DESIGNING NEW CHAOTIC AND HYPERCHAOTIC SYSTEMS FOR CHAOS-BASED CRYPTOGRAPHY

AL KARAWI HAYDER NATIQ KADHIM

IPM 2019 7

DESIGNING NEW CHAOTIC AND HYPERCHAOTIC SYSTEMS FOR CHAOS-BASED CRYPTOGRAPHY

By

AL KARAWI HAYDER NATIQ KADHIM

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

April 2019

DEDICATIONS

This study is dedicated to my parents, my wife and sons who have been our source of inspiration and gave us strength when I thought of giving up.

To my sisters, relatives, and friends who shared their words of advice and *encouragement to finish this study.*

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

DESIGNING NEW CHAOTIC AND HYPERCHAOTIC SYSTEMS FOR CHAOS-BASED CRYPTOGRAPHY

By

AL KARAWI HAYDER NATIQ KADHIM

April 2019

Chairman: Mohamad Rushdan Bin Md Said, PhD
Institute: Institute for Mathematical Research

The core of chaos-based cryptography is the selection of a good chaotic system. Most of chaotic ciphers have neglected the investigation of existence multistability in the employed chaotic systems. Meanwhile, many chaotic ciphers have applied chaotic systems with complex mathematical structure and limited chaotic behavior. Therefore, this thesis focuses on designing new chaotic and hyperchaotic systems with simple mathematical structure and complex dynamics, and discusses their performance in cryptographic applications. Furthermore, this thesis investigates the effect of existence multistability in the proposed systems from a cryptographic point of view.

In the beginning, this thesis presents a new 2D discrete hyperchaotic system. Dynamic characteristics of the 2D system are investigated from the following aspects: stability, trajectory, bifurcation diagram, Lyapunov exponents and sensitivity dependence. Moreover, the complexity performance of the system is evaluated by Sample Entropy algorithm. Simulation results show that the new system has a wide hyperchaotic range with high complexity and sensitivity dependence. To investigate its performance in terms of security, a new chaos-based image encryption algorithm is also proposed. In this algorithm, the essential requirements of confusion and diffusion are accomplished, and a stochastic sequence is used to enhance the security of encrypted image. Security analysis shows that the new algorithm has good security performance.

This thesis further proposed an M-dimension model as a methodological framework for producing new high-dimensional discrete hyperchaotic systems. Mathematical analysis demonstrates that the generated systems by this model have either no equilibria, or an arbitrarily large number of unstable equilibria. Moreover, numerical results show that the generated systems for certain values of parameters can produce two different behaviors: 1) single hyperchaotic attractor with high complexity and sensitivity dependence; and 2) coexistence of four attractors including single limit cycle, cluster of limit cycles, single hyperchaotic attractor, and cluster of hyperchaotic attractors, which is unusual behavior in discrete systems. However, we propose a simple feedback controller to change the chaos degradation in the multistability region from limit cycle to hyperchaotic behavior.

Additionally, this thesis presents a new 4D continuous chaotic system, which is derived from Lorenz-Haken equations. Dynamics analysis, including stability of symmetric equilibria and the existence of multiple Hopf bifurcations on these equilibria, are investigated, and the coexistence of two and three different attractors is numerically revealed. Moreover, a conducted research on the complexity of the new system reveals that the complexity of a system time series can locate the parameters and initial conditions that exhibit multistability behaviors. Besides that, randomness test results demonstrate that the generated pseudo-random sequences from the multistability regions fail to pass most of the statistical tests.

Finally, to choose valid pseudo-random sequences from multistability regions, this thesis constructs a new algorithm based on a new 3D multi-attribute chaotic system exhibiting extreme multistability behaviors. Unlike the existing algorithms, the proposed algorithm keeps the parameters constant with varying the initial conditions that show no non-chaotic behaviors. That means, the generated sequences are either chaotic or coexistence of chaotic attractors. Randomness test results show that the generated pseudo-random sequences by the new algorithm can pass all the statistical tests.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

PEREKABENTUKAN SISTEM HIPERKCELARU DAN CELARU BAHARU BAGI KRIPTOGRAFI BERDASARKAN KECELARUAN

Oleh

AL KARAWI HAYDER NATIQ KADHIM

April 2019

Pengerusi: Mohamad Rushdan bin Md Said, PhD
Institut : Institut Penyelidikan Matematik

Teras kriptografi berdasarkan kecelaruan adalah pada pemilihan sistem celaru yang baik. Kebanyakan sifer celaru telah mengabaikan penyiasatan mengenai kewujudan multistabil dalam sistem celaru yang digunakan. Manakala, kebanyakan sifer celaru telah mengaplikasikan sistem celaru dengan struktur matematik yang kompleks dan tingkah laku celaru yang terhad. Oleh sebab itu, tesis ini memfokuskan perekabentukan sistem hipercelaru dan celaru baharu dengan struktur matematik mudah dan dinamik kompleks, dan membincangkan prestasi mereka dalam aplikasi kriptografik. Di samping itu, tesis ini menyelidiki kesan kewujudan multistabil dalam sistem yang disyorkan dari sudut pandangan kriptografi.

Pada peringkat permulaan, tesis ini mempamerkan sebuah sistem hipercelaru diskret 2D baharu. Ciri-ciri dinamik sistem 2D disiasat dari aspek-aspek berikut: kestabilan, trajektori, gambarajah bifurkasi, eksponen Lyapunov dan kebersandaran kepekaan. Selain itu, prestasi kekompleksan sistem dinilai oleh algoritma Entropi Sampel. Dapatan simulasi menunjukkan bahawa ia mempunyai julat hipercelaru yang luas, kekompleksan tinggi dan kebersandaran kepekaan. Bagi meneliti prestasinya dari segi keselamatan, suatu algoritma penyulitan imej baharu berasas kecelaruan juga disyorkan. Dalam algoritma ini, keperluan utama kekeliruan dan resapan dicapai, dan jujukan stokastik digunakan untuk meningkatkan keselamatan imej yang disulitkan. Analisis keselamatan menunjukkan bahawa algoritma baharu mempunyai prestasi keselamatan yang baik.

Tesis ini seterusnya mengesyorkan sebuah model M-dimensi sebagai rangka kerja metodologi bagi menghasilkan sistem hipercelaru diskret berdimensi tinggi baharu. Analisis matematik menunjukkan bahawa sistem yang dijana oleh model ini tidak mempunyai keseimbangan, atau bilangan besar keseimbangan tidak stabil. Selain itu, keputusan berangka menunjukkan bahawa sistem yang dihasilkan untuk nilai-nilai parameter tertentu boleh menghasilkan dua kelakuan yang berbeza: 1) attraktor hypercelaru tunggal dengan kekompleksan yang tinggi dan kebersandaran kepekaan; dan 2) kewujudan bersama empat attraktor termasuk kitaran had tunggal, kelompok kitaran had, attraktor hypercelaru tunggal, dan kelompok attraktor hypercelaru, yang merupakan kelakuan yang tidak biasa dalam sistem diskret. Walau bagaimanapun, kami mencadangkan pengawal maklum balas yang mudah untuk mengubah kemerosotan celaru di rantau multistabil dari kitaran had ke tingkah laku hypercelaru.

