysis and simulation*. Springer Science & Business Media, 2011.
- [32] M. F. Tolba, A. M. AbdelAty, N. S. Soliman, L. A. Said, A. H. Madian, A. T. Azar, and A. G. Radwan, "FPGA implementation of two fractional order chaotic systems," *AEU-International Journal of Electronics and Communications*, vol. 78, pp. 162–172, 2017.
- [33] A. D. Pano-Azucena, E. Tlelo-Cuautle, J. M. Muñoz-Pacheco, and L. G. de la Fraga, "Fpga-based implementation of different families of fractional-order chaotic oscillators applying grünwald–letnikov method," *Communications in Nonlinear Science and Numerical Simulation*, vol. 72, pp. 516–527, 2019.
- [34] E. Tlelo-Cuautle, A. D. Pano-Azucena, O. Guillén-Fernández, and A. Silva-Juárez, *Analog/Digital Implementation of Fractional Order Chaotic Circuits and Applications*. Springer, 2020.
- [35] J. C. Sprott, "Simple chaotic systems and circuits," *American Journal of Physics*, vol. 68, no. 8, pp. 758–763, 2000.
- [36] J. C. Sprott, "A new class of chaotic circuit," *Physics Letters A*, vol. 266, no. 1, pp. 19–23, 2000.

- [37] J. C. Sprott and S. J. Linz, “Algebraically simple chaotic flows,” *International Journal of Chaos Theory and Applications*, vol. 5, no. 2, pp. 1–20, 2000.
- [38] C. Li and J. Sprott, “Amplitude control approach for chaotic signals,” *Nonlinear Dynamics*, vol. 73, no. 3, pp. 1335–1341, 2013.
- [39] C. Li and J. Sprott, “Finding coexisting attractors using amplitude control,” *Nonlinear Dynamics*, vol. 78, no. 3, pp. 2059–2064, 2014.
- [40] C. Li, W. Hu, J. C. Sprott, and X. Wang, “Multistability in symmetric chaotic systems,” *The European Physical Journal Special Topics*, vol. 224, no. 8, pp. 1493–1506, 2015.
- [41] C. Li, J. C. Sprott, and H. Xing, “Crisis in amplitude control hides in multistability,” *International Journal of Bifurcation and Chaos*, vol. 26, no. 14, p. 1650233, 2016.
- [42] H. Chen, A. Bayani, A. Akgul, M.-A. Jafari, V.-T. Pham, X. Wang, and S. Jafari, “A flexible chaotic system with adjustable amplitude, largest lyapunov exponent, and local kaplan–yorke dimension and its usage in engineering applications,” *Nonlinear Dynamics*, vol. 92, no. 4, pp. 1791–1800, 2018.
- [43] N. Wang, G. Zhang, L. Ren, and H. Bao, “Coexisting asymmetric behavior and free control in a simple 3-D chaotic system,” *AEU-International Journal of Electronics and Communications*, p. 153234, 2020.
- [44] C. Li and J. C. Sprott, “Variable-boostable chaotic flows,” *Optik*, vol. 127, no. 22, pp. 10389–10398, 2016.
- [45] D. Vo Hoang, S. Takougang Kingni, and V.-T. Pham, “A no-equilibrium hyperchaotic system and its fractional-order form,” *Mathematical Problems in Engineering*, vol. 2017, 2017.
- [46] V.-T. Pham, A. Akgul, C. Volos, S. Jafari, and T. Kapitaniak, “Dynamics and circuit realization of a no-equilibrium chaotic system with a boostable variable,” *AEU-International Journal of Electronics and Communications*, vol. 78, pp. 134–140, 2017.
- [47] V.-T. Pham, X. Wang, S. Jafari, C. Volos, and T. Kapitaniak, “From wang–chen system with only one stable equilibrium to a new chaotic system without equilibrium,” *International Journal of Bifurcation and Chaos*, vol. 27, no. 06, p. 1750097, 2017.
- [48] J. Munoz-Pacheco, E. Zambrano-Serrano, C. Volos, O. Tacha, I. Stouboulos, and V.-T. Pham, “A fractional order chaotic system with a 3D grid of variable attractors,” *Chaos, Solitons & Fractals*, vol. 113, pp. 69–78, 2018.
- [49] C. Li, X. Wang, and G. Chen, “Diagnosing multistability by offset boosting,” *Nonlinear Dynamics*, vol. 90, no. 2, pp. 1335–1341, 2017.
- [50] X. Wang, V.-T. Pham, S. Jafari, C. Volos, J. M. Munoz-Pacheco, and E. Tlelo-Cuautle, “A new chaotic system with stable equilibrium: From theoretical model to circuit implementation,” *IEEE Access*, vol. 5, pp. 8851–8858, 2017.

