



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
Phone: +201203226271
Address: 3 Msaken elsekka-elhadid-elgdeda,
Ramlet-Bolaq, Cairo
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 $\mu_{min} = -(1 + \frac{1}{b})$	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