Selain itu, tesis ini membentangkan sistem celaru 4D yang baru, yang diperolehi daripada persamaan Lorenz-Haken. Analisis dinamik, termasuk kestabilan keseimbangan simetri dan kewujudan pelbagai bifurkasi Hopf pada keseimbangan ini, diselidiki, dan kewujudan dua dan tiga attraktor berbeza adalah didedahkan secara numerik. Tambahan pula, penyelidikan yang dijalankan ke atas kekompleksan sistem baharu memperlihatkan kekompleksan siri masa sistem dapat mengesan parameter dan syarat awal yang memperlihatkan tingkah laku yang multistabil. Di samping itu, hasil ujian kerawakan menunjukkan bahawa jujukan pseudorawak yang dijana daripada medan multistabil gagal untuk lulus kebanyakan ujian statistik.

Akhir sekali, untuk memilih jujukan pseudo-rawak yang sah dari rantau multistabil, tesis ini membina algoritma baru berdasarkan sistem celaru multi-sifat 3D baru yang mempamerkan tingkah laku multistabil yang melampau. Tidak seperti algoritma yang sedia ada, algoritma yang disyorkan memastikan parameter tersebut malar dengan mempelbagaikan syarat awal yang menunjukkan tidak terdapatnya tingkah laku bukan celaru. Ini bermakna bahawa jujukan yang dijana sama ada celaru atau wujud sama pemikat celaru. Hasil ujian kecerapan menunjukkan bahawa jujukan pseudo-rawak yang dijana oleh algoritma baru boleh lulus semua ujian statistik.

ACKNOWLEDGEMENTS

Foremost, praise is to Allah for His blessing in completing this thesis. After an intensive period of three years, today is the day: writing this note of thanks is the finishing touch on my thesis. It has been a period of intense learning for me, not only in the scientific arena, but also on a personal level. Writing this thesis has had a big impact on me.

Firstly, I would like to deeply thank Assoc. Prof. Dr. Mohamad Rushdan bin Md Said for giving me the opportunity to pursue my PhD under his supervision on an interesting interdisciplinary topic that included chaos theory, and cryptography. This thesis would have not been possible without his continuous support and advice.

Besides my supervisor, I would like to thank the rest of my thesis committee: Assoc. Prof. Dr. Santo Banerjee for his never-ending guidance, insightful comments, understanding, patience and most importantly, his friendship. Moreover, my gratitude also goes to Prof. Nadia Mohammed, and Prof. Adem Kilicman, for words of encouragement, professional advices and valuable support in completing this thesis.

Last but not the least, I would like to thank my parents, Natiq and Samera, and my two sisters for their supports and prayers for me which have been the driving force that enabled me to finish this thesis. Special thanks go to my love and supportive wife, Rasha, and my two wonderful children, Taym and Aymen for their unending sacrifices. I believe that this journey would be impossible without their assistances.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Mohamad Rushdan bin Md Said, PhD
Assosiate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairperson)

Adem Kilicman, PhD
Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

Santo Banerjee, PhD
Research Fellow
Institute for Mathematical Research
Universiti Putra Malaysia
(Member)

Nadia Mohammed Ghanim Al-Saidi, PhD
Professor
Department of Applied Sciences
University of Technology Baghdad, Iraq
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature:____________________ Date:____________________

Name and Matric No: Al Karawi Hayder Natiq Kadhim, GS45312

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ________________________
Name of Chairman of Supervisory Committee
Assosiate Professor Dr. Mohamad Rushdan bin Md Said

Signature: ________________________
Name of Member of Supervisory Committee
Professor Dr. Adem Kilicman

Signature: ________________________
Name of Member of Supervisory Committee
Dr. Santo Banerjee

Signature: ________________________
Name of Member of Supervisory Committee
Professor Dr. Nadia Mohammed Ghanim Al-Saidi

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure | Page

LIST OF ABBREVIATIONS

1D	One-Dimensional
2D	Two-Dimensional
3D	Three-Dimensional
4D	Four-Dimensional
LE	Lyapunov Exponent
LLE	Largest lyapunov Exponent
IEA	Image Encryption Algorithm
2D-SLMM	Two-dimensional Sine Logistic Modulation Map
2D-LASM	Two-dimensional Logistic-Adjusted-Sine Map
2D-SIMM	Two-dimensional Sine ICMIC Modulation Map
ICMIC	Iterative Chaotic Map with Infinite Collapse
2D-SHAM	Two-dimensional Sine-Hénon Alteration Map
PRNG	Pseudo-Random Number Generator
SamEn	Sample Entropy
SD	Standard Deviation
SHAM-IEA	Sine-Hénon Alteration Map Based Image Encryption Algorithm
M-NHM	M-dimensional Nonlinear Hyperchaotic Model
MLEs	Maximum Lyapunov Exponents
MACS	Multi-Attribute Chaotic System

CHAPTER 1

INTRODUCTION

1.1 Background

Dynamics is the scientific study of changes in the time-evolution process and the corresponding system of equations is known as a dynamical system. The process of a dynamical system is deterministic if the whole future path of the system is uniquely determined by its initial conditions and parameters. Otherwise, the process is stochastic (Hirsch et al., 2012).

For the last two centuries, many studies have devoted their efforts to obtain the closed-form solutions of nonlinear dynamical systems. Unfortunately, the closed-form solution of nonlinear systems is very difficult to be obtained, except for a few particular cases (Layek, 2015). With the development of computer science, the numerical simulations (e.g. phase space, bifurcation diagrams, Lyapunov exponents, etc) have given a good understanding about the behavior of nonlinear dynamical systems.

During the last century, the endeavor to interpret the behavior of nonlinear dynamical systems led to observe that there exists an irregular (chaotic) dynamical system in nature. One of the most motivating examples of chaotic systems was given by the mathematician and meteorologist Lorenz (1963). In his study of weather-forecasting, he observed that the long-term weather has chaotic behavior and it is always unpredictable. Since then, chaotic behaviors have been observed in many natural and non-natural systems, and usually play a crucial role in the performance of systems (Ivancevic and Ivancevic, 2008).