- [51] L. K. Kengne, J. Kengne, and H. B. Fotsin, “The effects of symmetry breaking on the dynamics of a simple autonomous jerk circuit,” *Analog Integrated Circuits and Signal Processing*, vol. 101, no. 3, pp. 489–512, 2019.
- [52] Y. Yang, K. Ren, H. Qian, and X. Yao, “A simple hyperchaotic circuit with coexisting multiple bifurcations and offset boosting,” *The European Physical Journal Special Topics*, vol. 229, pp. 1163–1174, 2020.
- [53] V. K. Tamba, G. H. Kom, S. T. Kingni, J. R. Mboupda Pone, and H. B. Fotsin, “Analysis and electronic circuit implementation of an integer-and fractional-order four-dimensional chaotic system with offset boosting and hidden attractors,” *The European Physical Journal Special Topics*, vol. 229, pp. 1211–1230, 2020.
- [54] Q. Hong, Q. Xie, Y. Shen, and X. Wang, “Generating multi-double-scroll attractors via nonautonomous approach,” *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 26, no. 8, p. 083110, 2016.
- [55] Q. Hong, Q. Xie, and P. Xiao, “A novel approach for generating multi-direction multi-double-scroll attractors,” *Nonlinear Dynamics*, vol. 87, no. 2, pp. 1015–1030, 2017.
- [56] Q. Hong, Y. Li, X. Wang, and Z. Zeng, “A versatile pulse control method to generate arbitrary multidirection multibutterfly chaotic attractors,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 38, no. 8, pp. 1480–1492, 2018.
- [57] Q. Wu, Q. Hong, X. Liu, X. Wang, and Z. Zeng, “Constructing multi-butterfly attractors based on sprott C system via non-autonomous approaches,” *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 29, no. 4, p. 043112, 2019.
- [58] Q. Su, C. Wang, H. Chen, J. Sun, and X. Zhang, “A new method for generating chaotic system with arbitrary shaped distributed attractors,” *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 28, no. 7, p. 073106, 2018.
- [59] C. Li and J. Sprott, “Chaotic flows with a single nonquadratic term,” *Physics Letters A*, vol. 378, no. 3, pp. 178–183, 2014.
- [60] C. Li, J. C. Sprott, A. Akgul, H. H. Iu, and Y. Zhao, “A new chaotic oscillator with free control,” *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 27, no. 8, p. 083101, 2017.
- [61] W. Hu, A. Akgul, C. Li, T. Zheng, and P. Li, “A switchable chaotic oscillator with two amplitude–frequency controllers,” *Journal of Circuits, Systems and Computers*, vol. 26, no. 10, p. 1750158, 2017.
- [62] X. Zhang, C. Li, T. Lei, Z. Liu, and C. Tao, “A symmetric controllable hyperchaotic hidden attractor,” *Symmetry*, vol. 12, no. 4, p. 550, 2020.
- [63] I. Ahmad and B. Srisuchinwong, “Simple chaotic jerk flows with families of self-excited and hidden attractors: Free control of amplitude, frequency, and polarity,” *IEEE Access*, vol. 8, pp. 46459–46471, 2020.

- [64] C. Li, J. C. Sprott, W. Hu, and Y. Xu, “Infinite multistability in a self-reproducing chaotic system,” *International Journal of Bifurcation and Chaos*, vol. 27, no. 10, p. 1750160, 2017.
- [65] T. Gotthans and J. Petržela, “New class of chaotic systems with circular equilibrium,” *Nonlinear Dynamics*, vol. 81, no. 3, pp. 1143–1149, 2015.
- [66] T. Gotthans, J. C. Sprott, and J. Petržela, “Simple chaotic flow with circle and square equilibrium,” *International Journal of Bifurcation and Chaos*, vol. 26, no. 08, p. 1650137, 2016.
- [67] V.-T. Pham, S. Jafari, C. Volos, A. Giakoumis, S. Vaidyanathan, and T. Kapitaniak, “A chaotic system with equilibria located on the rounded square loop and its circuit implementation,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 63, no. 9, pp. 878–882, 2016.
- [68] X. Wang, V.-T. Pham, and C. Volos, “Dynamics, circuit design, and synchronization of a new chaotic system with closed curve equilibrium,” *Complexity*, vol. 2017, 2017.
- [69] V.-T. Pham, S. Jafari, and C. Volos, “A novel chaotic system with heart-shaped equilibrium and its circuital implementation,” *Optik*, vol. 131, pp. 343–349, 2017.
- [70] S. Vaidyanathan, A. Sambas, and M. Mamat, “A new chaotic system with axe-shaped equilibrium, its circuit implementation and adaptive synchronization,” *Archives of Control Sciences*, vol. 28, 2018.
- [71] A. Sambas, S. Vaidyanathan, M. Mamat, M. A. Mohamed, and M. S. Ws, “A new chaotic system with a pear-shaped equilibrium and its circuit simulation,” *International Journal of Electrical and Computer Engineering*, vol. 8, no. 6, p. 4951, 2018.
- [72] S. Mobayen, C. K. Volos, S. Kaçar, and Ü. Çavuşoğlu, “New class of chaotic systems with equilibrium points like a three-leaved clover,” *Nonlinear Dynamics*, vol. 91, no. 2, pp. 939–956, 2018.
- [73] S. Mobayen, S. Vaidyanathan, A. Sambas, S. Kacar, and Ü. Çavuşoğlu, “A novel chaotic system with boomerang-shaped equilibrium, its circuit implementation and application to sound encryption,” *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, no. 1, pp. 1–12, 2019.
- [74] A. Sambas, S. Vaidyanathan, E. Tlelo-Cuautle, S. Zhang, O. Guillen-Fernandez, Y. Hidayat, G. Gundara, *et al.*, “A novel chaotic system with two circles of equilibrium points: Multistability, electronic circuit and FPGA realization,” *Electronics*, vol. 8, no. 11, p. 1211, 2019.
- [75] V.-T. Pham, S. Jafari, X. Wang, and J. Ma, “A chaotic system with different shapes of equilibria,” *International Journal of Bifurcation and Chaos*, vol. 26, no. 04, p. 1650069, 2016.

