

QUANTUM CHAOTIC CRYPTOGRAPHY: A NEW APPROACH

AFSHIN AKHSHANI

UNIVERSITI SAINS MALAYSIA

2015

QUANTUM CHAOTIC CRYPTOGRAPHY: A NEW APPROACH

by

AFSHIN AKHSHANI

**Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy**

July 2015

ACKNOWLEDGEMENTS

First and foremost, I have to thank God for somehow turning an innumerable amount of seemingly hard into easy and golden decisions. I am deeply grateful to my dissertation advisor, Professor Zainuriah Hassan, who allowed me the opportunity to take the next step in my scientific vocation and do my PhD. She allowed me the scope to follow my thoughts and develop my scientific skills, the freedom to investigate my interests, whilst always being available to provide guidance, inspiration and discussion whenever it was needed over a period of several years. I would like to thank Dr. Lim Siew Choo for her invaluable review of my thesis. Also, I would like to thank friends and all of my colleagues.

I would like to extend my special thanks to Professor Sohrab Behnia, who taught me a lot about how to survive in my future career, whether in industry or in academia.

I would like to express my deepest gratitude to my parents, my brother Amir, my sister Afsoun, who gave me the strength and will to follow my love for knowledge. I would like to extend my special thanks to my wife's parents for their kindness and unrelenting support. Of course, this thesis would not be possible without the unwavering support of my wonderful wife Mahsa. This thesis is dedicated to her patience, understanding and loving support.

TABLE OF CONTENTS

Acknowledgements.....	ii
Table of Contents	iii
List of Tables	x
List of Figures	xiii
List of Abbreviations	xxv
List of Symbols.....	xxvi
Abstrak.....	xxviii
Abstract	xxx

CHAPTER 1 – INTRODUCTION

1.1 Motivation of the Research	1
1.2 Problem Statement	4
1.3 Objectives	5
1.4 Organization of the Thesis	6

CHAPTER 2 – DYNAMICAL SYSTEMS: FOUNDATIONS AND BASIC CONCEPTS

2.1 Functions.....	8
2.1.1 Iterating a function	9
2.1.2 Phase space	10
2.2 Dynamical Systems.....	11
2.2.1 Fixed point	12
2.2.1.1 Classification of fixed point.....	13
2.2.1.2 Finding fixed points and stability classification	15
2.3 Determinism and Randomness.....	15
2.4 Invertible and Non-invertible Dynamical Systems.....	17

2.5	Linear and Non-linear Systems	18
2.6	Chaos	18
2.6.1	Definition of chaos	19
2.7	The Source of the Chaotic Behavior	20
2.8	Quantifying Chaos	21
2.8.1	Bifurcation diagram	22
2.8.2	Lyapunov exponent	24
2.8.3	Entropy	25
2.8.3.1	Shannon information entropy	26
2.8.3.2	Block entropy	27
2.8.3.3	Rényi entropy	28
2.8.3.4	Shannon mutual information	29
2.8.3.5	Kullback-Leibler divergence	31
2.8.3.6	Jensen-Shannon divergence.....	32
2.9	Fractal Geometry	33
2.9.1	Self-similarity	34
2.9.2	Dimensions	34
2.9.3	Topological Dimension	35
2.9.4	Self-similarity dimension	35
2.9.5	Box-counting dimension.....	37
2.9.6	Dimension of Cantor set	38
2.9.7	Lacunarity analysis.....	39
2.9.8	Succolarity analysis	44
2.9.8.1	Calculation of succolarity for box size 1×1 pixel	46
2.10	Synchronization	47
2.11	Synchronization of chaotic systems	48
2.12	Types of chaos synchronization.....	48

2.13	Applications of chaos synchronization	49
2.14	Quantum Chaos	50
2.14.1	A Short Introduction to Quantum World	50
2.14.2	Postulates of Quantum Mechanics	51
2.14.3	Quantum Chaos	53
2.14.4	Quantum Maps	55
2.14.5	The δ –kicked Rotor	56
2.14.5.1	The classical δ –kicked rotor	56
2.14.5.2	The quantum δ –kicked rotor	59

CHAPTER 3 – OVERVIEW ON CHAOS-BASED CRYPTOGRAPHY

3.1	Cryptography: Basic Concepts	61
3.1.1	Cryptanalysis	63
3.2	Chaos and Cryptography	64
3.3	Conventional and Chaotic Cryptography	65
3.4	Digital and Analog Chaos-based Cryptosystems	66
3.4.1	Digital degradation	67
3.5	Efficiency of Chaos-based Cryptosystem	68
3.6	Image Encryption	68
3.7	Pseudo Random Number Generator (PRNG)	70

CHAPTER 4 – A BRIEF INTRODUCTION TO WAVELET ANALYSIS

4.1	Fourier Transform	72
4.2	Short Time Fourier Transform	72
4.3	Wavelet Analysis	74
4.4	Continuous Wavelet Transform (CWT)	74
4.5	Discrete Wavelet Transform (DWT)	76

CHAPTER 5 – CHARACTERIZATION OF CHAOTIC MAPS BASED ON THE SCALE INDEX TECHNIQUE

5.1	Introduction	77
5.2	The Scale Index.....	78
5.3	Examples of Dynamical Systems	83
5.3.1	Discrete-time chaotic maps	83
5.3.1.1	Logistic map.....	83
5.3.1.2	Generalized logistic map.....	84
5.3.1.3	Hénon map	84
5.3.1.4	Quantum logistic map.....	84
5.3.1.5	Synchronized chaotic coupled map	85
5.3.2	Continuous-time chaotic maps	85
5.3.2.1	Rössler system	85
5.4	Results and Discussion	86

CHAPTER 6 – PSEUDO RANDOM NUMBER GENERATOR BASED ON SYNCHRONIZED CHAOTIC MAPS AND QUANTUM MAP

6.1	Introduction	95
6.2	Pseudo Random Number Generator Based on Synchronized Chaotic Maps	96
6.3	One-parameter Family of Chaotic Maps	98
6.4	Coupled Map in Synchronized State	99
6.4.1	Synchronization	100
6.5	Experimental Results	101
6.6	Pseudo Random Number Generator Based on Quantum Chaotic Map	108
6.7	Quantum Chaotic Map	112
6.8	Degree of Non-periodicity	113
6.8.1	Comparison of the Non-periodicity	116

6.9	Statistical Complexity Measure.....	116
6.10	Proposed Algorithm	120
6.11	Correlation Analysis.....	121
6.12	Tests for Randomness	123
6.12.1	Key space analysis	126
6.12.2	Guess-and-determine and distinguishing attacks	127
6.12.3	Differential attack	128
6.12.4	Analysis of speed	129
6.13	Concluding Remarks	130

CHAPTER 7 – AN IMAGE ENCRYPTION SCHEME BASED ON QUANTUM MAP

7.1	Introduction	132
7.2	Quantum Chaos.....	134
7.3	Quantum Chaotic Map	135
7.4	Proposed Algorithm	136
7.5	Experimental Results	137
7.6	Statistical Complexity	139
7.7	Security Analysis	141
7.7.1	Distribution of the cipher-text	141
7.7.2	Correlation analysis of two adjacent pixels	142
7.7.3	Key space analysis	144
7.7.4	Information entropy	144
7.7.5	Randomness tests for the cipher.....	145
7.7.6	Avalanche criterion	146
7.7.7	Differential attack	146
7.8	Conclusion	148

CHAPTER 8 – COMPREHENSIVE ANALYSIS OF CHAOS-BASED IMAGE ENCRYPTION ALGORITHMS BASED ON DIFFERENT ENTROPY MEASURES

8.1	Introduction	149
8.2	Definition of Entropy Measures	151
8.2.1	Shannon entropy	151
8.2.2	Block entropy	151
8.2.3	Rényi entropy and min-entropy	154
8.2.4	Mutual information	154
8.2.5	Kullback-Leibler (KL) divergence	154
8.2.6	Jensen-Shannon (JS) divergence	155
8.3	Comparison of Different Images Based on Entropy Measures	155
8.3.1	Mutual information	174
8.3.2	Kullback-Leibler (KL) divergence	175
8.3.3	Jensen-Shannon (JS) divergence	179
8.4	Summary and Discussion	181

CHAPTER 9 – LACUNARITY AND SUCCOLARITY ANALYSES OF CHAOS-BASED IMAGE CRYPTOSYSTEMS

9.1	Introduction	187
9.2	Definition of Fractal Measures	190
9.2.1	Box-counting dimension.....	190
9.2.2	Lacunarity	191
9.2.3	Succolarity.....	192
9.3	Fractal Dimension Analysis of Chaos-based Cipher Images	192
9.3.1	Verification of the box-counting algorithm	193
9.3.2	Box-counting dimension of cipher images.....	195
9.4	Lacunarity Analysis of Chaos-based Cipher Images	199

9.4.1	Verification of the lacunarity analysis	199
9.5	Lacunarity Analysis of Cipher Images	201
9.6	Succolarity Analysis of Chaos-based Cipher Images	208
9.7	Summary and Discussion	219
9.7.1	Fractal dimension	219
9.7.2	Lacunarity analysis.....	219
9.7.3	Succolarity analysis	221
CHAPTER 10 -CONCLUSIONS AND FUTURE RESEARCH		
10.1	Summary and Conclusions	224
10.2	Perspectives of Future Research	228
	References	230
	APPENDICES	257
	APPENDIX A – MULTIREOLUTION ANALYSIS (MRA)	258
	APPENDIX B – STABILITY ANALYSIS	260
B.1	Stability analysis of chaotic map	260
B.1.1	Invariant measure in synchronized state	260
B.1.2	KS-entropy in synchronized state	263
B.1.3	Lyapunov exponent in synchronized state	266
	List of Publications	268