The theory of chaos is one of the mathematical and physical frameworks focusing on the study of the behavior of deterministic nonlinear dynamical systems that have high sensitivity to initial conditions and parameters (Li and Yorke, 1975). Although chaotic systems are deterministic models, those systems have unpredictable solutions, and this is due to their high sensitivity dependence (Houtekamer and Zhang, 2016). Besides that, most of the chaotic systems have simple mathematical structure, but their time-series are really complex in terms of behavior.

The abundant characteristics of chaotic systems make them increasingly used as a mathematical model in various fields such as cryptography, physics and engineering (Strogatz, 2018). In particular, many researchers have observed that there is a strong relationship between cryptography and chaos, hence chaos-based cryptography can effectively guarantee the information security (Kocarev, 2001). Therefore, there is an immense interest to develop chaotic systems for cryptographic applications. Such applications are as image encryption, secure communications, and smart card encryption, etc.

1.2 Fundamentals of Dynamical Systems

A dynamical system provides a mathematical description of the evolution of a system along time. Hence, it can be used to determine the behavior of a system, which is particularly important, because it allows correcting the behavior of the system before it fails. Generally, existing dynamical systems are represented by either discrete-time or continuous-time process. The discrete dynamical systems are defined by difference equations, and those can be performed via iterative methods. While, the continuous dynamical systems are commonly described through ordinary differential equations.

1.2.1 Discrete Dynamical Systems

A time-evolution process of a nonlinear dynamical system can be described as discrete steps in time. Typically, a discrete system takes the current state as input and updates the situation by producing a new state as output. Therefore, a discrete dynamical system is represented mathematically by a map (difference equation), and the dynamics or flow of the discrete dynamical system is generated by the composition of the map (Li and Yorke, 1975).

Consider a map $f : \mathbb{R} \longrightarrow \mathbb{R}$ where $\mathbb{R}$ is the set of real numbers. Subsequently, the forward orbit of a point x_0 2 $\mathbb{R}$ is defined by

$$B(x_0) \quad \mathrm{f} x_0,\ f(x_0),\ f^2(x_0),\ f^3(x_0),\ \ldots \mathrm{g}, \tag{1.1}$$

where $f^2(x_0) \quad (f \circ f)(x_0)$, $f^3(x_0) \quad (f \circ f \circ f)(x_0)$, etc. Since all maps that we deal with have no continuous inverse (noninvertible), there is no need to mention backward orbit here.

1.2.1.1 Equilibrium (Fixed) Points

Equilibrium points (equilibria) are very important to analyze the local behavior of a dynamical system. An equilibrium point is also known as a fixed point or a critical point. A dynamical system may have no equilibrium point, one equilibrium point, finite number of equilibria, or infinite number of equilibria.

Definition 1.1 : (Grove and Ladas, 2004) A point x^* is called to be an equilibrium point of the map f if $f(x^*) \quad x^*$.

Consequently, to obtain all equilibria of the equation $y \quad f(x)$, one has to solve the equation $f(x) \quad x$. For example, the equilibria of square map $f(x) \quad x^2$ and cubic map $f(x) \quad x^3$ can be found by solving the equations $x^2 \quad x$ and $x^3 \quad x$, respectively. It is obvious that the former has two equilibria f$0, 1$g, whereas the latter has three equilibria $\{-1, 0, 1$g. Moreover, graphically speaking, an equilibrium point of a map f is a point where the curve $y \quad f(x)$ intersects the diagonal line $y \quad x$ (Elaydi, 2007).

1.2.1.2 The Notion of Stability in Discrete Systems

Studying the behavior of orbits near equilibria is considered as one of the main objectives in the theory of dynamical systems. Such an approach of investigation is known as stability theory. Different definitions were presented to analyze the stability of a dynamical system. Here, we study the notion of local stability of discrete dynamical systems.

Theorem 1.1 : Consider the 2D map $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, and let $X^* \quad \begin{pmatrix} x_1^* \\ x_2^* \end{pmatrix}$ be an equilibrium point of f. Then the following statements hold true:

1. If jλ_1j < 1 and jλ_2j < 1, then X^* is asymptotically stable.
2. If jλ_1j > 1 and jλ_2j > 1, then X^* is unstable source.
3. If jλ_1j < 1 and jλ_2j > 1 or jλ_1j > 1 and jλ_2j < 1, then X^* is unstable saddle.

where λ_1 and λ_2 are the zeros of the characteristic equation of the Jacobian matrix at the equilibrium point, which can be calculated by j$\lambda I - J_{X^*}$j.

Proof:
The above theorem is stated without proof; the interested reader can refer to (Elaydi, 2007). ■

Example 1.1 : *Consider the 2D Hénon map*

$$\begin{cases} x_{n \quad 1} \quad 1 - ax_n^2 \quad y_n, \\ y_{n \quad 1} \quad bx_n, \end{cases}$$

where a and b are real parameters with $|b| < 1$. *This map has two fixed points if* $a > -\frac{1}{4}(1-b)^2$. *These fixed points are*

$$\begin{cases} E_1^* = \left(\frac{1}{2a}(b-1+\sqrt{(1-b)^2+4a}), \frac{b}{2a}(b-1+\sqrt{(1-b)^2+4a})\right), \\ E_2^* = \left(\frac{1}{2a}(b-1-\sqrt{(1-b)^2+4a}), \frac{b}{2a}(b-1-\sqrt{(1-b)^2+4a})\right). \end{cases}$$

For $a = 0.2$ and $b = 0.3$, *the fixed points of the map are given by*

$$\begin{cases} E_1^* = (0.0436, 0.0131), \\ E_2^* = (-0.1836, -0.0551). \end{cases}$$

The corresponding Jacobian matrix at E_1^* is given by

$$J_{E_1^*} = \begin{pmatrix} -0.0174 & 1 \\ 0.3 & 0 \end{pmatrix}.$$

The characteristic equation of Jacobian matrix becomes

$$\lambda^2 + 0.0174\lambda - 0.3 = 0.$$

Consequently, the corresponding eigenvalues are

$$\lambda_{11} = 0.539, \quad \lambda_{12} = -0.556.$$

Obviously, E_1^* is asymptotically stable. By the same way, we can obtain the eigenvalues at E_2^*, which are given by

$$\lambda_{21} = 0.585, \quad \lambda_{22} = -0.512.$$

That means, E_2^* is also asymptotically stable.

For $a = 1.4$ and $b = 0.3$, *the fixed points of the map are given by*

$$\begin{cases} E_1^* = (1.2375, 0.3712), \\ E_2^* = (-2.2175, -0.6652). \end{cases}$$

the corresponding eigenvalues at E_1^* and E_2^* are given by

$$\lambda_{11} = 0.084, \quad \lambda_{12} = -3.549,$$
$$\lambda_{21} = 6.256, \quad \lambda_{22} = -0.047.$$

It is obvious that both fixed points are unstable saddle.