- [76] V.-T. Pham, S. Jafari, C. Volos, S. Vaidyanathan, and T. Kapitaniak, “A chaotic system with infinite equilibria located on a piecewise linear curve,” *Optik*, vol. 127, no. 20, pp. 9111–9117, 2016.
- [77] E. Tlelo-Cuautle, L. G. de la Fraga, V.-T. Pham, C. Volos, S. Jafari, and A. de Jesus Quintas-Valles, “Dynamics, FPGA realization and application of a chaotic system with an infinite number of equilibrium points,” *Nonlinear Dynamics*, vol. 89, no. 2, pp. 1129–1139, 2017.
- [78] S. T. Kingni, V.-T. Pham, S. Jafari, and P. Wofo, “A chaotic system with an infinite number of equilibrium points located on a line and on a hyperbola and its fractional-order form,” *Chaos, Solitons & Fractals*, vol. 99, pp. 209–218, 2017.
- [79] V.-T. Pham, C. Volos, T. Kapitaniak, S. Jafari, and X. Wang, “Dynamics and circuit of a chaotic system with a curve of equilibrium points,” *International Journal of Electronics*, vol. 105, no. 3, pp. 385–397, 2018.
- [80] V.-T. Pham, C. Volos, S. T. Kingni, T. Kapitaniak, and S. Jafari, “Bistable hidden attractors in a novel chaotic system with hyperbolic sine equilibrium,” *Circuits, Systems, and Signal Processing*, vol. 37, no. 3, pp. 1028–1043, 2018.
- [81] Y. Chen and Q. Yang, “A new lorenz-type hyperchaotic system with a curve of equilibria,” *Mathematics and Computers in Simulation*, vol. 112, pp. 40–55, 2015.
- [82] S. Jafari, J. Sprott, V.-T. Pham, C. Volos, and C. Li, “Simple chaotic 3D flows with surfaces of equilibria,” *Nonlinear Dynamics*, vol. 86, no. 2, pp. 1349–1358, 2016.
- [83] X. Zhang and G. Chen, “Constructing an autonomous system with infinitely many chaotic attractors,” *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 27, no. 7, p. 071101, 2017.
- [84] C. Li, J. C. Sprott, and Y. Mei, “An infinite 2-D lattice of strange attractors,” *Nonlinear Dynamics*, vol. 89, no. 4, pp. 2629–2639, 2017.
- [85] C. Li and J. C. Sprott, “An infinite 3-D quasiperiodic lattice of chaotic attractors,” *Physics Letters A*, vol. 382, no. 8, pp. 581–587, 2018.
- [86] C. Li, J. C. Sprott, T. Kapitaniak, and T. Lu, “Infinite lattice of hyperchaotic strange attractors,” *Chaos, Solitons & Fractals*, vol. 109, pp. 76–82, 2018.
- [87] C. Li, T. Lu, G. Chen, and H. Xing, “Doubling the coexisting attractors,” *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 29, no. 5, p. 051102, 2019.
- [88] C. Zhang and S. Yu, “On constructing complex grid multi-wing hyperchaotic system: Theoretical design and circuit implementation,” *International Journal of Circuit Theory and Applications*, vol. 41, no. 3, pp. 221–237, 2010.
- [89] X. Ai, K. Sun, S. He, and H. Wang, “Design of grid multiscroll chaotic attractors via transformations,” *International Journal of Bifurcation and Chaos*, vol. 25, no. 10, p. 1530027, 2015.

- [90] S. Dai, K. Sun, S. He, and W. Ai, “Complex chaotic attractor via fractal transformation,” *Entropy*, vol. 21, no. 11, p. 1115, 2019.
- [91] X. Zhang, “Constructing a chaotic system with any number of attractors,” *International Journal of Bifurcation and Chaos*, vol. 27, no. 08, p. 1750118, 2017.
- [92] X. Wang and G. Chen, “Constructing a chaotic system with any number of equilibria,” *Nonlinear Dynamics*, vol. 71, no. 3, pp. 429–436, 2013.
- [93] K. Bouallegue, A. Chaari, and A. Toumi, “Multi-scroll and multi-wing chaotic attractor generated with julia process fractal,” *Chaos, solitons & fractals*, vol. 44, no. 1-3, pp. 79–85, 2011.
- [94] K. Bouallegue, “Gallery of chaotic attractors generated by fractal network,” *International Journal of Bifurcation and Chaos*, vol. 25, no. 01, p. 1530002, 2015.
- [95] Y. Guo, G. Qi, and Y. Hamam, “A multi-wing spherical chaotic system using fractal process,” *Nonlinear Dynamics*, vol. 85, no. 4, pp. 2765–2775, 2016.
- [96] N. B. Slimane, K. Bouallegue, and M. Machhout, “Designing a multi-scroll chaotic system by operating logistic map with fractal process,” *Nonlinear Dynamics*, vol. 88, no. 3, pp. 1655–1675, 2017.
- [97] A. Atangana, G. Bouallegue, and K. Bouallegue, “New multi-scroll attractors obtained via julia set mapping,” *Chaos, Solitons & Fractals*, vol. 134, p. 109722, 2020.
- [98] S. Jafari, S. Dehghan, G. Chen, S. T. Kingni, and K. Rajagopal, “Twin birds inside and outside the cage,” *Chaos, Solitons & Fractals*, vol. 112, pp. 135–140, 2018.
- [99] F. Nazarimehr, V.-T. Pham, K. Rajagopal, F. E. Alsaadi, T. Hayat, and S. Jafari, “A new imprisoned strange attractor,” *International Journal of Bifurcation and Chaos*, vol. 29, no. 13, p. 1950181, 2019.
- [100] L. Chen, E. Tlelo-Cuautle, I. I. Hamarash, V.-T. Pham, and H. R. Abdolmohammadi, “A novel chaotic system in the spherical coordinates,” *The European Physical Journal Special Topics*, vol. 229, pp. 1257–1263, 2020.
- [101] D. Mishra, R. Sharma, R. Ranjan, and M. Hanmandlu, “Security of RGB image data by affine hill cipher over $SL_n(F_q)$ and $M_n(F_q)$ domains with Arnold transform,” *Optik*, vol. 126, no. 23, pp. 3812–3822, 2015.
- [102] J. Ahmad and S. O. Hwang, “A secure image encryption scheme based on chaotic maps and affine transformation,” *Multimedia Tools and Applications*, vol. 75, no. 21, pp. 13951–13976, 2016.
- [103] Z. Hua, Y. Zhou, and H. Huang, “Cosine-transform-based chaotic system for image encryption,” *Information Sciences*, vol. 480, pp. 403–419, 2019.
- [104] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, “A new hybrid digital chaotic system with applications in image encryption,” *Signal Processing*, vol. 160, pp. 45–58, 2019.