LIST OF TABLES

		Page
Table 3.1	Level of cryptanalysis attacks.	63
Table 6.3	Max grade of ENT test suite.	106
Table 6.4	TestU01 test suite for the proposed PRNG.	106
Table 6.1	Results of the SP800-22 tests suite for the proposed PRNG.	107
Table 6.2	DIEHARD tests suite for the proposed PRNG.	108
Table 6.5	Correlation coefficients of three pairs of pseudo random sequences.	123
Table 6.6	Results of the SP800-22 tests suite for the 32-bit proposed PRNG.	124
Table 6.7	Results of the SP800-22 tests suite for the 32-bit proposed PRNG.	125
Table 6.8	DIEHARD tests suite for the 32-bit proposed PRNG.	125
Table 6.9	Max grade of ENT test suite.	126
Table 6.10	TestU01 test suite for the 32-bit proposed PRNG.	126
Table 6.11	Mean values of the absolute difference (d).	129
Table 7.1	Correlation coefficient of two adjacent pixels in simulated original image.	143
Table 7.2	TestU01 test suite for the 32-bit proposed quantum map.	145
Table 8.1	Shannon and min-entropy of the sample images.	164
Table 8.2	Mean-block entropy of the sample images.	165
Table 8.4	Shannon entropy of the cipher images.	168
Table 8.3	Chaos-based image encryption algorithms.	168
Table 8.5	Min-entropy of the cipher images.	172
Table 8.6	Mean-Block entropy of plain image <i>Boat</i> and corresponding ciphered images based on the algorithms in Table 8.3.	172

Table 8.7	Mean-Block entropy of plain image <i>Lena</i> and corresponding ciphered images based on the algorithms in Table 8.3.	173
Table 8.8	Mean-Block entropy of plain image <i>Peppers</i> and corresponding ciphered images based on the algorithms in Table 8.3.	174
Table 8.9	Mutual information of the plain images and corresponding cipher images.	175
Table 8.10	Kullback-Leiber divergence of the <i>Reference</i> and <i>Lena</i> ciphered images.	176
Table 8.11	Kullback-Leiber divergence of the <i>Reference</i> and <i>Boat</i> ciphered images.	177
Table 8.12	Kullback-Leiber divergence of the <i>Reference</i> and <i>Peppers</i> ciphered images.	178
Table 8.13	Mean of Kullback-Leiber divergence of three ciphered images.	179
Table 8.14	Jensen-Shannon divergence of three ciphered images.	180
Table 9.1	Chaos-based image encryption algorithms.	193
Table 9.2	Theoretical and estimated fractal dimensions of 2D <i>fBm</i> images.	195
Table 9.3	Fractal dimensions of cipher images.	195
Table 9.4	Fractal dimensions of the Reference, Pattern and Random noise images.	195
Table 9.5	Lacunarity values of cipher images at $\ln(r) \simeq 1$.	202
Table 9.6	Succolarity values ($\ln(\text{Succolarity} \times 10000)$) of <i>Boat</i> plain image.	210
Table 9.7	Succolarity values ($\ln(\text{Succolarity} \times 10000)$) of <i>Lena</i> plain image.	210
Table 9.8	Succolarity values ($\ln(\text{Succolarity} \times 10000)$) of <i>Peppers</i> plain image.	210
Table 9.9	Succolarity values ($\ln(\text{Succolarity} \times 10000)$) of ciphered image of Ref. [171].	211
Table 9.10	Succolarity values ($\ln(\text{Succolarity} \times 10000)$) of <i>Random noise</i> image.	211
Table 9.11	Succolarity values ($\ln(\text{Succolarity} \times 10000)$) of <i>Lena shuffled</i> image.	211

Table 9.12	Succolarity values ($\ln(\text{Succolarity} \times 10000)$) of <i>Boat shuffled</i> image.	211
Table 9.13	Succolarity values ($\ln(\text{Succolarity} \times 10000)$) of <i>Peppers shuffled</i> image.	213
Table 9.14	Mean succolarity values ($\ln(\text{Succolarity} \times 10000)$) of <i>Lena</i> cipher image.	215
Table 9.15	Mean succolarity values ($\ln(\text{Succolarity} \times 10000)$) of <i>Boat</i> cipher image.	216
Table 9.16	Mean succolarity values ($\ln(\text{Succolarity} \times 10000)$) of <i>Peppers</i> cipher image.	217
Table 9.17	Mean values of succolarity of three cipher images.	218

LIST OF FIGURES

		Page
Figure 2.1	Function.	8
Figure 2.2	A schematic view of an iterated function.	9
Figure 2.3	A schematic illustration of an unstable fixed point.	14
Figure 2.4	A schematic view of a stable fixed point.	14
Figure 2.5	A schematic view of a neutral fixed point.	14
Figure 2.6	Fixed points of $f(x) = x^2 - 1$.	16
Figure 2.7	Non-invertibility of the logistic map.	17
Figure 2.8	Generic bifurcations of one-dimensional maps.	23
Figure 2.9	Bifurcation diagram of the logistic map.	23
Figure 2.10	Schematic illustration of the exponential dependence on initial conditions.	25
Figure 2.11	Typical example of Rényi entropy $H_q(x)$ versus order q .	29
Figure 2.12	Mutual information.	30
Figure 2.13	Construction of the middle-third Cantor set.	39
Figure 2.14	A schematic view of 3D lacunarity based on Differential Box Counting method.	42
Figure 2.15	A $3 \times 3 \times 3$ gliding-box positions within a 4×4 image.	43
Figure 2.16	Succolarity for 1×1 box size.	46
Figure 3.1	The general cryptosystem.	63
Figure 3.2	Relationship between chaos and cryptography.	64
Figure 5.1	Bifurcation diagram, Lyapunov exponent and scale index of the logistic map.	86
Figure 5.1(a)	Bifurcation	86
Figure 5.1(b)	Lyapunov exponent	86

Figure 5.1(c)	scale index	86
Figure 5.2	Bifurcation diagram, Lyapunov exponent and scale index of the generalized logistic map.	87
Figure 5.2(a)	Bifurcation	87
Figure 5.2(b)	Lyapunov exponent	87
Figure 5.2(c)	scale index	87
Figure 5.3	Bifurcation diagram, Lyapunov exponent and scale index of the Hénon map with $b = 0.3$.	88
Figure 5.3(a)	Bifurcation	88
Figure 5.3(b)	Lyapunov exponent	88
Figure 5.3(c)	scale index	88
Figure 5.4	Bifurcation diagram, Lyapunov exponent and scale index of the Quantum map with $r=3.99$.	89
Figure 5.4(a)	Bifurcation	89
Figure 5.4(b)	Lyapunov exponent	89
Figure 5.4(c)	scale index	89
Figure 5.5	Bifurcation diagram, Lyapunov exponent and scale index of the synchronized chaotic map with $a_2 = 270$ and $\varepsilon = 0.24$.	90
Figure 5.5(a)	Bifurcation	90
Figure 5.5(b)	Lyapunov exponent	90
Figure 5.5(c)	scale index	90
Figure 5.6	Bifurcation diagram, Lyapunov exponent and scale index of the Rössler system with $a = 0.1$ and $b = 0.1$.	91
Figure 5.6(a)	Bifurcation	91
Figure 5.6(b)	Lyapunov exponent	91
Figure 5.6(c)	scale index	91
Figure 6.1	Bifurcation diagram of Eq. (6.4), while $N=2$.	101

Figure 6.2	Lyapunov exponents: Red line shows the variation of Lyapunov exponents of Eq. (6.4) in terms of the control parameter α , while blue line shows the variation of Lyapunov exponent of the logistic map in term of the control parameter.	102
Figure 6.3	Lyapunov exponents in synchronized state: $\Phi(x,x)$ (Eq. (B.9)) while $N=2$ and $\varepsilon = 0.1$ vs. α_1 and α_2 .	102
Figure 6.4	Bifurcation diagram (in synchronized sate) of $\Phi(x,x)$ (Eq. (B.9)) vs. a_1 while $N = 4$, $a_2= 270$ and $\varepsilon = 0.24$.	103
Figure 6.5	Block diagram of the proposed PRNG.	104
Figure 6.6	Bifurcation diagram of the quantum map for different control parameter (r).	114
Figure 6.6(a)	$r = 3.84$	114
Figure 6.6(b)	$r = 3.85$	114
Figure 6.6(c)	$r = 3.90$	114
Figure 6.6(d)	$r = 3.93$	114
Figure 6.6(e)	$r = 3.99$	114
Figure 6.7	Lyapunov exponent of the quantum map for different control parameter (r).	115
Figure 6.7(a)	$r = 3.84$	115
Figure 6.7(b)	$r = 3.85$	115
Figure 6.7(c)	$r = 3.90$	115
Figure 6.7(d)	$r = 3.93$	115
Figure 6.7(e)	$r = 3.99$	115
Figure 6.8	The scale index of the quantum map for control parameter $r = 3.99$.	116
Figure 6.9	Bifurcation diagrams and scale indices of the Hénon map and the Rössler system.	117
Figure 6.9(a)	$b = 0.3$	117
Figure 6.9(b)	$a = 0.1$ and $b = 0.1$	117
Figure 6.9(c)	$b = 0.3$	117
Figure 6.9(d)	$a = 0.1$ and $b = 0.1$	117