1.2.2 Continuous Dynamical Systems

The other important type of dynamical systems is essentially the limit of discrete systems with smaller and smaller updating times. Thus, the governing rule in that case becomes a set of differential equations as follows:

$$\frac{dx}{dt} \quad x \quad f(x,t), \qquad t \; \mathbf{2} \;\; t_{\mathbf{0}}, \mathbf{1} \quad , \tag{1.2}$$

where x $\quad x(t)$ **2** $\mathrm{I\!R}^{\mathrm{n}}$ is the vector representing the state of the system, and $f(x,t)$ is continuously differentiable function.

Definition 1.2 : (Wiggins, 2003) The continuous dynamical system (1.2) is said to be autonomous if the time variable t does not appear independently from the state vector; otherwise, the system is called non-autonomous.

For example, the following ordinary-differential equation

$$x \quad ax,$$

is autonomous because the time variable t does not explicitly appear. While, the forced damped pendulum equation

$$x \quad -ax - sin(x) \quad bsin(t),$$

is nonautonomous because t appears explicitly in the differential equation.

1.2.2.1 Equilibria of Autonomous Dynamical Systems

An equilibrium point of the autonomous dynamical system (1.2) is a solution x^* of the algebraic equation

$$f(x^*) \quad \mathbf{0}. \tag{1.3}$$

Remark 1.1 : Non-autonomous dynamical systems are beyond the scope of this thesis.

1.2.2.2 Stability Criteria in High-Dimensional Systems

We present here another important criterion of stability analysis of high-dimensional nonlinear dynamical systems, which is called Routh-Hurwitz criterion. This criterion is used to analyze the stability of both discrete and continuous systems by determining whether the zeros of their polynomial are all in the left half of the complex plane or not.

Theorem 1.2 : (Routh, 1877)
Consider the characteristic polynomial $P(\lambda) \quad \lambda^{\mathrm{M}} \quad a_1\lambda^{\mathrm{M}-1} \quad \cdots \quad a_{\mathrm{M}} \quad 0$ *with real coefficients* $\mathbf{f}\, a_{\mathrm{j}}\, \mathbf{g}_{\mathrm{j}}^{\mathrm{M}}\ {}_{1}$**. Let**

$$\Delta_1 \quad a_1, \qquad \Delta_2 \quad \begin{vmatrix} a_1 & a_3 \\ 1 & a_2 \end{vmatrix}, \ldots, \qquad \Delta_{\mathrm{k}} \quad \begin{vmatrix} a_1 & a_3 & a_5 & \ldots & a_{2\mathrm{k}-1} \\ 1 & a_2 & a_4 & \ldots & a_{2\mathrm{k}-2} \\ 0 & a_1 & a_3 & \ldots & a_{2\mathrm{k}-3} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & a_{\mathrm{k}} \end{vmatrix}.$$

Then the roots of the characteristic polynomial $P(\lambda)$ have negative real parts if and only if $\Delta_{\mathrm{k}} > 0$ for all $k \quad 1, 2, \ldots, M$.

Proof:
The above classical theorem is stated without proof; the interested reader can refer to the indicated reference for its proof. ■

Remark 1.2 : By stable manifold theorem (Robinson, 1998), a dynamical system is stable when all the zeros of the characteristic polynomial $P(\lambda)$ have negative real parts; otherwise, the system is unstable.

1.2.2.3 Stability in the Sense of Lyapunov

The autonomous dynamical system (1.2) at the equilibrium point x is said to be stable in the sense of Lyapunov (Layek, 2015), if for any $\epsilon > 0$ there exist $\delta > 0$, such that the orbit $\theta(t, x)$ of the system satisfies the following relation:

$$\mathrm{jj}x - x^*\mathrm{jj} < \delta \ ) \ \ \mathrm{jj}\theta(t, x) - x^*\mathrm{jj} < \epsilon, \quad 8\ t \geq 0. \tag{1.4}$$

Figure 1.1 (a) depicts the schematic diagram of the stability in the sense of Lyapunov. Additionally, the system (1.2) at the equilibrium point $x \quad x^*$ is said to be asymptotically stable, if it is stable in the sense of Lyapunov, and the system satisfies the following relation

$$\mathrm{jj}x - x^*\mathrm{jj} < \delta \ ) \ \ \mathrm{jj}\theta(t, x) - x^*|| \longrightarrow 0, \quad as\ t \longrightarrow \infty. \tag{1.5}$$

The asymptotic stability of an autonomous dynamical system is illustrated in Figure 1.1 (b).

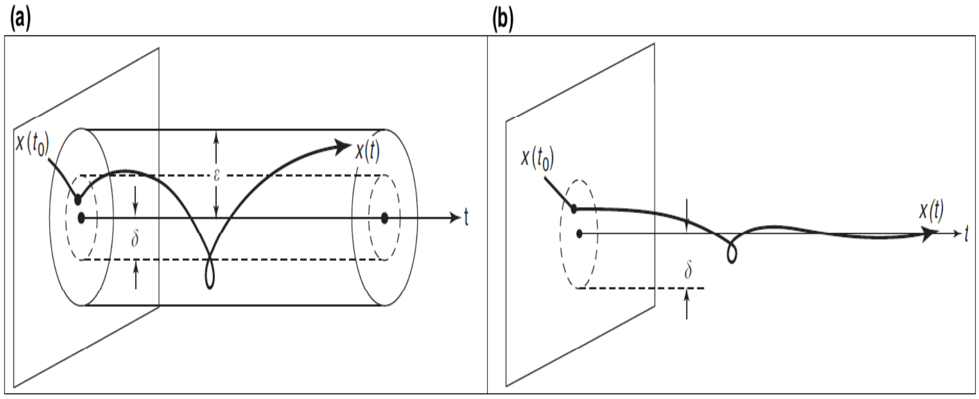

Figure 1.1: Schematic diagram of the stability of an autonomous dynamical system: (a) the stability in the sense of Lyapunov; (b) the asymptotic stability.

1.2.2.4 Conservative and Dissipative Continuous Dynamical Systems

The divergence of the vector field of the autonomous dynamical system (1.2) is defined by

$$\vec{\nabla} \cdot f \quad trace(\frac{\partial f}{\partial x}). \tag{1.6}$$

Thus, the system (1.2) is said to be conservative when its vector field divergence is zero. Meanwhile, if the vector field of the system (1.2) has negative divergence, then it is proven to be dissipative (Graham and Tél, 1984).