- [105] J. Yang, Y. Chen, and F. Zhu, “Associated observer-based synchronization for uncertain chaotic systems subject to channel noise and chaos-based secure communication,” *Neurocomputing*, vol. 167, pp. 587–595, 2015.
- [106] A. Kajbaf, M. A. Akhaee, and M. Sheikhan, “Fast synchronization of non-identical chaotic modulation-based secure systems using a modified sliding mode controller,” *Chaos, Solitons & Fractals*, vol. 84, pp. 49–57, 2016.
- [107] M. F. A. Elzaher, M. Shalaby, Y. Kamal, and S. El Ramly, “Securing digital voice communication using non-autonomous modulated chaotic signal,” *Journal of Information Security and Applications*, vol. 34, pp. 243–250, 2017.
- [108] H. Wang, J.-M. Ye, Z.-H. Miao, and E. A. Jonckheere, “Robust finite-time chaos synchronization of time-delay chaotic systems and its application in secure communication,” *Transactions of the Institute of Measurement and Control*, vol. 40, no. 4, pp. 1177–1187, 2018.
- [109] W. Wang, X. Jia, X. Luo, J. Kurths, and M. Yuan, “Fixed-time synchronization control of memristive MAM neural networks with mixed delays and application in chaotic secure communication,” *Chaos, Solitons & Fractals*, vol. 126, pp. 85–96, 2019.
- [110] E. E. Mahmoud and O. A. Althagafi, “A new memristive model with complex variables and its generalized complex synchronizations with time lag,” *Results in Physics*, vol. 15, p. 102619, 2019.
- [111] B. Naderi and H. Kheiri, “Exponential synchronization of chaotic system and application in secure communication,” *Optik*, vol. 127, no. 5, pp. 2407–2412, 2016.
- [112] B. Vaseghi, M. A. Pourmina, and S. Mobayen, “Secure communication in wireless sensor networks based on chaos synchronization using adaptive sliding mode control,” *Nonlinear Dynamics*, vol. 89, no. 3, pp. 1689–1704, 2017.
- [113] M. H. Abd, F. R. Tahir, G. A. Al-Suhail, and V.-T. Pham, “An adaptive observer synchronization using chaotic time-delay system for secure communication,” *Nonlinear Dynamics*, vol. 90, no. 4, pp. 2583–2598, 2017.
- [114] I. Ahmad, M. Shafiq, and M. M. Al-Sawalha, “Globally exponential multi switching-combination synchronization control of chaotic systems for secure communications,” *Chinese journal of physics*, vol. 56, no. 3, pp. 974–987, 2018.
- [115] E. E. Mahmoud and S. Abo-Dahab, “Dynamical properties and complex anti synchronization with applications to secure communications for a novel chaotic complex nonlinear model,” *Chaos, Solitons & Fractals*, vol. 106, pp. 273–284, 2018.
- [116] S. Khorashadizadeh and M.-H. Majidi, “Chaos synchronization using the Fourier series expansion with application to secure communications,” *AEU-International Journal of Electronics and Communications*, vol. 82, pp. 37–44, 2017.

- [117] M. M. Zirkohi *et al.*, “Chaos synchronization using higher-order adaptive PID controller,” *AEU-International Journal of Electronics and Communications*, vol. 94, pp. 157–167, 2018.
- [118] L. N. Nguenjou, G. Kom, J. M. Pone, J. Kengne, and A. Tiedeu, “A window of multistability in Genesio-Tesi chaotic system, synchronization and application for securing information,” *AEU-International Journal of Electronics and Communications*, vol. 99, pp. 201–214, 2019.
- [119] K. Fallahi and H. Leung, “A chaos secure communication scheme based on multiplication modulation,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 2, pp. 368–383, 2010.
- [120] N. Khalifa, R. L. Filali, and M. Benrejeb, “A fast selective image encryption using discrete wavelet transform and chaotic systems synchronization,” *Information technology and control*, vol. 45, no. 3, pp. 235–242, 2016.
- [121] K. Nosrati, C. Volos, and A. Azemi, “Cubature Kalman filter-based chaotic synchronization and image encryption,” *Signal Processing: Image Communication*, vol. 58, pp. 35–48, 2017.
- [122] H. Tirandaz and A. Karimi-Mollaei, “Modified function projective feedback control for time-delay chaotic Liu system synchronization and its application to secure image transmission,” *Optik*, vol. 147, pp. 187–196, 2017.
- [123] H. Wang, J.-M. Ye, H.-F. Liang, and Z.-H. Miao, “A medical image encryption algorithm based on synchronization of time-delay chaotic system,” *Advances in Manufacturing*, vol. 5, no. 2, pp. 158–164, 2017.
- [124] L. Wang, T. Dong, and M.-F. Ge, “Finite-time synchronization of memristor chaotic systems and its application in image encryption,” *Applied Mathematics and Computation*, vol. 347, pp. 293–305, 2019.
- [125] G. M. Mahmoud, A. A. Farghaly, T. M. Abed-Elhameed, and M. M. Darwish, “Adaptive dual synchronization of chaotic (hyperchaotic) complex systems with uncertain parameters and its application in image encryption,” *Acta Physica Polonica B*, vol. 49, no. 11, pp. 1923–1939, 2018.
- [126] O. Guillén-Fernández, A. Meléndez-Cano, E. Tlelo-Cuautle, J. C. Núñez-Pérez, and J. de Jesus Rangel-Magdaleno, “On the synchronization techniques of chaotic oscillators and their FPGA-based implementation for secure image transmission,” *PloS one*, vol. 14, no. 2, 2019.
- [127] W. He, T. Luo, Y. Tang, W. Du, Y.-C. Tian, and F. Qian, “Secure communication based on quantized synchronization of chaotic neural networks under an event-triggered strategy,” *IEEE Transactions on Neural Networks and Learning Systems*, 2019.
- [128] R.-G. Li and H.-N. Wu, “Secure communication on fractional-order chaotic systems via adaptive sliding mode control with teaching–learning–feedback-based optimization,” *Nonlinear Dynamics*, vol. 95, no. 2, pp. 1221–1243, 2019.