Figure 6.10	Normalized Shannon entropy (H_S) and intensive statistical complexity measure (C_I) for the proposed PRNG.	120
Figure 6.10(a)	Normalized Shannon entropy	120
Figure 6.10(b)	Statistical complexity	120
Figure 7.1	Block diagram of the proposed algorithm.	138
Figure 7.2	Boat plain image and corresponding ciphered image.	138
Figure 7.2(a)	Plain image	138
Figure 7.2(b)	Ciphered image.....	138
Figure 7.3	Statistical complexity: Blue line shows the variation of complexity of quantum logistic map in terms of the control parameter r , while Red line shows the variation of complexity of logistic map in terms of the control parameter.	140
Figure 7.4	The histogram: (a) Plain image. (b) Ciphered image.	141
Figure 7.4(a)	Plain image	141
Figure 7.4(b)	Ciphered image.....	141
Figure 7.5	Correlation coefficient of two adjacent pixels.	143
Figure 7.5(a)	Plain image	143
Figure 7.5(b)	Ciphered image.....	143
Figure 7.6	The effect of one bit change.	146
Figure 7.6(a)	Difference in plain image	146
Figure 7.6(b)	Difference in corresponding ciphered image	146
Figure 8.1	Mean-block entropy of the plain image <i>Peppers</i> at different block sizes.	153
Figure 8.1(a)	Block size: 20×20 ; Entropy= 5.6818	153
Figure 8.1(b)	Block size: 35×35 ; Entropy= 6.3264	153
Figure 8.1(c)	Block size: 50×50 ; Entropy= 6.6867	153
Figure 8.1(d)	Block size: 100×100 ; Entropy= 7.2501	153
Figure 8.2	<i>Boat</i> image, histogram and correlation of two horizontally, vertically and diagonally adjacent pixels in <i>House</i> image.	157

Figure 8.2(a)	<i>Boat</i> ; Entropy=7.0964	157
Figure 8.2(b)	Histogram.....	157
Figure 8.2(c)	Horizontally	157
Figure 8.2(d)	Vertically.....	157
Figure 8.2(e)	Diagonally	157
Figure 8.3	<i>Cipher</i> image of Chapter 7, histogram and correlation of two horizontally, vertically and diagonally adjacent pixels in <i>Cipher</i> image.	158
Figure 8.3(a)	<i>Cipher</i> : Chapter 7; Entropy=7.9974	158
Figure 8.3(b)	Histogram.....	158
Figure 8.3(c)	Horizontally	158
Figure 8.3(d)	Vertically.....	158
Figure 8.3(e)	Diagonally	158
Figure 8.4	<i>Pattern</i> image, histogram and correlation of two horizontally, vertically and diagonally adjacent pixels in <i>Pattern</i> image.	159
Figure 8.4(a)	<i>Pattern</i> ; Entropy=8.....	159
Figure 8.4(b)	Histogram.....	159
Figure 8.4(c)	Horizontally	159
Figure 8.4(d)	Vertically.....	159
Figure 8.4(e)	Diagonally	159
Figure 8.5	<i>Reference</i> image, histogram and correlation of two horizontally, vertically and diagonally adjacent pixels in <i>Reference</i> image.	160
Figure 8.5(a)	<i>Reference</i> ; Entropy=8	160
Figure 8.5(b)	Histogram.....	160
Figure 8.5(c)	Horizontally	160
Figure 8.5(d)	Vertically.....	160
Figure 8.5(e)	Diagonally	160

Figure 8.6	<i>Random noise</i> image, histogram and correlation of two horizontally, vertically and diagonally adjacent pixels in Random noise image.	161
Figure 8.6(a)	<i>Random noise</i> ; Entropy=7.3527	161
Figure 8.6(b)	Histogram.....	161
Figure 8.6(c)	Horizontally	161
Figure 8.6(d)	Vertically.....	161
Figure 8.6(e)	Diagonally	161
Figure 8.7	<i>Shuffled Boat</i> image, histogram and correlation of two horizontally, vertically and diagonally adjacent pixels in Boat Shuffled image.	162
Figure 8.7(a)	<i>Shuffled Boat</i> ; Entropy=7.0965	162
Figure 8.7(b)	Histogram.....	162
Figure 8.7(c)	Horizontally	162
Figure 8.7(d)	Vertically.....	162
Figure 8.7(e)	Diagonally	162
Figure 8.8	Rényi entropy of the sample images.	163
Figure 8.8(a)	<i>Boat</i> ; $H_{\infty}(X) = 5.5347$	163
Figure 8.8(b)	<i>Cipher: Chapter 7</i> ; $H_{\infty}(X) = 7.8163$	163
Figure 8.8(c)	<i>Pattern</i> ; $H_{\infty}(X) = 8$	163
Figure 8.8(d)	<i>Reference</i> ; $H_{\infty}(X) = 8$	163
Figure 8.8(e)	<i>Random noise</i> ; $H_{\infty}(X) = 5.7967$	163
Figure 8.8(f)	<i>Boat Shuffled</i> ; $H_{\infty}(X) = 5.5347$	163
Figure 8.9	The entropy growth curves of the sample images.	166
Figure 8.9(a)	<i>Boat</i>	166
Figure 8.9(b)	<i>Cipher: Chapter 7</i>	166
Figure 8.9(c)	<i>Pattern</i>	166
Figure 8.9(d)	<i>Reference</i>	166

Figure 8.9(e)	<i>Random noise</i>	166
Figure 8.9(f)	<i>Boat Shuffled</i>	166
Figure 8.10	Plain image <i>Lena</i> and corresponding ciphered images based on the algorithms in Table 8.3.	169
Figure 8.10(a)	Plain image: <i>Lena</i>	169
Figure 8.10(b)	Ciphered: Ref. [166]	169
Figure 8.10(c)	Ciphered: Ref. [164]	169
Figure 8.10(d)	Ciphered: Ref. [163]	169
Figure 8.10(e)	Ciphered: Ref. [168]	169
Figure 8.10(f)	Ciphered: Ref. [353]	169
Figure 8.10(g)	Ciphered: Ref. [171]	169
Figure 8.10(h)	Ciphered: Ref. [167]	169
Figure 8.10(i)	Ciphered: Ref. [169]	169
Figure 8.10(j)	Ciphered: Chapter 7	169
Figure 8.10(k)	Ciphered: Ref. [162]	169
Figure 8.10(l)	Ciphered: Ref. [332]	169
Figure 8.11	Plain image <i>Boat</i> and corresponding ciphered images based on the algorithms in Table 8.3.	170
Figure 8.11(a)	Plain image: <i>Boat</i>	170
Figure 8.11(b)	Ciphered: Ref. [166]	170
Figure 8.11(c)	Ciphered: Ref. [164]	170
Figure 8.11(d)	Ciphered: Ref. [163]	170
Figure 8.11(e)	Ciphered: Ref. [168]	170
Figure 8.11(f)	Ciphered: Ref. [353]	170
Figure 8.11(g)	Ciphered: Ref. [171]	170
Figure 8.11(h)	Ciphered: Ref. [167]	170
Figure 8.11(i)	Ciphered: Ref. [169]	170

Figure 8.11(j)	Ciphered: Chapter 7	170
Figure 8.11(k)	Ciphered: Ref. [162]	170
Figure 8.11(l)	Ciphered: Ref. [332]	170
Figure 8.12	Plain image <i>Peppers</i> and corresponding ciphered images based on the algorithms in Table 8.3.	171
Figure 8.12(a)	Plain image: Peppers	171
Figure 8.12(b)	Ciphered: Ref. [166]	171
Figure 8.12(c)	Ciphered: Ref. [164]	171
Figure 8.12(d)	Ciphered: Ref. [163]	171
Figure 8.12(e)	Ciphered: Ref. [168]	171
Figure 8.12(f)	Ciphered: Ref. [353]	171
Figure 8.12(g)	Ciphered: Ref. [171]	171
Figure 8.12(h)	Ciphered: Ref. [167]	171
Figure 8.12(i)	Ciphered: Ref. [169]	171
Figure 8.12(j)	Ciphered: Chapter 7	171
Figure 8.12(k)	Ciphered: Ref. [162]	171
Figure 8.12(l)	Ciphered: Ref. [332]	171
Figure 9.1	Two dimensional synthesized fBm images with various Hurst index	194
Figure 9.1(a)	Hurst Index= 0.1	194
Figure 9.1(b)	Hurst Index= 0.2	194
Figure 9.1(c)	Hurst Index= 0.3	194
Figure 9.1(d)	Hurst Index= 0.4	194
Figure 9.1(e)	Hurst Index= 0.5	194
Figure 9.1(f)	Hurst Index= 0.6	194
Figure 9.1(g)	Hurst Index= 0.7	194
Figure 9.1(h)	Hurst Index= 0.8	194