1.3 Chaos in Dynamical Systems

The study of what we call ”chaotic system” is due to Henri Poincaré when he was studying simplified solar systems of three bodies and concluded that the motions were sometimes incredibly complicated. Important further contributions were made by Lorenz (1963) when setting the new computer to calculate numerical solutions of a system of 12 differential equations that model a miniature atmosphere. He discovered that the weather is unpredictable, in which small changes in temperature at the poles or the equator will result in dramatic changes of the climate. The metaphor says ”the flapping of a butterfly’s wings in Brazil may cause a tornado in Texas several weeks latter” (Elaydi, 2007). This is called ”butterfly effect”. However, the expression ”chaos” became more popularized through the paper of Li and Yorke (1975), ”Period three implies chaos”.

Several definitions of chaos have been presented in the literature. Here, we adopt Devaney’s definition of chaos (Banks et al., 1992), which has three components:

the density of the set of periodic points, transitivity, and sensitivity dependence on initial conditions.

Definition 1.3 : Let I be an interval in $\mathbb{R}$. Then a set of periodic points B is called dense in I if for any x 2 I any open interval containing x must intersect B.

Example 1.2 (Elaydi, 2007): Consider the 1D Tent map

$$T \quad \begin{cases} 2x; & 0 \leq x \leq \frac{1}{2}, \\ 2(1-x); & \frac{1}{2} < x \leq 1. \end{cases}$$

To show that the set of periodic points of T is dense in the closed interval $0, 1$, *let us do some explanation. Recall that the fixed points of* T are x_1^* 0 and x_2^* $\frac{2}{3}$. Consider now the following rational numbers:

$$\begin{array}{lllll}
\frac{1}{3} & \frac{2}{3}; & & & \frac{1}{3}\ \textit{is eventually fixed.} \\
\frac{1}{4} & \frac{1}{2} & 1 & 0; & \frac{1}{4}\ \textit{is eventually fixed.} \\
\frac{3}{4} & \frac{1}{2} & 1 & 0; & \frac{3}{4}\ \textit{is eventually fixed.} \\
\frac{1}{5} & \frac{2}{5} & \frac{4}{5} & \frac{2}{5}; & \frac{1}{5}\ \textit{is eventually } 2-\textit{periodic.} \\
\frac{2}{5} & \frac{4}{5}; & & & \frac{2}{5}\ \textit{is of period } 2. \\
\frac{3}{5} & \frac{4}{5} & \frac{2}{5}; & & \frac{1}{4}\ \textit{is eventually } 2-\textit{periodic.} \\
\frac{4}{5} & \frac{2}{5}; & & & \frac{4}{5}\ \textit{is of period } 2.
\end{array}$$

Generally, all points of the form $\frac{\mathrm{r}}{2^{\mathrm{k}}}$ *are eventually fixed points. Furthermore,* points of the form $\frac{\mathrm{r}}{\mathrm{s}}$ with s odd are eventually periodic when r is also odd, and periodic if r is even. That means, the set of periodic points is dense.

Definition 1.4 : Let f be a map on an interval $\mathbb{R}$. Then f is said to be transitivity if for any pair of nonempty open intervals I_1 and I_2 in $\mathbb{R}$ there exists a positive integer k such that $f^{\mathrm{k}}(I_1)$ I_2 6 ϕ.

Definition 1.5 : A map of an interval I is said to possess sensitivity dependence on initial conditions if there exists $v > 0$ such that for any x_0 2 I and $\delta > 0$, there exists y_0 2 $(x_0 - \delta, x_0 \quad \delta)$ and a positive integer k such that

$$\mathrm{j}f^{\mathrm{k}}(x_0) - f^{\mathrm{k}}(y_0)| \geq v. \tag{1.7}$$

Example 1.3 (Elaydi, 2007): The doubling map $D :\ 0, 1 \qquad 0, 1$ *is defined as*

$$\begin{array}{lll} & 8 & \\ & 2x & \text{for } 0 \le x < \frac{1}{2}, \\ D(x) & 2x - 1 & \text{for } \frac{1}{2} \le x < 1, \\ & : \; 0 & \text{for } x \quad 1. \end{array}$$

To show that D has sensitive dependence on the initial conditions, let $I_1 \quad 0, \frac{1}{2})$ and $I_2 \quad \frac{1}{2}, 1)$. For any two points $x, y\ 2\ \ 0, 1)$, either (i) $x, y\ 2\ I$ or (ii) $x\ 2\ I_1,\ y\ 2\ I_2$.

Case (i): If $x, y\ 2\ I_1$, then $\mathrm{j}\, D(x) - D(y)\, \mathrm{j}\quad \mathrm{j}\, 2x - 2y\, \mathrm{j}\quad 2\,\mathrm{j}\, x - y\, \mathrm{j}$ on the other hand if $x, y\ 2\ I_2$, then $\mathrm{j}\, D(x) - D(y)\, \mathrm{j}\quad \mathrm{j}\, 2x - 1 - 2y\quad 1\, \mathrm{j}\quad 2\,\mathrm{j}\, x - y\, \mathrm{j}$.

Case (ii): Suppose now that $x\ 2\ I_1$ and $y\ 2\ I_2$. Then $\mathrm{j}\ D(x) - D(y)\ \mathrm{j}\quad \mathrm{j}\ 2x - 2y\quad 1\, | \ge 1 - 2\,\mathrm{j}\, x - y\, \mathrm{j}$. Note that if $\mathrm{j}\, x - y\, \mathrm{j} < \frac{1}{4}$, then $-2\,\mathrm{j}\, x - y\, \mathrm{j} > -\frac{1}{2}$. Hence

$$\mathrm{j}\, D(x) - D(y)\, | \ge 1 - \frac{1}{2} \quad \frac{1}{2}.$$

Select $v \quad \frac{1}{4}$ where v is the sensitivity constant of D. If $x_0\ 2\ I$ and $\delta > 0$, we pick any point $y_0\ 2\ (x_0 - \delta, x_0 \quad \delta)$. If $x_0, y_0\ 2\ I_1$ or I_2, then the distance between $x_{\mathrm{j}} \quad D^{\mathrm{j}}(x_0)$ and $y_{\mathrm{k}} \quad D^{\mathrm{k}}(y_0)$ will at least double the distance between $y_{\mathrm{k}-1}$ and $x_{\mathrm{k}-1}$. Hence

$$\begin{aligned} \mathrm{j}\, y_{\mathrm{k}} - x_{\mathrm{k}}\, | &\ge 2\,\mathrm{j}\, y_{\mathrm{k}-1} - x_{\mathrm{k}-1}\, \mathrm{j} \\ &\ge 2^{\mathrm{k}}\, \mathrm{j}\, y_0 - x_0\, \mathrm{j}\, . \end{aligned}$$

Hence, eventually $\mathrm{j}\, x_{\mathrm{j}} - y_{\mathrm{j}}\, | \ge \frac{1}{4} \quad v$ for some positive integer j. On the other hand if $x_0\ 2\ I_1$ and $y_0\ 2\ I_2$ and $\mathrm{j}\ x_0 - y_0\ \mathrm{j} < \frac{1}{4}$, then $\mathrm{j}\ D(x_0) - D(y_0)\ \mathrm{j} > \frac{1}{4} \quad v$. Finally, if $x_0 \quad 0$ or $x_0 \quad 1$, the above argument will carry over in a straightforward manner.