- [129] L. J. Sheu, “A speech encryption using fractional chaotic systems,” *Nonlinear dynamics*, vol. 65, no. 1-2, pp. 103–108, 2011.
- [130] P. Muthukumar, P. Balasubramaniam, and K. Ratnavelu, “Sliding mode control for generalized robust synchronization of mismatched fractional order dynamical systems and its application to secure transmission of voice messages,” *ISA transactions*, vol. 82, pp. 51–61, 2018.
- [131] Y. Xu, H. Wang, Y. Li, and B. Pei, “Image encryption based on synchronization of fractional chaotic systems,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 10, pp. 3735–3744, 2014.
- [132] J. J. Montesinos-García and R. Martínez-Guerra, “Colour image encryption via fractional chaotic state estimation,” *IET Image Processing*, vol. 12, no. 10, pp. 1913–1920, 2018.
- [133] J. J. Montesinos-García and R. Martínez-Guerra, “A numerical estimation of the fractional-order Liouvillian systems and its application to secure communications,” *International Journal of Systems Science*, vol. 50, no. 4, pp. 791–806, 2019.
- [134] H. Tirandaz and A. Karami-Mollaei, “On active synchronization of fractional-order Bloch chaotic system and its practical application in secure image transmission,” *International Journal of Intelligent Computing and Cybernetics*, 2018.
- [135] P. Muthukumar, P. Balasubramaniam, and K. Ratnavelu, “A novel cascade encryption algorithm for digital images based on anti-synchronized fractional order dynamical systems,” *Multimedia Tools and Applications*, vol. 76, no. 22, pp. 23517–23538, 2017.
- [136] P. Muthukumar, P. Balasubramaniam, and K. Ratnavelu, “Sliding mode control design for synchronization of fractional order chaotic systems and its application to a new cryptosystem,” *International Journal of Dynamics and Control*, vol. 5, no. 1, pp. 115–123, 2017.
- [137] M. Shukla and B. Sharma, “Secure communication and image encryption scheme based on synchronisation of fractional order chaotic systems using backstepping,” *International Journal of Simulation and Process Modelling*, vol. 13, no. 5, pp. 473–485, 2018.
- [138] M. L. Barakat, A. S. Mansingka, A. G. Radwan, and K. N. Salama, “Generalized hardware post-processing technique for chaos-based pseudorandom number generators,” *ETRI Journal*, vol. 35, no. 3, pp. 448–458, 2013.
- [139] M. L. Barakat, A. S. Mansingka, A. G. Radwan, and K. N. Salama, “Hardware stream cipher with controllable chaos generator for colour image encryption,” *IET image processing*, vol. 8, no. 1, pp. 33–43, 2014.
- [140] W. S. Sayed, M. F. Tolba, A. G. Radwan, and S. K. Abd-El-Hafiz, “FPGA realization of a speech encryption system based on a generalized modified chaotic transition map and bit permutation,” *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 16097–16127, 2019.

- [141] A. G. Radwan, A. M. Soliman, and A.-L. El-Sedeek, “An inductorless CMOS realization of Chua’s circuit,” *Chaos, Solitons & Fractals*, vol. 18, no. 1, pp. 149–158, 2003.
- [142] A. T. Azar, C. Volos, N. A. Gerodimos, G. S. Tombras, V.-T. Pham, A. G. Radwan, S. Vaidyanathan, A. Ouannas, and J. M. Munoz-Pacheco, “A novel chaotic system without equilibrium: dynamics, synchronization, and circuit realization,” *Complexity*, vol. 2017, 2017.
- [143] Y. Bar-Yam, *Dynamics of complex systems*. CRC Press, 2019.
- [144] T. Bonny and A. S. Elwakil, “FPGA realizations of high-speed switching-type chaotic oscillators using compact VHDL codes,” *Nonlinear Dynamics*, vol. 93, no. 2, pp. 819–833, 2018.
- [145] M. A. Zidan, A. G. Radwan, and K. N. Salama, “The effect of numerical techniques on differential equation based chaotic generators,” in *International Conference on Microelectronics (ICM)*, pp. 1–4, IEEE, 2011.
- [146] A. S. Mansingka, A. G. Radwan, M. A. Zidan, and K. Salama, “Analysis of bus width and delay on a fully digital signum nonlinearity chaotic oscillator,” in *54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 1–4, IEEE, 2011.
- [147] W. S. Sayed, A. G. Radwan, A. A. Rezk, and H. A. Fahmy, “Finite precision logistic map between computational efficiency and accuracy with encryption applications,” *Complexity*, vol. 2017, 2017.
- [148] E. G. Nepomuceno, S. A. Martins, B. C. Silva, G. F. Amaral, and M. Perc, “Detecting unreliable computer simulations of recursive functions with interval extensions,” *Applied Mathematics and Computation*, vol. 329, pp. 408–419, 2018.
- [149] L. G. Nardo, E. G. Nepomuceno, J. Arias-Garcia, and D. N. Butusov, “Image encryption using finite-precision error,” *Chaos, Solitons & Fractals*, vol. 123, pp. 69–78, 2019.
- [150] W. S. Sayed, A. G. Radwan, and H. A. Fahmy, “Double-sided bifurcations in tent maps: Analysis and applications,” in *3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA)*, pp. 207–210, IEEE, 2016.
- [151] W. S. Sayed, A. G. Radwan, and H. A. Fahmy, “Design of positive, negative, and alternating sign generalized logistic maps,” *Discrete Dynamics in Nature and Society*, vol. 2015, 2015.
- [152] W. S. Sayed, A. G. Radwan, and H. A. Fahmy, “Design of a generalized bidirectional tent map suitable for encryption applications,” in *11th International Computer Engineering Conference (ICENCO)*, pp. 207–211, IEEE, 2015.