Figure 9.1(i)	Hurst Index= 0.9.....	194
Figure 9.2	Plain image <i>Lena</i> and corresponding ciphered images based on the algorithms in Table 9.1.	196
Figure 9.2(a)	Plain image: <i>Lena</i>	196
Figure 9.2(b)	Ciphered: Ref. [166]	196
Figure 9.2(c)	Ciphered: Ref. [164]	196
Figure 9.2(d)	Ciphered: Ref. [163]	196
Figure 9.2(e)	Ciphered: Ref. [168]	196
Figure 9.2(f)	Ciphered: Ref. [353]	196
Figure 9.2(g)	Ciphered: Ref. [171]	196
Figure 9.2(h)	Ciphered: Ref. [167]	196
Figure 9.2(i)	Ciphered: Ref. [169]	196
Figure 9.2(j)	Ciphered: Chapter 7	196
Figure 9.2(k)	Ciphered: Ref. [162]	196
Figure 9.2(l)	Ciphered: Ref. [332]	196
Figure 9.3	Plain image <i>Boat</i> and corresponding ciphered images based on the algorithms in Table 9.1.	197
Figure 9.3(a)	Plain image: <i>Boat</i>	197
Figure 9.3(b)	Ciphered: Ref. [166]	197
Figure 9.3(c)	Ciphered: Ref. [164]	197
Figure 9.3(d)	Ciphered: Ref. [163]	197
Figure 9.3(e)	Ciphered: Ref. [168]	197
Figure 9.3(f)	Ciphered: Ref. [353]	197
Figure 9.3(g)	Ciphered: Ref. [171]	197
Figure 9.3(h)	Ciphered: Ref. [167]	197
Figure 9.3(i)	Ciphered: Ref. [169]	197
Figure 9.3(j)	Ciphered: Chapter 7	197

Figure 9.3(k)	Ciphered: Ref. [162]	197
Figure 9.3(l)	Ciphered: Ref. [332]	197
Figure 9.4	Plain image <i>Peppers</i> and corresponding ciphered images based on the algorithms in Table 9.1.	198
Figure 9.4(a)	Plain image: Peppers	198
Figure 9.4(b)	Ciphered: Ref. [166]	198
Figure 9.4(c)	Ciphered: Ref. [164]	198
Figure 9.4(d)	Ciphered: Ref. [163]	198
Figure 9.4(e)	Ciphered: Ref. [168]	198
Figure 9.4(f)	Ciphered: Ref. [353]	198
Figure 9.4(g)	Ciphered: Ref. [171]	198
Figure 9.4(h)	Ciphered: Ref. [167]	198
Figure 9.4(i)	Ciphered: Ref. [169]	198
Figure 9.4(j)	Ciphered: Chapter 7	198
Figure 9.4(k)	Ciphered: Ref. [162]	198
Figure 9.4(l)	Ciphered: Ref. [332]	198
Figure 9.5	Images with Uniform and Normal distributions respectively: (a) Reference (U), (b) Pattern (U) and (c) Random noise (N).	199
Figure 9.5(a)	Reference	199
Figure 9.5(b)	Pattern.....	199
Figure 9.5(c)	Random noise	199
Figure 9.6	Lacunarity analysis of 2D synthesized <i>fBm</i> images with different Hurst index.	200
Figure 9.6(a)	Hurst Index= 0.4.....	200
Figure 9.6(b)	Hurst Index= 0.6.....	200
Figure 9.6(c)	Hurst Index= 0.7.....	200
Figure 9.6(d)	Hurst Index= 0.8.....	200
Figure 9.6(e)	Hurst Index= 0.9.....	200

Figure 9.7	Lacunarity analysis of the plain images.	204
Figure 9.7(a)	Lacunarity: Lena	204
Figure 9.7(b)	Lacunarity: Boat	204
Figure 9.7(c)	Lacunarity: Peppers	204
Figure 9.8	Lacunarity analysis of the Reference, Pattern and Random noise images.	205
Figure 9.8(a)	Lacunarity: Reference	205
Figure 9.8(b)	Lacunarity: Pattern	205
Figure 9.8(c)	Lacunarity: Random noise	205
Figure 9.9	Lacunarity analysis of cipher images of Chapter 7.	206
Figure 9.9(a)	Lacunarity: Lena ciphered image based on Chapter 7	206
Figure 9.9(b)	Lacunarity: Boat ciphered image based on Chapter 7	206
Figure 9.9(c)	Lacunarity: Peppers ciphered image based on Chapter 7	206
Figure 9.10	Lacunarity analysis of cipher images based on chaotic shuffling process.	207
Figure 9.10(a)	Lacunarity: Lena ciphered image	207
Figure 9.10(b)	Lacunarity: Boat ciphered image	207
Figure 9.10(c)	Lacunarity: Peppers ciphered image	207
Figure 9.11	Encrypted images based on chaotic shuffling process.	208
Figure 9.11(a)	Ciphered image: Lena.....	208
Figure 9.11(b)	Ciphered image: Boat.....	208
Figure 9.11(c)	Ciphered image: Peppers	208
Figure 9.12	Succolarity analysis of Boat plain image along four directions.	209
Figure 9.12(a)	Dir: Top to Bottm ($T2B$)	209
Figure 9.12(b)	Dir: Left to Right ($L2R$)	209
Figure 9.12(c)	Boat: Binary image	209
Figure 9.12(d)	Dir: Right to Left ($R2L$)	209

Figure 9.12(e) Dir: Bottom to Top (B2T)	209
Figure 9.13 Succolarity analysis of plain images along four directions.	212
Figure 9.13(a) Succolarity curves: Lena	212
Figure 9.13(b) Succolarity curves: Boat	212
Figure 9.13(c) Succolarity curves: Peppers	212
Figure 9.14 Succolarity analysis of ciphered image of Ref. [171] and Random noise images along four directions.	213
Figure 9.14(a) Succolarity curves: Ciphered image of Ref. [171]	213
Figure 9.14(b) Succolarity curves: Random noise image	213
Figure 9.15 Succolarity analysis of shuffled images along four directions.	214
Figure 9.15(a) Succolarity curves: Lena shuffled image	214
Figure 9.15(b) Succolarity curves: Boat shuffled image	214
Figure 9.15(c) Succolarity curves: Peppers shuffled image	214

LIST OF ABBREVIATIONS

AES: Advanced Encryption Standard

CWT: Continuous Wavelet Transform

DES: Data Encryption Standard

DWT: Discrete Wavelet Transform

FFT: Fast Fourier Transform

K-S entropy: Kolmogorov-Sinai entropy

MRA: Multiresolution Analysis

NIST: National Institute of Standards and Technology

NPCR: Number of Pixels Change Rate

PRNG: Pseudo Random Number Generator

QKD: Quantum Key Distribution

RSA: Rivest-Shamir-Adleman, Public key

SRB: Sinai Ruelle Bowen

TRNG: True Random Number Generator

UACI: Unified Average Changing Intensity

LIST OF SYMBOLS

$H(L)$: Block entropy

a^\dagger : Boson creation operator

D_b : Box-counting dimension

$T_N(x)$ Chebyshev polynomial type one

$U_N(x)$ Chebyshev polynomial type two

x^* : Complex conjugate

C : Complexity

ε : Coupling strength

β : Dissipation parameter

x^* : Fixed point

\mathcal{H} : Hilbert space

μ : Invariant measure

D_{JS} : Jensen-Shannon divergence

D_{KL} : Kullback-Leibler divergence

$\Lambda(r)$: Lacunarity

λ : Lyapunov exponent

ψ : Mother wavelet

$I(X;Y)$: Mutual Information

$\Phi_N(x,a)$: One-parameter families of chaotic maps

\hbar : Planck constant

$H_q(X)$: Rényi entropy

i_{scale} : Scale index

$\mathcal{S}(s)$: Scalogram

D : Self-similarity dimension

$H(X,p)$: Shannon entropy

$\sigma_{(dir,B)}$: Succolarity

D_T : Topological dimension

$Wf(u,s)$: Wavelet transform

KRIPTOGRAFI RAWAK KUANTUM: SATU PENDEKATAN BARU

ABSTRAK

Sejak 1990-an, sistem rawak dinamik digunakan secara meluas untuk mereka bentuk strategi baru bagi menyulitkan maklumat dalam bidang analog dan digital. Kini, banyak kriptosistem yang berasaskan rawak digital dicadangkan dan sebilangan daripada mereka dikriptanalisis. Fakta bahawa terdapat reka bentuk optimum dalam konteks kriptografi rawak tidak hanya memerlukan latar belakang yang kukuh dalam kriptografi, malahan juga melalui pengetahuan dinamik dan rawak yang tidak linear. Namun demikian, dalam reka bentuk kriptosistem rawak digital, terdapat dua isu penting yang tidak diberi perhatian yang serius oleh kebanyakan pereka bentuk sifer rawak digital. Pertama: mengelak pembinaan semula dinamik pada sistem rawak dan, kedua: ketidakberkalaan orbit rawak. Dua sumbangan utama kajian ini adalah respon terhadap permasalahan teori dan metodologi. Satu daripada penyelesaian bagi mengelak pembinaan semula orbit rawak adalah meningkatkan kekompleksan orbit. Dalam kajian ini, dua sistem dinamik baru, peta rawak kuantum dan gandingan disegerak dicadangkan dan diaplikasikan dalam dua bidang aplikasi utama, iaitu penjana nombor rawak pseudo dan medan penyulitan imej. Kedua-dua analisis teori dan eksperimen daripada kriptosistem yang dicadangkan dilaporkan dan dibincangkan. Di samping itu, dalam usaha mengkuantiti darjah ketidakberkalaan orbit rawak, pendekatan indeks skala sebagai kaedah matematik dicadangkan. Kaedah ini membolehkan pemilihan konfigurasi yang