Now, according to the above three components, Devaney's definition of chaos can be defined as

Definition 1.6 : A map $f : I \longrightarrow I$, where I is an interval, is called chaotic if:

1. f is transitive;
2. The set of periodic points is dense in I;
3. f has sensitivity dependence on initial conditions.

1.3.1 Features of Chaotic Motion

Chaotic systems have many striking features that make them different from linear systems and other nonlinear systems (Lorenz, 1963). Among the main characteristics of chaotic systems are the following :

1. **Boundedness:** the movement of a chaotic orbit is always limited to a specific region, which is known as the chaotic domain;

2. **Randomness:** Under certain parameters, the state of a chaotic system may change in a qualitative way from chaotic to periodic and vice versa.

3. **Long-term unpredictability:** Since chaotic systems are very sensitive to initial conditions, so small change in initial conditions could make enormous consequences in the future, which means that it is impossible to predict long-term behavior of a chaotic system;

1.3.2 Lyapunov Exponent

Lyapunov Exponent (LE) was presented by Lyapunov (1992) when studying the stability of solutions of ordinary differential equations. However, the Lyapunov Exponent $\lambda(x)$ at a point x measures the average loss of information during iterates of points near x or the growth in error per iteration.

Over the last four decades, LE plays a crucial role in the study of the behaviors of nonlinear dynamical systems through determining whether a nonlinear system is chaotic or not (Rozenbaum et al., 2017). In general, a dynamical system is chaotic when it has one positive value of LE and if it has more than one, then it is proved to be hyperchaotic (Wolf et al., 1985). Meanwhile, a dynamical system is non-chaotic when its LE values are non-positive. However, the Poincaré-Bendixson theorem (Hirsch et al., 2012) requires that continuous dynamical systems be at least 3D to have chaotic solutions, whereas, discrete dynamical systems can have chaotic solutions with only 1D.

The QR decomposition algorithm (Hubertus et al., 1997) is widely used numerical scheme for computing the LE of discrete and continuous dynamical systems. The process of QR decomposition algorithm, when J represents the Jacobian matrix of the system, is given by

$$\begin{aligned} qr\; J_M J_{M-1}\cdots J_1 \quad & qr\; J_M J_{M-1}\cdots J_2(J_1Q_0)\\ & qr\; J_M J_{M-1}\cdots J_3(J_2Q_1)\;\; R_1 \\ & qr\; J_M J_{M-1}\cdots J_i(J_{i-1}Q_{i-2})\;\; R_{i-1}\cdots R_1\\ & \cdots \\ & Q_M\; R_M\cdots R_2R_1 \quad\; Q_MR\end{aligned}$$

where qr · is the QR decomposition function. Thus, the LEs can be obtained by

$$LE \quad \frac{1}{N}\overset{N}{\mathbf{X}}_{i\;\;1} \ln \mathrm{j}\, R_i(v,v)\,\mathrm{j} \tag{1.8}$$

where v $1, 2, \ldots$ and N is the iteration number.

1.3.3 Bifurcation Diagram

Generally, the bifurcation diagram is used to demonstrate the behavior of a dynamical system when its parameter varying (Hale and Koçak, 1991). The horizontal axis of the bifurcation diagram represents the parameter of a dynamical system, meanwhile, the vertical axis describes the system behavior near fixed points. As an example, consider the 1D map as follows

$$F(x_0) : R \times R \longrightarrow R, \tag{1.9}$$

where x_0 2 R is an initial value, and ω 2 R is a parameter. Then, the corresponding computer-generated bifurcation diagram can be depicted by Elaydi (2007) procedure as follows

1. Select a specific initial value x_0 to generate a high iterate orbit as follows $x_0,\ F\ \ (x_0),\ F^2(x_0),\ \ldots,\ F^{400}(x_0),\ F^{401}(x_0),\ \ldots,\ F^{500}(x_0)$.
2. Neglect the iterations from x_0 to $F^{400}(x_0)$, and then depict the iterations from $F^{401}(x_0)$ to $F^{500}(x_0)$ in the bifurcation diagram.
3. Repeat the above two steps for various values of the parameter ω.

However, we will discuss the bifurcation diagram of the 1D logistic map in more detail later on in Section 2.2.1.

1.4 Cryptography

Cryptography is essentially the study of mathematical techniques that protect information by transforming it into a secure format. For the time being, modern communication technologies, especially, the Internet and mobile phone applications, have transmitted numerous kinds of digital data over wireless networks. With this rapid development, there is a growing demand for cryptographic applications to secure the transmitted multimedia contents (e.g. audios, images, videos) over the Internet and mobile-phone networks (Alvarez and Li, 2006).

The development of cryptography can be classified into two parts: traditional cryptography and modern cryptography. The former is quite simple, in which it is easy to encrypt and decrypt the information manually or mechanically because traditional techniques used individual letters in the encrypted text. The latter, which is founded by Shannon (1949), is more complicated, and its foundation is based on various disciplines including mathematics, computer science and electrical engineering.

1.4.1 Cryptographic System

From the mathematical point of view, the cryptosystem is a five-tuple defined as follows:

1. P is a finite set of possible plaintexts;

2. C is a finite set of possible ciphertexts;

3. K is a finite set of possible keys;

4. For each e 2 K, there is $E_{\mathrm{e}} : P \longrightarrow C$ that uniquely determines a bijection between P and C, which is called the encryption function;

5. For each d 2 K, there is $D_{\mathrm{d}} : C \longrightarrow P$ that uniquely determines a bijection between C and P, which is called the decryption function.

However, in the following we provide the basic terminology related to cryptographic system (Stallings, 2006):

- Plaintext is ordinary readable information that we need to encrypt it, which can be in a form of numerical data, characters, pictures, or any other kind of information. On the other hand, ciphertext is the information that has been encrypted by an encryption scheme (cipher), and it is usually unclear and nobody can understand it, except the recipients. Consequently, the encryption process is a mechanism of converting readable data to something that appears to be random and meaningless using a secret key. Meanwhile, recovering the readable data from senseless data using a secret key is called decryption process.