- [153] D. Monniaux, “The pitfalls of verifying floating-point computations,” *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 30, no. 3, p. 12, 2008.
- [154] A. Elwakil, K. Salama, and M. Kennedy, “A system for chaos generation and its implementation in monolithic form,” in *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*, vol. 5, pp. 217–220, IEEE, 2000.
- [155] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, “Determining lyapunov exponents from a time series,” *Physica D: Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, 1985.
- [156] V. N. Govorukhin, “Calculation lyapunov exponents for ODE.” MATLAB Central File Exchange, file ID 4628, 2004.
- [157] D. Goldberg, “What every computer scientist should know about floating-point arithmetic,” *ACM Computing Surveys (CSUR)*, vol. 23, no. 1, pp. 5–48, 1991.
- [158] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” tech. rep., DTIC Document, 2001.
- [159] J. D. Lawrence, *A catalog of special plane curves*. Courier Corporation, 2013.
- [160] A. G. Weber, “The USC-SIPI image database version 5,” *USC-SIPI Report*, vol. 315, pp. 1–24, 1997.
- [161] G. Ye and K.-W. Wong, “An efficient chaotic image encryption algorithm based on a generalized arnold map,” *Nonlinear dynamics*, vol. 69, no. 4, pp. 2079–2087, 2012.
- [162] H. Kwok and W. K. Tang, “A fast image encryption system based on chaotic maps with finite precision representation,” *Chaos, solitons & fractals*, vol. 32, no. 4, pp. 1518–1529, 2007.
- [163] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, 2007.
- [164] F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal, “A noisy channel tolerant image encryption scheme,” *Wireless personal communications*, vol. 77, no. 4, pp. 2771–2791, 2014.
- [165] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-Elyazeed, “Generalized double-humped logistic map-based medical image encryption,” *Journal of advanced research*, vol. 10, pp. 85–98, 2018.
- [166] X. Zhang and Z. Li, “Hidden extreme multistability in a novel 4D fractional-order chaotic system,” *International Journal of Non-linear Mechanics*, vol. 111, pp. 14–27, 2019.

- [167] M. Wang, X. Liao, Y. Deng, Z. Li, Y. Su, and Y. Zeng, “Dynamics, synchronization and circuit implementation of a simple fractional-order chaotic system with hidden attractors,” *Chaos, Solitons & Fractals*, vol. 130, p. 109406, 2020.
- [168] K. Li, J. Cao, and J.-M. He, “Hidden hyperchaotic attractors in a new 4D fractional order system and its synchronization,” *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 30, no. 3, p. 033129, 2020.
- [169] P. Zhou and K. Huang, “A new 4-D non-equilibrium fractional-order chaotic system and its circuit implementation,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 2005–2011, 2014.
- [170] K. Rajagopal, A. Karthikeyan, and A. K. Srinivasan, “FPGA implementation of novel fractional-order chaotic systems with two equilibriums and no equilibrium and its adaptive sliding mode synchronization,” *Nonlinear Dynamics*, vol. 87, no. 4, pp. 2281–2304, 2017.
- [171] H. Li, X. Liao, and M. Luo, “A novel non-equilibrium fractional-order chaotic system and its complete synchronization by circuit implementation,” *Nonlinear Dynamics*, vol. 68, no. 1-2, pp. 137–149, 2012.
- [172] D. Cafagna and G. Grassi, “Elegant chaos in fractional-order system without equilibria,” *Mathematical Problems in Engineering*, vol. 2013, 2013.
- [173] D. Cafagna and G. Grassi, “Fractional-order systems without equilibria: the first example of hyperchaos and its application to synchronization,” *Chinese Physics B*, vol. 24, no. 8, p. 080502, 2015.
- [174] K. Rajagopal, A. Akgul, S. Jafari, A. Karthikeyan, and I. Koyuncu, “Chaotic chameleon: Dynamic analyses, circuit implementation, FPGA design and fractional-order form with basic analyses,” *Chaos, Solitons & Fractals*, vol. 103, pp. 476–487, 2017.
- [175] V.-T. Pham, S. T. Kingni, C. Volos, S. Jafari, and T. Kapitaniak, “A simple three-dimensional fractional-order chaotic system without equilibrium: Dynamics, circuitry implementation, chaos control and synchronization,” *AEU-international Journal of Electronics and Communications*, vol. 78, pp. 220–227, 2017.
- [176] V.-T. Pham, A. Ouannas, C. Volos, and T. Kapitaniak, “A simple fractional-order chaotic system without equilibrium and its synchronization,” *AEU-International Journal of Electronics and Communications*, vol. 86, pp. 69–76, 2018.
- [177] X. Wang, A. Ouannas, V.-T. Pham, and H. R. Abdolmohammadi, “A fractional-order form of a system with stable equilibria and its synchronization,” *Advances in Difference Equations*, vol. 2018, no. 1, pp. 1–13, 2018.
- [178] J. M. Munoz-Pacheco, E. Zambrano-Serrano, C. Volos, S. Jafari, J. Kengne, and K. Rajagopal, “A new fractional-order chaotic system with different families of hidden and self-excited attractors,” *Entropy*, vol. 20, no. 8, p. 564, 2018.