mencukupi (pemilihan parameter optimum) daripada sistem dinamik untuk melaksanakan strategi kekeliruan dan pembauran maklumat. Analisis sekuriti kriptosistem berasaskan rawak adalah satu daripada aspek penting dalam kriptografi rawak. Begitu juga dengan pengukuran kerawakan dan kekompleksan ruang daripada imej sifer adalah dua tugas utama yang perlu diberi pertimbangan khusus. Setakat ini, pertama, kejituan ukuran entropi yang berbeza (sebagai satu ukuran kerawakan) seperti entropi Shannon, entropi Min dan entropi Renyi dikaji. Namun demikian, keputusan yang diperoleh tidak boleh dipercayai. Dalam kajian ini, pendekatan alternatif baru, entropi Mean-block dan lengkung pertumbuhan entropi dicadangkan bagi mengkuantiti kerawakan yang terdapat dalam imej sifer. Tambahan pula, dua ukuran fraktal, lakunariti dan sukolariti, dicadangkan untuk mengkuantiti kekompleksan ruang dalam imej sifer berasaskan rawak. Kerana dimensi fraktal sendirian tidak mencukupi untuk menjelaskan corak imej tersulit yang kompleks. Keputusan yang diperoleh menunjukkan bahawa entropi Mean-block lebih tepat daripada entropi Shannon, Min dan Renyi. Ditemui juga, perlakuan asimptotik bagi lengkung pertumbuhan entropi boleh dianggap sebagai penanda kerawakan. Tambahan pula, keputusan analisis lakunariti dan sukolariti dengan jelas menunjukkan bahawa proses penyulitan boleh mengakibatkan pemusnahan kesamaan-diri dan keterhubungan dalam kalangan piksel, masing-masing. Sebagai kesimpulan, disarankan digunakan kaedah matematik yang dicadangkan di samping ukuran kekompleksan bersandar skala, termasuk entropi Mean-block, lengkung pertumbuhan entropi dan ukuran fraktal untuk membimbing para penyelidik dalam merekabentuk dan melaksanakan kriptosistem yang baru.

QUANTUM CHAOTIC CRYPTOGRAPHY: A NEW APPROACH

ABSTRACT

Since 1990s chaotic dynamical systems have been widely used to design new strategies to encrypt information in analog and digital areas. Recently, many digital chaos-based cryptosystems are proposed and a number of them have been cryptanalyzed. The fact that an optimum designs in the context of chaotic cryptography not only demands a solid background in cryptography, but also a thorough knowledge of nonlinear dynamics and chaos. However, in the design of digital chaotic cryptosystems, there are two important issues that have not been seriously considered by most designers of digital chaotic ciphers. First, avoiding the reconstruction of the dynamics of the underlying chaotic systems and the second, non-periodicity of chaotic orbits. The two main contributions of this work are its responses to these two theoretical and methodological problems. In this way, one possible solution for avoiding the reconstruction of chaotic orbits is increasing the complexity of orbits. In this work, two new dynamical systems, quantum and synchronized coupled chaotic maps are proposed and applied in two main application fields, which are pseudo random number generator and image encryption fields. Both theoretical and experimental analysis of proposed cryptosystems are reported and discussed. In addition, in this work in order to quantify the degree of non-periodicity of chaotic orbits, the scale index approach as a mathematical tool is proposed. This method allows the selection of the adequate configurations (op-

timal parameter selection) of a dynamical system to implement strategies of confusion and diffusion of information. The security analysis of the chaos-based cryptosystems is one of the most important aspects in chaotic cryptography. In this sense, measuring the randomness and spatial complexity of cipher images are two important tasks that should be considered. To this end, first the accuracy of different entropy (as a measure of randomness) measures such as Shannon entropy, Min-entropy and Renyi entropy is examined. However, the results obtained are not reliable. In this work, new alternative approaches, the Mean-block entropy and entropy growth curve, are proposed for quantifying the presence randomness in the cipher images. Moreover, in this work two fractal measures, lacunarity and succolarity, are proposed to quantify spatial complexity in the chaos-based cipher images since the fractal dimension alone could not sufficiently explain the complex patterns of the encrypted images. The results obtained indicate that the mean-block entropy is more accurate than Shannon, Min and Renyi entropies. Also, the asymptotic behavior of entropy growth curve can be considered as a signature of randomness. Moreover, the results of lacunarity and succolarity analyses clearly show that the encryption process could lead to the destruction of self-similarity and connectivity among the pixels, respectively. As a conclusion, it can be strongly recommended to use the proposed mathematical tool and scale-dependent complexity measures including mean-block entropy, entropy growth curve and fractal measures, to guide researchers through designing and implementing of new cryptosystems.

CHAPTER 1

INTRODUCTION

1.1 Motivation of the Research

The Internet and communication systems have become an important component of information technology to provide connectivity at global and local scales, for the sharing of the different information. This leads to an explosive increase in transmission of messages containing useful information through different ways. It is no surprise then, in such transmission, implementing and keeping security and secrecy is a prerequisite to protect the information as well as the systems involved in transmission. Cryptography becomes necessary when higher security and privacy are specially required, especially when the message is transmitted over any untrusted medium, which includes any network, particularly, the Internet. The main objective of cryptography is to develop a cryptosystem, which keeps the transmission information secret and tamper-proof; protects information from unauthorized parties; prevents fraud; and ensures personal privacy. Therefore, in light of their important role, cryptosystems have become an indispensable part of modern information technology.

Beginning with the pioneer contribution of Lorenz [1], chaos theory has captured the interest of the scientific community. Chaos theory has been applied to model complex systems in the real world using rather simple mathematical models. In fact, chaos theory can be considered as a method to explain the complex processes in the real world.

Chaotic systems have several interesting features such as the ergodicity, randomness, non-periodicity and sensitive dependence on initial conditions [2, 3], which make them very attractive to the cryptographer. In fact, some researchers have pointed out that such significant properties can be connected with several cryptographic primitive characters such as "diffusion" and "confusion" required by modern cryptography ([4–6]. Interestingly, the idea of using chaos in cryptography is not novel and can be traced back to Shannon's classic paper titled "Communication Theory of Secrecy Systems" published in 1949 [7]. Of course, he could not use the phrase chaos; he just pointed out that the good mixing transformations, used in a good secrecy system, depend on their arguments in a "sensitive" way. The good mixing transformations can be considered as chaotic maps or equations bounded in limited phase space with positive Lyapunov exponents. In fact, from an algorithmic point of view, any good cryptosystem can be regarded as a chaotic or "pseudo-chaotic" system [8], since perfect cryptographic properties are ensured by pseudo-random disorder, generated from deterministic encryption operations, which is just like chaos generated from chaotic dynamical systems [9]. In Ref. [10], it has been shown that some conventional cryptosystems can present chaotic behavior. This definitely reveals that there exists a strong connection between chaos and cryptography, that's why it's a natural idea to make use of chaos and chaotic dynamical systems to enrich the design of new cryptosystems.

In the last few decades, the construction of chaos-based cryptosystems has attracted a great deal of attention, and plenty of chaotic cryptosystems have been developed, among which two main design paradigms for two different purposes can be found in literature: the discrete-time chaotic cryptosystem and the continuous time chaotic cryptosystem. Discrete-time chaotic cryptosystems, as the name suggest, is used to encrypt

the digital information by employing discrete-time chaotic dynamical systems. In this application, discrete-time chaotic systems are usually used as the pseudo-random bit generators, which serve as a one-time pad for encrypting the information. The use of discrete-time chaotic systems for the encryption purpose has been done for the first time by Matthews [11]. In his approach, a one-dimensional chaotic map, exhibiting chaotic behavior for a range of initial conditions and control parameters, has been utilized to generate a sequence of "pseudo-random numbers" in order to encrypt and decrypt the message. Shortly thereafter, in 1990, a cryptosystem based on a piecewise linear chaotic Tent map was developed by Habutsu with his colleague [12], where the parameter of the Tent map was used as a secret key, and the encryption and decryption were achieved by performing the inverse and forward iterations of the chaotic Tent map, respectively. A great number of discrete chaotic cryptographic algorithms have also been proposed in the recent years. However, a number of them are effectively attacked.

Continuous-time chaotic cryptosystems, on the other hand, aim mainly to use continuous-time chaotic dynamical systems to generate the broadband, non-periodic and noise-like chaotic signals for secure communications, where message signals, usually continuous signals, are hidden into the chaotic signal at the transmitter side, and recovered at the receiver side through the chaos synchronization technique. The idea of utilizing synchronous chaotic systems for secure communications was first discovered by Pecora and Carroll [13]. Although being demonstrated successfully in computer simulations and hardware implementation, the preliminary application of chaotic systems for the secure communications has a low level of security because an intruder can extract the hidden message signal from the transmission signal by using different

unmasking techniques [14, 15].