- Secret Key in cryptographic system is a variable that can be used in encryption and decryption processes. The secret key plays a crucial role in both symmetric and asymmetric cryptography. Security of the modern cryptography are depended on the key only (Kerckhoffs principle). Kerckhkey principle was stated by Auguste (1883): "cryptographic system should be a secure even if everything about the system, except the key, is public knowledge", (Tang et al., 2016).

- Symmetric encryption refers to the process of converting plaintext into ciphertext and vice versa using the same secret key. On the other hand, asymmetric encryption refers to the process of converting plaintext into ciphertext and vice versa using different secret keys.

- Cryptographic schemes can be divided into two types: block and stream ciphers. The block cipher is a function that maps n-bit plaintext blocks to n-bit ciphertext blocks, where n is the block-length. Each n-block encrypts (decrypts) independently from another one. In the contrast, the stream cipher process the plaintext in the much smaller blocks (up to a single bit) and the function of encryption may vary as plaintext is processed.

- Cryptanalysis includes the techniques and principles of decoding without knowing the secret key, generally this leads to obtain and estimate the secrete key. In fact, it is complicated procedure involving mathematical tools, statistical analysis, and analytical reasoning. Chosen plain-text attack is one of cryptanalysis technique, in which opponent aims to find the secret key by temporary accessing to the encryption machinery, subsequently he can choose some plaintexts and get the corresponding ciphertexts. Meanwhile, the opponent in the chosen cipher-text attack tries to find the secret key by choosing some ciphertexts and get the corresponding plaintexts. Besides that, differential attack is another form of cryptanalysis applicable primarily to study how differences in information input can affect the resultant difference at the output.

1.4.2 Chaos-Based Cryptography

One of the interesting applications of chaos is in the field of cryptography. The concept of using chaotic systems in cryptography can be traced back to the paper of Shannon (1949) entitled "Communication Theory of Secrecy Systems". In this paper, he wrote "Good mixing transformations are often formed by repeated products of two simple non-commuting operations. Hopf has shown, for example, that pastry dough can be mixed by such a sequence of operations. The dough is first rolled out into a thin slab, then folded over, then rolled, and then folded again, etc". That means, good mixing transformations in good secrecy systems are achieved by basic operations, and this is the heart of chaotic maps (Alvarez and Li, 2006).

Table 1.1: Analogy between chaos and cryptography properties (Alvarez and Li, 2006).

Chaotic property	Cryptographic property	Description
Ergodicity	Confusion	The output has the same distribution for any input
Sensitivity to initial conditions control parameter	Diffusion with tiny change in the plaintext secret key	A small deviation in the input can cause a large change at the output
Mixing property (topological transitivity)	Diffusion with tiny change in one plainblock of the whole plaintext	A small deviation in the local area can cause a large change in the whole space
Deterministic dynamics	Deterministic pseudo-randomness	A deterministic process can cause a random-like (pseudo-random) behavior
Structure complexity	Algorithm complexity	A simple process has a very high complexity

More interestingly, Shannon s paper presented the most fundamental concepts of cryptographic properties, namely ”confusion” and ”diffusion”. The former property is aimed to create the strong relationship between the key and the ciphertext as much as possible, hence disappointing endeavors to study the ciphertext looking for redundancies and statistical patterns. The latter property indicates to reordering the bits in the message, which means that the influence of individual plaintext or key bits is spread out over as much of the ciphertext as possible. However, the more detailed research in this field was started later on together with the development of the modern theory of computer science and chaos.

Since 1990s, many studies have emphasized that there exists a strong relationship between chaos and cryptography, in which numerous characteristics of cryptographic systems including confusion, and diffusion can be connected to their corresponding counterparts in chaotic systems, such as the ergodicity, mixing property (topological transitivity) and the sensitivity to initial conditions (Matthews, 1989; Wheeler and Matthews, 1991; Brown and Chua, 1996; Gotz et al., 1997; Fridrich, 1998). Table 1.1 illustrates the analogy between chaos theory and cryptography.

1.4.3 Image Encryption Using Chaotic Systems

In recent years, encryption of images has received much attention in the researches of information security and a lot of image encryption algorithms have

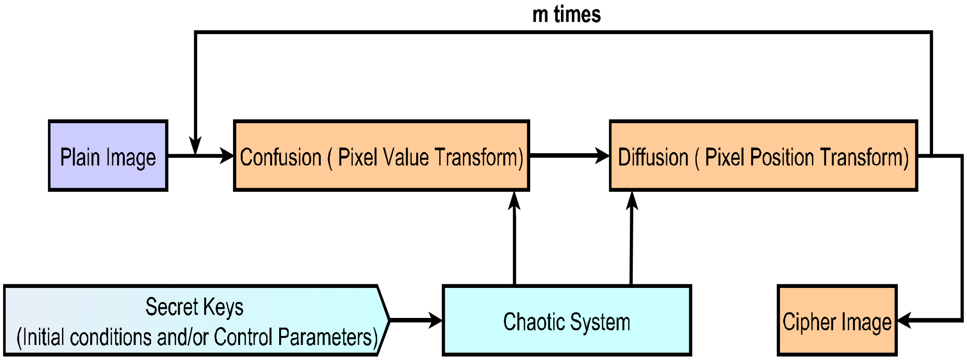
m times
Plain Image
Confusion (Pixel Value Transform)
Diffusion (Pixel Position Transform)
Secret Keys
(Initial conditions and/or Control Parameters)
Chaotic System
Cipher Image

Figure 1.2: Typical Architecture of Chaos-Based Image Encryption.

been proposed to meet the demand for real-time secure image transmission over the Internet and through wireless networks. Due to some inherent features of images such as high correlation among pixels and bulk data capacity, the encryption of image is different from that of text. Therefore, traditional cryptographic techniques such as DES, IDES and RSA are no longer appropriate for image encryption (Chen et al., 2004; Zhang and Xiao, 2014).

Among all image encryption schemes that have been proposed using different kinds of techniques, chaos encryption algorithms have shown some exceptionally good properties in many concerned aspects regarding security, complexity, speed, computing power and computational overhead, etc. A structural design of prevailing chaos-based image encryption is presented in Figure 1.2. As can be observed, a chaotic system generates a pseudo-random sequence, which is governed by initial conditions and or parameters (secret key). Meanwhile, the chaotic image encryption algorithm includes two significant operations: pixel value transform and pixel position transform. In image pixel value transform, the generated pseudo-random sequence performs certain operation with plaintext, which results in cipher text. In pixel coordinate transform, however, image pixel coordinate is changed by a chaotic matrix, which is also built from the generated pseudo-random sequence.