- [179] G. Zheng, L. Liu, and C. Liu, “Hidden coexisting attractors in a fractional-order system without equilibrium: Analysis, circuit implementation, and finite-time synchronization,” *Mathematical Problems in Engineering*, vol. 2019, 2019.
- [180] C. Yan, H. Hongjun, L. Chenhui, and S. Guan, “Finite time synchronization for fractional order Sprott C systems with hidden attractors,” *Complexity*, vol. 2019, 2019.
- [181] H. Jahanshahi, A. Yousefpour, J. M. Munoz-Pacheco, I. Moroz, Z. Wei, and O. Castillo, “A new multi-stable fractional-order four-dimensional system with self-excited and hidden chaotic attractors: Dynamic analysis and adaptive synchronization using a novel fuzzy adaptive sliding mode control method,” *Applied Soft Computing*, vol. 87, p. 105943, 2020.
- [182] S. He, K. Sun, and H. Wang, “Complexity analysis and DSP implementation of the fractional-order Lorenz hyperchaotic system,” *Entropy*, vol. 17, no. 12, pp. 8299–8311, 2015.
- [183] D. E. Knuth, *Art of computer programming, volume 2: Seminumerical algorithms*. Addison-Wesley Professional, 2014.
- [184] M. A. Zidan, A. G. Radwan, and K. N. Salama, “Controllable V-shape multiscroll butterfly attractor: system and circuit implementation,” *International Journal of Bifurcation and Chaos*, vol. 22, no. 06, p. 1250143, 2012.
- [185] N. S. Soliman, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, “Fractional X-shape controllable multi-scroll attractor with parameter effect and FPGA automatic design tool software,” *Chaos, Solitons & Fractals*, vol. 126, pp. 292–307, 2019.
- [186] M. E. YALÇIN, J. A. Suykens, J. Vandewalle, and S. Özoğuz, “Families of scroll grid attractors,” *International Journal of Bifurcation and Chaos*, vol. 12, no. 01, pp. 23–41, 2002.
- [187] S. Lian, *Multimedia content encryption: techniques and applications*. CRC press, 2008.
- [188] “The royer track (audio), accessed,” 2020. <https://www.prosoundtraining.com/2010/03/10/a-downloadable-speech-track-the-royer-track/>.
- [189] M. Alçın, İ. Pehlivan, and İ. Koyuncu, “Hardware design and implementation of a novel ANN-based chaotic generator in FPGA,” *Optik*, vol. 127, no. 13, pp. 5500–5505, 2016.
- [190] W. S. Sayed, M. M. Henein, S. K. Abd-El-Hafiz, and A. G. Radwan, “Generalized dynamic switched synchronization between combinations of fractional-order chaotic systems,” *Complexity*, vol. 2017, 2017.
- [191] A. G. Radwan, K. Moaddy, and S. Momani, “Stability and non-standard finite difference method of the generalized Chua’s circuit,” *Computers & Mathematics with Applications*, vol. 62, no. 3, pp. 961–970, 2011.

- [192] A. G. Radwan, K. Moaddy, K. N. Salama, S. Momani, and I. Hashim, “Control and switching synchronization of fractional order chaotic systems using active control technique,” *Journal of advanced research*, vol. 5, no. 1, pp. 125–132, 2014.
- [193] J.-M. Muller, *Elementary functions: Algorithms and Implementations*. Springer.
- [194] E. Tlelo-Cuautle, J. D. Díaz-Muñoz, A. M. González-Zapata, R. Li, W. D. León-Salas, F. V. Fernández, O. Guillén-Fernández, and I. Cruz-Vega, “Chaotic image encryption using hopfield and hindmarsh–rose neurons implemented on FPGA,” *Sensors*, vol. 20, no. 5, p. 1326, 2020.
- [195] S. L. Altmann, *Rotations, quaternions, and double groups*. Courier Corporation, 2005.
- [196] A. W. Paeth, “A fast algorithm for general raster rotation,” in *Graphics Interface*, vol. 86, 1986.
- [197] W. S. Sayed, H. A. Fahmy, A. A. Rezk, and A. G. Radwan, “Generalized smooth transition map between tent and logistic maps,” *International Journal of Bifurcation and Chaos*, vol. 27, no. 01, p. 1730004, 2017.

الملخص

إن النظم الفوضوية المعممة والتي يمكن التحكم فيها مطلوبة في العديد من التطبيقات الهندسية المختلفة مثل: توليد الأرقام شبه العشوائية للاتصالات القائمة على الفوضى، وتخطيط الحركة، ونمذجة الظواهر الطبيعية والسلوك البشري. في هذه الرسالة، يتم عرض عدة طرق لتعميم النظم الفوضوية والتحكم فيها، مع إبراز مزايا هذه الطرق ومناقشة حدود عملها.

تتحكم الطريقة الأولى في الجاذبات المعتمدة على معدل تغير التسارع من خلال استخدام خرائط منفصلة معممة مع متغيرات إضافية كدوال غير خطية. كما يتم الكشف عن تأثير عوامل التنفيذ المختلفة على أنظمة التشفير الفوضوية التقليدية ويتم وضع توصيات لقابلية إعادة النتائج. يتم أيضاً استخدام إشارات عدم التطابق بين التطبيقات المختلفة قليلاً بوعي في تطبيقات توليد الأرقام شبه العشوائية والتشفير. أما عن الطريقة الثانية فهي مناسبة لأي من النظم الفوضوية، حيث يوفر التحويل الترابطي ثنائي الأبعاد إمكانيات التدرج، والانعكاس، والدوران، والقص، والنقل، وتوليد الجاذبات متعددة اللغائف من النظم التقليدية ذات الجاذبات الفردية أو المحدودة. بناء على الطريقة الثانية، يتم تقديم تطبيق تشفير للتحقق من صحة خصائص التشفير الجيدة ودور التعميم المقترح في تعزيز مساحة مفتاح التشفير، وبالتالي القدرة على صد هجمات القوة العاشمة. بعد ذلك، يتم تقديم امتداد للطريقة الثانية يشمل التحويلات ثلاثية الأبعاد والتحكم في نظم الترتيب الكسري بجاذبات مخفية التي تتميز ببعض الخصائص الصعبة. باستخدام التحويل الترابطي، يتم تطبيق التحكم غير المستقل في المسار وتوليد جاذبات ذاتية الإنتاج موزعة على هيئة خط أو منحني أو سطح اختياري من خلال المتغيرات الديناميكية.