No doubt, there exists a strong relationship between the degree of randomness and quality of the cryptosystem. From the seminal contribution of Shannon [7, 16], Shannon entropy is employed as an indicator of randomness in cryptosystems. However, the results obtained are not completely true at least in chaos-based image encryption since the Shannon entropy measures the average information contents of the whole event source. In addition, the statistical complexity of the chaos-based encrypted images was studied, but spatial complexity has not been fully explored. Therefore, from the viewpoint of security, new dynamical systems and new approaches need to be explored.

1.2 Problem Statement

Security is the main problem of chaos-based cryptography. During last decade, according to data from ISI Web of Knowledge and Scopus more than 900 papers have been published. However, more than 30% of these papers are based on showing the weaknesses of other cryptosystems. Technically, the main problems are low key space and low performance. However, technical fixes to security problems typically have failed to address the root of the problems [17–22].

The fact that, fundamentally, cryptosystem designers are expert in cryptography and algorithms. But there is no solid knowledge about nonlinear dynamics and chaos. This lack of knowledge causes a few difficulties and problems such as: (i) extraction of dynamical properties of chaotic maps, (ii) selection of the proper chaotic map for cryptography, (iii) the design of new dynamical systems for chaotic cryptography purposes

and (iv) the suggestion of new methods for security analysis. The main contributions of this work are its responses to these four theoretical and methodological problems.

1.3 Objectives

The main objectives of this work were (i) to propose a mathematical tool to quantify the degree of non-periodicity of chaotic systems (scale index), (ii) to introduce new method and new dynamical system to enhance the security level of chaos-based cryptosystems and pseudo random number generators, (iii) to present new approaches to evaluate the security of chaos-based image cryptosystems more accurately.

The specific objectives of this study were:

- 1- To use the scale index for parameter selection and choosing the optimal values for keys and introducing the degree of non-periodicity as a fundamental concept in chaotic cryptography.
- 2- To propose two pseudo random number generators based on complete synchronization process and quantum map.
- 3- To propose an image encryption scheme based on quantum map.
- 4- To introduce the mean-block entropy and entropy growth curve to quantify the randomness of the chaos-based image encryption cryptosystems.
- 5- To introduce the lacunarity analysis to quantify the degree of heterogeneity and self-similarity of chaos-based encrypted images.
- 6- To introduce the succolarity analysis to characterize the degree of connectivity chaos-based cipher images.

1.4 Organization of the Thesis

This research was multidisciplinary and involved several different fields of research: nonlinear dynamics, chaos theory, quantum maps, cryptography, wavelets and complexity. The first portion of this dissertation provides a comprehensive overview of those fields of research. The second portion provides a detailed description of this research contribution:

Introducing mathematical tool for analyzing chaotic dynamical systems. As new perspectives on chaotic cryptography, designing two new cryptosystems, which are based on the synchronization scheme and quantum map. Introducing alternative approaches for security analysis of chaos-based cryptosystems.

A more comprehensive survey of dynamical systems and chaos by describing the definition, classification and characteristics of chaos and chaotic systems is presented in Chapter 2.

In Chapter 3, some basic principles of cryptography are introduced and the relationship between chaotic systems and modern cryptography is presented and two different kinds of chaotic cryptosystems are described. Also, the efficiency and applications of chaos-based cryptosystems are presented. A short introduction to wavelet analysis is provided in Chapter 4.

Non-periodicity analysis of discrete-time and continuous-time dynamical systems based on the *Scale Index* technique is presented in Chapter 5. In Chapter 6, two novel pseudo random number generators based on synchronized coupled chaotic map and quantum map are proposed. In Chapter 7, a novel image encryption algorithms based on quantum chaotic map is presented. In Chapter 8, the *Mean – block entropy* and *entropy growth curve* as two new entropy measures are introduced. Also, different en-

entropy measures such as mutual information, Kullback-Leibler divergence and Jensen-Shannon divergence are proposed for security analysis of chaos-based cryptosystems. In addition, comprehensive analysis of chaos-based image encryption algorithms based on different entropy measures is presented. In Chapter 9, Lacunarity and Succolarity, two relatively new measures from fractal geometry, are used for the analysis of chaos-based cipher images. Finally, conclusions are summarized in Chapter 10, and the future work is also described.

CHAPTER 2

DYNAMICAL SYSTEMS: FOUNDATIONS AND BASIC CONCEPTS

2.1 Functions

In mathematics, it is important to think of a function as an action or a process; a function takes a number as input, does something to it, and outputs a new number. This is illustrated in Figure 2.1. Here, the function is called f . There are a number of ways

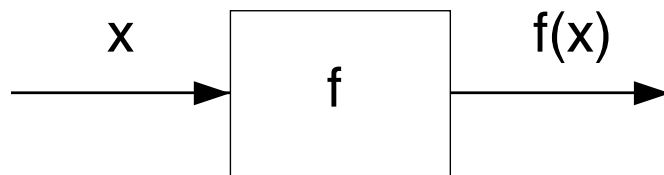


Figure 2.1: Function.

that to denote this symbolically. One way is as follows:

$$20 \xrightarrow{f} 160 \quad \text{and} \quad 2.7 \xrightarrow{f} 21.6.$$

Also, the function can be specified by algebra:

$$f(x) = 8x, \quad f(m) = 8m \quad \text{or} \quad f(s) = 8s.$$

In fact, the letter x (or m or s) is just a placeholder. A mathematical function is a rule that assigns an output value $f(x)$ to every input x . Another way to describe or specify a function is via a graph. A function is also sometimes referred to as a map. This terminology is common in mathematics, but less so in physics and other scientific fields.

2.1.1 Iterating a function

Iteration entails doing the same thing again and again using the previous step's output as the next step's input. This process is illustrated schematically in Figure 2.2. The output of the function is used as input for the next step. This can also be thought

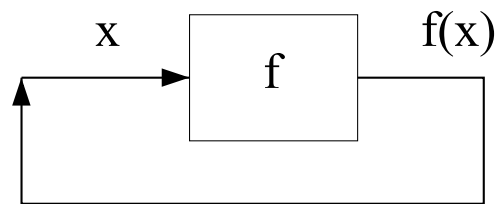


Figure 2.2: A schematic view of an iterated function.

of as a feedback process, in which output is used as input. Suppose the function is $f(x) = 4x$. Let us use 3 as an input. Then the function is applied and the result is $f(3) = 4 \times 3 = 12$. Then take 12, which is output, and use it as an input for the function to get $f(12) = 4 \times 12 = 48$. Then repeat the process:

$$3 \xrightarrow{f} 12 \xrightarrow{f} 48 \xrightarrow{f} 192 \dots$$

The number I start with, 3 in this particular case, is known as the *initial condition* or the *seed*.

The process of iterating can be demonstrated by making use of functional notation. When iterating, the first step is to apply the function, f , to the seed or initial condition x_0 to obtain x_1 : $x_1 = f(x_0)$. The next step is apply f to x_1 : $x_2 = f(x_1)$. Also these two equations can be combined as follows: $x_2 = f(x_1) = f(f(x_0))$. In general, for n application of f :

$$\overbrace{f(f(f(\dots f(x))))}^{n\text{-times}} = f^{(n)}(x).$$

It should be noted that, the expression $f^{(n)}(x)$ means f applied to x a total of n times. It does not mean $f(x)$ times itself n times. Iterating a function produces a sequence of numbers. A sequence is simply a list with an order to it. This sequence is often called the *orbit* or *trajectory*.

2.1.2 Phase space

A phase space is a geometric representation of the state variables of a system. The phase space is completely filled with trajectories, since each point can serve as an initial condition. Depending on the system, there can be any number of state variables. Thus, the phase space could consist of a line, a plane, three-dimensional space, or a higher-dimensional space. A phase space, for both discrete and continuous systems, is a set of all known possible states of that system, along with a rule for updating all of the states at each instant.

2.2 Dynamical Systems

A dynamical system is a function with an attitude. In principle, every dynamical system consists of two components: (i) a rule, which allows us to find a state at any positive time given an initial state; (ii) the space of states.

There are two main types of dynamical systems: *Flow* and *Map*. Flows are specified by differential equations. Similarly, maps are specified by difference equations. Dynamical systems generated by the iterative formulae belong to the category of dynamical systems with discrete-time. In contrast, the physical systems governed by differential equations are labeled as dynamical systems with continuous-time. In fact, time here either may be a continuous variable, or else it may be a discrete integer-valued variable.

An example of a dynamical system in which time (denoted t) is a continuous variable is a system of N first-order, ordinary differential equations (Flow):

$$\left\{ \begin{array}{l} \frac{dx^{(1)}}{dt} = F_1(x^{(1)}, x^{(2)}, x^{(3)}, \dots, x^{(N)}) \\ \frac{dx^{(2)}}{dt} = F_2(x^{(1)}, x^{(2)}, x^{(3)}, \dots, x^{(N)}) \\ \frac{dx^{(3)}}{dt} = F_3(x^{(1)}, x^{(2)}, x^{(3)}, \dots, x^{(N)}) \\ \vdots \\ \frac{dx^{(N)}}{dt} = F_N(x^{(1)}, x^{(2)}, x^{(3)}, \dots, x^{(N)}). \end{array} \right. \quad (2.1)$$

which can be written in vector form as:

$$\frac{dX(t)}{dt} = F[X(t)]. \quad (2.2)$$

where X is an N -dimensional vector. This is a dynamical system because, for any initial state of the system $x(0)$, I can in principle solve the equations to obtain the future system state $x(t)$ for $t > 0$.