نقدم في بقية الرسالة تعديل طفيف على الطريقة الثانية بحيث يتم الدوران في المستوى متبوعاً بالنقل والتدرج. ويتم تطبيق هذه الطريقة المعدلة على نظم متعددة اللغائف ذات حوض جاذبية عريض بالفعل لتكون قادرة على تغطية المساحة بأكملها. يتم تصميم كاتب فوضوي متعدد الأحرف اعتماداً على الدوران ثنائي الأبعاد لنظام فوضوي على شكل حرف V في المستوى مع التحكم في التدرج وتعزيز الإزاحة. يتم أيضاً تقديم جاذب فوضوي كسري شبكي متعدد اللغائف قابل للدوران والنقل. كذلك يستخدم بنجاح في تطبيقات تشفير الكلام والصور ويتم التحقق منه تجريبياً على مصفوفة البوابات المنطقية القابلة للبرمجة (FPGA). وفقاً لذلك، يتم اقتراح نظام معمم جديد للاتصال الآمن يعتمد على التزامنة التبادلية، وهو مناسب للاتصال من واحد إلى واحد ومن واحد إلى متعدد والاتصال البيني المتبادل وتبديل الأدوار. كما يتم تفعيله في تشفير الصور عن طريق تعديل زاوية الدوران لنظام الفوضوي من الدرجة الكسرية باستخدام الصورة قبل التشفير ثم يستخدم نفس النظام بعد ذلك كمولد للأرقام شبه العشوائية في استبدال عناصر الصورة من أجل التشفير، وقد اجتاز التشفير المقدم اختبارات الأداء القياسية بنجاح. يمتد تحويل الدوران ليصبح ثلاثي الأبعاد مع تقديم جاذبات فوضوية تدور مكانياً. يتم تقديم ثلاث طرق مختلفة لتنفيذ الدوران ثلاثي الأبعاد: القائمة على المصفوفة، والقائمة على الرباعية، والقائمة على القص. يتم التحقق من التنفيذ القائم على المصفوفة تجريبياً أيضاً. في النهاية يتم عرض نتائج أولية للنظم الفوضوية في الإحداثيات القطبية والكروية كطريقة ثالثة للتعميم والتحكم.



مهندسة:
تاريخ الميلاد:
الجنسية:
تاريخ التسجيل:
تاريخ المنح:
القسم:
الدرجة:
المشرفون:

وفاء صابر عبد الحليم سيد
١٩٩١٣٢٠
مصرية
٢٠١٥١١
٢٠٢٠-١-١١
الرياضيات و الفيزيكا الهندسية
دكتوراه الفلسفة

أ.د. عبد اللطيف الصديق حسين
أ.د. أحمد جمعة أحمد رضوان
جامعة النيل الأهلية
أ.د. حسام على حسن فهمي

المتحنون:

أ.د. حسن ابراهيم محمد حسن صالح (المتحن الخارجي)
قسم الهندسة الإشعاعية-المركز القومي لبحوث وتكنولوجيا الإشعاع-
هيئة الطاقة الذرية
أ.د. محمد عبدالعزيز أحمد البلتاجي (المتحن الداخلي)
أ.د. عبد اللطيف الصديق حسين (المشرف الرئيسي)
أ.د. أحمد جمعة أحمد رضوان (مشرف)
جامعة النيل الأهلية

عنوان الرسالة:

التعميم والتحكم في النظم الفوضوية باستخدام متغيرات إضافية والتحويل الترابطي

الكلمات الدالة:

الديناميات الكسرية، الجاذبات الخفية، تشفير الصور، التحكم غير المستقل، التزامن المبدل

ملخص الرسالة:

تقدم الرسالة طرق معممة لإنشاء الجاذبات الفوضوية المترتبة، المنعكسة، المدورة، المقصوصة و/أو المنقولة باستخدام متغيرات إضافية والتحويل الترابطي. نقوم بتعيين قواعد قابلة إعادة النتائج ومناقشة التطبيقات المحتملة لخاصية الحساسية للتنفيذ. نقوم بإنشاء جاذبات ذاتية الإنتاج موزعة على مسار اختياري باستخدام متغيرات ديناميكية. نقدم طريقة غير تقليدية للكتابة عبر نظام فوضوي متعدد العلامات والأحرف. نقوم بالتحقق من النظم المعممة المقدمة تجريبياً واستغلالها بنجاح في أنظمة تشفير بسيطة وأخرى تعتمد على التزامن.

التعميم والتحكم في النظم الفوضوية باستخدام متغيرات إضافية والتحويل
الترابطي

اعداد

وفاء صابر عبد الحليم سيد

رسالة مقدمة إلى كلية الهندسة - جامعة القاهرة

كجزء من متطلبات الحصول على درجة

دكتوراه الفلسفة

في

الرياضيات الهندسية

يعتمد من لجنة الممتحنين:

الاستاذ الدكتور: عبد اللطيف الصديق حسين المشرف الرئيسي

الاستاذ الدكتور: أحمد جمعة أحمد رضوان مشرف
جامعة النيل الأهلية

الاستاذ الدكتور: محمد عبدالعزيز أحمد البلتاجي الممتحن الداخلي

الاستاذ الدكتور: حسن ابراهيم محمد حسن صالح الممتحن الخارجي
قسم الهندسة الإشعاعية-المركز القومي لبحوث وتكنولوجيا الإشعاع-
هيئة الطاقة الذرية

كلية الهندسة - جامعة القاهرة

الجيزة - جمهورية مصر العربية

٢٠٢٠

التعميم والتحكم في النظم الفوضوية باستخدام متغيرات إضافية والتحويل
الترابطي

اعداد

وفاء صابر عبد الحليم سيد

رسالة مقدمة إلى كلية الهندسة - جامعة القاهرة

كجزء من متطلبات الحصول على درجة

دكتوراه الفلسفة

في

الرياضيات الهندسية

تحت اشراف

أ.د. أحمد جمعة أحمد رضوان

أستاذ

قسم الرياضيات و الفيزيكا الهندسية

كلية الهندسة - جامعة القاهرة

ومعار لجامعة النيل الأهلية

أ.د. عبد اللطيف الصديق حسين

أستاذ

قسم الرياضيات و الفيزيكا الهندسية

كلية الهندسة - جامعة القاهرة

أ.د. حسام على حسن فهمي

أستاذ

قسم الالكترونيات و الاتصالات الكهربائية

كلية الهندسة - جامعة القاهرة

كلية الهندسة - جامعة القاهرة

الجيزة - جمهورية مصر العربية

٢٠٢٠



التعميم والتحكم في النظم الفوضوية باستخدام متغيرات إضافية والتحويل الترابطي

اعداد

وفاء صابر عبد الحليم سيد

رسالة مقدمة إلى كلية الهندسة - جامعة القاهرة

كجزء من متطلبات الحصول على درجة

دكتوراه الفلسفة

في

الرياضيات الهندسية

كلية الهندسة - جامعة القاهرة

الجيزة - جمهورية مصر العربية

٢٠٢٠