2.2.1 Fixed point

By considering an example: the function $f(x) = x^2$. Let's choose a seed, 3, and find what happens under iteration:

$$3 \rightarrow 9 \rightarrow 81 \rightarrow 6561 \rightarrow 43046721 \rightarrow \dots$$

Obviously, the numbers are getting bigger. Indeed, this is the case for just about any seed greater than 1. So any seed larger than 1 will get bigger and bigger and the iterates go to infinity. This indicates that the iterates grow without bound; there is no restriction to how large the orbits become. If I square a number between 0 and 1, the number gets smaller. E.g.,

$$0.3 \rightarrow 0.09 \rightarrow 0.0081 \rightarrow 0.00006561 \rightarrow 0.0000000043046721 \rightarrow \dots$$

So, numbers between 0 and 1 get smaller and smaller, closer to zero. Zero squared is definitely zero. Therefore, if I iterate zero I do not go anywhere:

$$0 \rightarrow 0 \rightarrow 0 \rightarrow 0 \rightarrow 0 \rightarrow \dots$$

It is clear that 0 is a *fixed point* since it is unchanged by the function. Symbolically,

$f(0) = 0$. Also initial condition $x_0 = 1$ is a fixed point because 1 squared is 1: $f(1) = 1$.

A fixed point of a function f is an input x that yields the same output. Then, the equation for a fixed point is:

$$f(x^*) = x^*. \quad (2.3)$$

Note that, the symbol x^* is used to remind that Eq. (2.3) is not true in general. It is only true for some special values of x -namely, fixed points.

2.2.1.1 Classification of fixed point

In more general terms, understanding the fixed points of a dynamical system can tell us much about the global behavior of the system. Typically, a fixed point can be classified into one of the three categories: stable, marginally stable (neutral) and unstable.

1- *Unstable fixed point*: If x is somehow moved away from the fixed point, even a small perturbation, the orbit of this new x will move away from the fixed point and nearby orbits are repelled by it. So this type of fixed point is called a repeller (or repellor) and there are orbits (trajectories) which start near x^* and move far away from x^* .

2- *Stable fixed point*: If x is somehow moved away from the fixed point, a small perturbation will cause the orbit of new x to move back toward the fixed point. This type of a fixed point is also known as an attractor and all orbits (trajectories), which begin near x^* remain near, and converge to, x^* . Stable fixed points give excellent

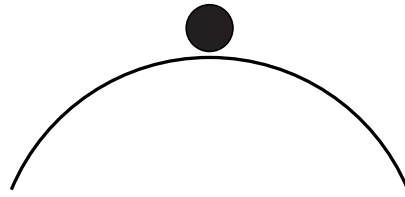


Figure 2.3: A schematic illustration of an unstable fixed point.

information about the fate of a dynamical system.

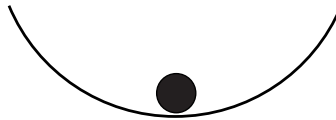


Figure 2.4: A schematic view of a stable fixed point.

3- *Neutral fixed point*: One could have a fixed point for which it is the case that if one moves away from the fixed point the resulting orbits neither move away from the fixed point (as a repeller) nor back toward the fixed point (as an attractor). The orbits which begin near x^* stay nearby but never converge to x^* . Such a fixed point is called neutral. The distinction between stable and unstable fixed points is an important one. In real systems or computer simulations, one does not expect to observe unstable fixed point, for the simple reason that unstable fixed points do not hang in there for long.



Figure 2.5: A schematic view of a neutral fixed point.

2.2.1.2 Finding fixed points and stability classification

1- Discrete-time dynamical systems:

Let x^* be a fixed point of the discrete-time dynamical system, $x(n+1) = f(x(n))$. If $|f'(x^*)| < 1$, then x^* is a stable fixed point. If $|f'(x^*)| > 1$, then x^* is an unstable fixed point.

Example: $f(x) = x^2$

To find the fixed points, $f(x^*) = x^*$ and solve for x^* . Thus $x_1^* = 0$ and $x_2^* = 1$. $f'(x) = 2x$.

Then

$f'(x_1^*) = 0$ and $f'(x_2^*) = 2$. Thus $x_1^* = 0$ is stable fixed point and $x_2^* = 1$ is an unstable fixed point.

2- Continuous-time dynamical systems:

Let x^* be a fixed point of the continuous-time dynamical system, $\dot{x} = f(x)$. If $f'(x^*) < 0$, then x^* is a stable fixed point. If $f'(x^*) > 0$, then x^* is an unstable fixed point.

Example: $\dot{x} = x^2 - 1$

To find the fixed points, $f(x^*) = 0$ and solve for x^* . Thus $x^* = \pm 1$. In order to determine the stability of $f(x) = x^2 - 1$, the function was plotted and vector field was sketched. The flow is to right where $x^2 - 1 > 0$ and the flow is to the left where $x^2 - 1 < 0$. Thus $x_1^* = -1$ is stable fixed point and $x_2^* = 1$ is an unstable fixed point.

2.3 Determinism and Randomness

An important distinction between dynamical systems surrounds whether the dynamics is completely deterministic, or whether the evolution proceeds as a result of

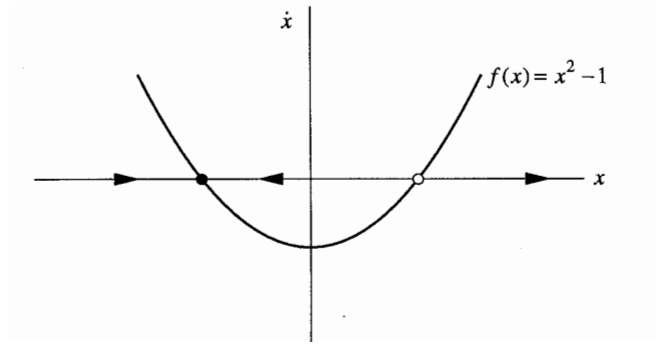


Figure 2.6: Fixed points of $f(x) = x^2 - 1$.

stochastic effects. A mathematical function is a rule that assigns an output value $f(x)$ to every input x . So the output depends on the input and the output is determined entirely by the input. Such a function is said to be deterministic, because the output is completely determined by the input.

A dynamical system is one whose state changes in time. If the changes are determined by specific rules, rather than being random, I say that the system is deterministic; otherwise it is stochastic. Dynamical systems can be stochastic, if there is a probability associated with the evolution of the movement between state spaces. For example, perhaps $h(x) = 2x$ with probability $1/2$, and $h(x) = x$ with probability $1/2$. So, if one used $x = 5$ as input, approximately half of the time one would get 10 as output, and approximately half of the time one would get 5. Clearly, the input does not completely determine the output.

For deterministic systems, for a given initial state x_t , then the state at some later time $x_{t+\delta t}$, is uniquely determined via the rule. This property implies that for deterministic systems, trajectories in phase space may never cross at finite time. But for stochastic systems only the probability $P(x_{t+\delta t})$ may be determined from the knowledge of x_t , and trajectories in phase space may cross.

2.4 Invertible and Non-invertible Dynamical Systems

The map F , is invertible if for a given state x_{n+1} there exists a unique x_n in such a way that $x_n = F^{-1}(x_{n+1})$, where F^{-1} is the inverse of F . Obviously, a map with an inverse is called invertible and a map without an inverse is called non-invertible. For example, consider the one-dimensional ($N = 1$) map:

$$x_{n+1} = rx_n(1 - x_n). \quad (2.4)$$

which is commonly called the logistic map.

As shown in Figure (2.7), this map is not invertible since for a given x_{n+1} there exist two possible values of x_n (except for the critical point at $x=0.5$).

$$x_n = \frac{r \pm \sqrt{r^2 - 4rx_{n+1}}}{2r}. \quad (2.5)$$

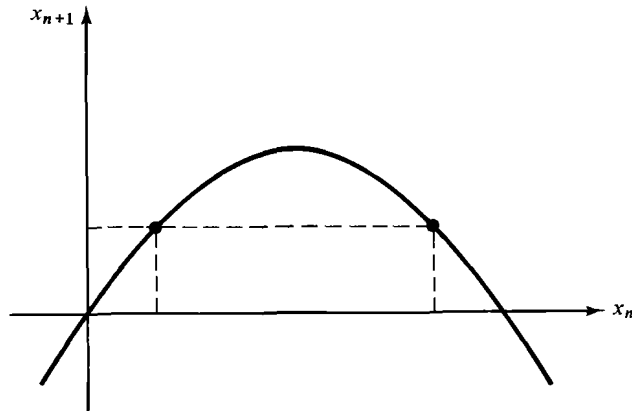


Figure 2.7: Non-invertibility of the logistic map.

If the map is invertible, then there can be no chaos unless $N \geq 2$. If the map is non-invertible, chaos is possible even in one-dimensional maps. Indeed, the logistic map as

a one-dimensional map (Eq. (2.4)) exhibits chaos for large enough control parameter (r). Note that, most of the maps I will deal with are non-invertible, meaning that their inverses are not existing.

2.5 Linear and Non-linear Systems

Linear models are preferable from a scientist's point of view as typically they are much more amenable to mathematical analysis. Nonlinear systems, in contrast, are much more difficult to analyze mathematically. A nonlinear system is a system whose time evolution equations are nonlinear; that is, the dynamical variables describing the properties of the system (for example, position, velocity, acceleration, pressure, etc.) appear in the equations in a nonlinear form. Typical nonlinear terms are products, powers, and functions of the x_i , such as x_1x_2 , x_1^3 or $\cos x$. The essential difference between linear and nonlinear systems is that linear systems can be broken down into parts. Then each part can be solved separately and finally recombined to get the answer. This idea allows a fantastic simplification of complex problems, and underlies such methods as normal modes, Laplace transforms, superposition arguments, and Fourier analysis. In this sense, a linear system is precisely equal to the sum of its parts. But many things in nature do not act this way. Whenever parts of a system interfere, or cooperate, or compete, there are nonlinear interactions going on.

2.6 Chaos

The nonscientific concept of chaos' is very old and is often associated with a physical state or human behavior without pattern and out of control. Chaos is a phenomenon encountered in science and mathematics wherein a deterministic (rule-based) system

behaves unpredictably. Some sudden and dramatic changes in nonlinear systems may give rise to the complex behavior called *chaos*. Chaos per se is really only one type of behavior exhibited by nonlinear systems. The phenomenon of chaos is usually considered to be part of the field of study known as nonlinear dynamics, an interdisciplinary area that lies mainly at the intersection of physics and mathematics, but also includes researchers from biology, economics, and elsewhere. It should be noted that nonlinearity is a necessary, but not a sufficient condition for the generation of chaotic motion. In fact, all chaotic systems are nonlinear but not all nonlinear systems are chaotic.

2.6.1 Definition of chaos

A dynamical system is chaotic if it possesses all of the following properties:

(1) The dynamical rule is deterministic.

In this case, the rule is just the function that iterates. A deterministic function is one where the input determines the output. The logistic map, along with all the other functions which have been working with, is deterministic, as discussed in Section 2.3.

(2) The orbits are aperiodic.

An orbit is aperiodic if it never repeats.

(3) The orbits are bounded.

In any event, for an orbit to be chaotic it must be bounded. This means that, the iterates usually do not fly off to infinity; they remain between an upper limit and a lower limit. For instance, these limits for logistic map are 1 and 0, respectively.

(4) The dynamical system has sensitive dependence on initial conditions.

This implies that even though chaotic systems are deterministic even the smallest difference in initial state can cause a huge difference in the end state. This is famously

described as the butterfly effect whereby the flapping of a butterfly's wings in one part of the world can eventually lead to a radical change in weather in another part.

In fact, once the systems have sensitive dependence on initial conditions, impossible to accurately predict for anything other than the short-term. In particular, the evolution of a chaotic system is utterly unpredictable in long-term. Note that, this unpredictability happens despite the fact that the equation governing the orbit is totally deterministic. For this reason, chaotic systems certainly are a deterministic source of randomness.

2.7 The Source of the Chaotic Behavior

Let me suppose that a system with random-like, complex behavior. One might try to explain this behavior by either an argument based on *complexity* or an argument based on *noise*. According to the complexity argument, the most of real systems are made of billions of molecules and atoms and since the behavior of all these molecules and atoms are not possible to be controlled precisely. Hence, these lack of control leads to fluctuations and randomness in the overall behavior of the system. On the other hand, the noise argument is that the complex behavior might be due to the influence of uncontrolled outside effects such as temperature fluctuations, electrical pickup or mechanical vibrations. From a more technical point of view, these complex systems have many degrees of freedom, and it is the activity of these many degrees of freedom that leads to the apparently random behavior. But the observed random-like behavior is neither due to external sources of noise nor to an infinite number of degrees of freedom nor to the uncertainty associated with quantum mechanics.

Considering the Lorenz system:

$$\begin{cases} \dot{X} = \sigma(Y - X) \\ \dot{Y} = -XZ + rX - Y \\ \dot{Z} = XY - bZ \end{cases} \quad (2.6)$$

As it can be seen, in this system, there isn't any noise, there are only three degrees of freedom and the system considered is purely classical. In fact, the actual source of irregularity is the property of the nonlinear system of separating initially close trajectories exponentially fast in a bounded region of phase space which is, three-dimensional for the Lorenz model. The crucial importance of chaos is that it provides an alternative explanation for this pseudo-randomness. It should be noted that, stochastic systems mimic many of the features of chaos, but they are not chaotic because chaos is a property of deterministic systems.

In the following, deterministic chaos denotes the irregular or chaotic motion that is generated by nonlinear systems:

Forced pendulum [23], Fluids near the onset of turbulence [24], Lasers [25], Nonlinear optical devices [26], Josephson junctions [27], Chemical reactions [28], Plasmas with interacting nonlinear waves [29] and Stimulated heart cells [30].

2.8 Quantifying Chaos

Two different, but related, types of description are used for quantitative characterization of chaos. The first type of quantifier emphasizes the *dynamics* (time dependence) of chaotic behavior. The *Lyapunov exponent* and various kinds of *entropy*,

are two examples of this type of descriptor. These quantifiers tell us how the system evolves in time and what happens to nearby trajectories as time goes on [3].

The second type of quantifier emphasizes the geometric nature of the trajectories in state space. The dynamical system is allowed to evolve for a reasonably long time, and then the geometry of the resulting trajectories in state space is examined. In this particular geometric method I will meet the important and interesting concept of *fractals*. These two types of description are complementary.

2.8.1 Bifurcation diagram

Bifurcation means a sudden qualitative change in the nature of a fixed point or orbit of a dynamical system, as a control parameter is varied. Obviously, the bifurcational phenomena play constructive role in the investigation of nonlinear dynamical systems. As a result of the qualitative content analysis of a dynamical system, it would be desirable to obtain the bifurcation diagram. A bifurcation diagram is a representation of an attractor on the vertical axis and plots a control parameter on the horizontal axis. The bifurcation diagram is able to classify all possible modes of behavior of the system and transitions between them as control parameter is varied continuously. There are actually three types of bifurcations in one-dimensional maps: the period doubling bifurcation, the tangent bifurcation, and the inverse period doubling bifurcation. These bifurcations are illustrated in Figure 2.8, where the control parameter (r) is taken as increasing to the right. Dashed lines are used for unstable orbits and solid lines for stable orbits.

The diagram in Figure 2.9 is bifurcation diagram of the logistic map as a period





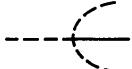
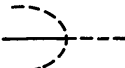
Type of bifurcation	Forward	Backward
Period doubling		
Tangent		
Inverse period doubling		

Figure 2.8: Generic bifurcations of one-dimensional maps.

doubling bifurcation. The figure is obtained by plotting, for various control parameter (r) values between $r = 3$ and $r = 4$ with high resolution. There appears to be some interesting structure in this region. It should be noted that, the diagram is obtained by discarding the first 1000 iterates to screen out transient effects. Since transients are often difficult to handle both computationally and experimentally, so that the discussion shall be confined to long-term behavior of the dynamical system. However, transients can give very useful information about the dynamics of the system.

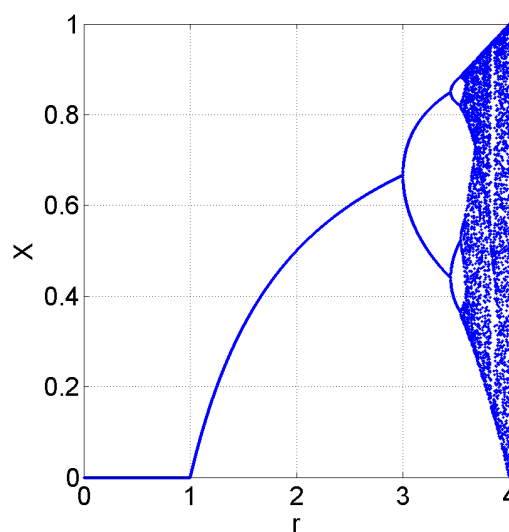


Figure 2.9: Bifurcation diagram of the logistic map.

2.8.2 Lyapunov exponent

Lyapunov was one of the first to explore dynamic stability and the Lyapunov exponent is named in honor of him as well. The main defining feature of chaos is the sensitive dependence on initial conditions. If a dynamical system has sensitive dependence on initial conditions, so that two orbits will eventually get far apart. However, there is no information about how fast they diverge. Let x_0 and y_0 denote two initial conditions that start off close together. So $d_0 = |x_0 - y_0|$ at $t = t_0$ is very small. Then for increasing time t (after t iterations) the orbits (trajectories) that start at these initial conditions diverge exponentially. It is schematically illustrated in Figure 2.10.

The dependence of the distance d between two trajectories at t , and their initial separation d_0 at $t = t_0$ as well, is assumed to be governed by the exponential function

$$d(t) = d_0(t_0)e^{\lambda t}. \quad (2.7)$$

Exponent denoted λ is an indicator of the sensitivity to initial conditions, and is referred to as Lyapunov exponent. It may be expressed in the form:

$$\lambda = \lim_{t \rightarrow \infty} \frac{1}{t} \ln \frac{d}{d_0}. \quad (2.8)$$

If the Lyapunov exponent (λ) is positive, on average the orbits are pushed apart, and the system has sensitive dependence on initial conditions (as shown in Figure 2.10). The larger λ is, the faster the orbits are pushed apart, and also the orbits are more unpredictable. If the Lyapunov exponent is negative, it means that the trajectories con-