1.5 Motivations and Problem Statement

Chaos theory has established itself as an important branch of modern mathematics and physics with a broad range of applications in different areas of biology and engineering. The future behavior of chaotic systems is totally determined by its control parameters and initial conditions, which means that any arbitrarily small change in a control parameter or an initial value can produce a totally different orbit. Besides that, chaotic systems have many others properties, such as generating one or more pseudo random sequences, and long-term prediction of its behaviors is impossible. With these significant features, chaotic systems can be considered as ideal nonlinear mathematical models for cryptography and communications.

Due to their simple structure, complex dynamics, and low-implementation-cost, one-dimensional (1D) discrete chaotic systems, including Logistic, Tent, Sine, Gaussian, and Chebyshev maps, have become very popular mathematical tools in cryptographic applications. However, applying 1D chaotic maps in different disciplines of cryptography has revealed that these maps have performance limitations in different aspects. First, with the rapid development of chaos technologies, it is found that the chaotic sequences of existing 1D chaotic maps can be estimated by identifying their initial states (Arroyo et al., 2008, 2011). Moreover, many existing 1D chaotic maps have frail chaos. Frail chaos means that the chaotic map exhibits chaotic behaviors only in limited regions of its parameters and initial conditions (Zeraoulia, 2012). Consequently, the space of secret keys in chaos-based cryptosystems will also be limited, since these keys are usually constructed from the parameters and initial values.

Therefore, many studies have devoted their efforts to developing new discrete dynamical systems with robust chaotic behaviors. The effective studies can be classified into two categories: designing new 1D or two-dimensional (2D) chaotic or hyperchaotic maps based on the existing classical maps, and developing methodologies to produce a series of high-dimensional hyperchaotic maps. The former aims to produce new chaotic or hyperchaotic maps by applying nonlinear transforms to the classical chaotic maps. Even though some of the proposed maps have good chaotic proprieties, these maps have some limitations, which can be summarized as follows:

1. The proposed 1D chaotic maps use two or more classical chaotic maps to generate one pseudo random sequence, which means that these maps have no hyperchaotic behavior.
2. The mathematical structures of the proposed 1D and 2D chaotic or hyperchaotic maps are complicated, thus the encryption speed of the corresponding chaotic ciphers is generally slower than the chaotic ciphers that use simple chaotic maps.
3. Most of the existing 1D and 2D chaotic or hyperchaotic maps have low complexity performance.

The latter is to propose a framework or a system that can provide more than two pseudo random sequences with high complexity for cryptographic applications. In fact, these high-dimensional maps are constructed in the same way that were used to construct the 2D ones. Thus, they share the same problems, in which both of them have complex mathematical structures.

However, it is well-known that most of the classical discrete and continuous chaotic systems are characterized by one attractor. Therefore, it was really surprising to find that many natural and non-natural chaotic systems can generate more than one attractor. This nonlinear phenomenon is known as multistability or coexisting attractors. Actually, there are many studies that discovered the existence of various kinds of multistability behaviors in continuous chaotic systems including coexisting non-chaotic with non-chaotic attractors, chaotic with chaotic attractors, and chaotic with non-chaotic attractors. On the other hand, to the best of our knowledge, the coexistence of chaotic with non-chaotic attractants has not reported yet in discrete chaotic systems. Therefore, this new phenomenon motivates us to ask whether the selected pseudo random sequences from multistability regions are suitable for cryptographic applications.

1.6 Research Objectives

The objectives of the research are as follows:

1. To propose a new 2D discrete hyperchaotic system that has simple mathematical structure with complex dynamical behaviors and high complexity performance.
2. To propose a new image encryption algorithm based on the proposed 2D hyperchaotic map.
3. To design a new methodological framework that can generate a series of new high-dimensional discrete hyperchaotic systems, which have simple mathematical structure, complex dynamics, high sensitivity, and high complexity performance.
4. To demonstrate that discrete hyperchaotic systems with high complexity performance can generate various kinds of coexisting attractors including coexisting hyperchaotic with periodic attractors.
5. To prove that choosing pseudo random sequences from multistability regions of a new 4D continuous chaotic system can make the corresponding chaos-based cryptosystem completely insecure.
6. To demonstrate how we can generate pseudo random sequences from multistability regions of a new 3D continuous chaotic system that can be used in cryptographic applications.

1.7 Thesis Outline and Contributions

This thesis is composed of a number of chapters which are categorized according to the objectives of the study. A brief overview of each chapter as well as their associated contributions are outlined below:

Chapter 2: In this chapter, we review the existing discrete and continuous chaotic systems from a cryptographic point of view. We also determine the main issue that confronts the existing chaos-based pseudo random number generators. Furthermore, a brief literature review on chaotic image encryption algorithms is provided, which is not exhaustive and is not aimed to provide a complete account of what has been done within this domain. Instead, it is intended to provide the reader with enough information to situate this work among the relevant state of the art approaches.

Chapter 3: This chapter presents a new 2D Sine-Hénon alteration model (2D-SHAM), which is derived from the 2D Hénon map and the 1D Sine maps. The basic dynamics and the complexity performance of the 2D-SHAM are studied through stability analysis, trajectory, bifurcation diagram, Lyapunov exponents, cross-correlation coefficient and Sample Entropy algorithm. Furthermore, this chapter introduces a new image encryption algorithm, namely IEA, based on the 2D-SHAM.

Chapter 4: This chapter introduces an M-dimension nonlinear hyperchaotic model (M-NHM) as a methodological framework to produce new high-dimensional discrete hyperchaotic systems. The stability of the M-NHM is analyzed near its equilibria using Routh-Hurwitz criterion. As typical examples, the 2-NHM and 3-NHM are presented and their dynamical properties are investigated from the following aspects: trajectories, bifurcation diagram, Lyapunov exponents, and sensitivity dependence test. Besides that, the maximum Lyapunov exponents and Sample Entropy algorithm are used as evaluation tools to study the complexity performance of the 2-NHM and 3-NHM.

Chapter 5: In this chapter, we further investigate the M-NHM, where the occurrence of various multistability behaviors can be observed including the coexistence of hyperchaotic with hyperchaotic attractors as well as coexisting non-chaotic with hyperchaotic attractors. In the endeavor of chaotification, this chapter introduces a simple controller on the M-NHM, which can add one more loop in each iteration, to overcome the chaos degradation in the multistability regions.

Chapter 6: Derived from Lorenz-Haken equations, this chapter presents a new 4D continuous chaotic system with three equilibria and only two quadratic nonlinearities. The detailed dynamics of the proposed system are carefully studied, which revealed that the proposed laser system has complicated multistability behaviors. To investigate how much such chaotic systems with multistability behavior are suitable for cryptographic applications, we generate PRNG from the multistability regions, and then examine its randomness using statistical tests.

Chapter 7: In this chapter, we present a new 3D multi-attribute continuous chaotic system (MACS), which can show self-excited attractors with one unstable equilibrium and hidden attractors with either no equilibria or one stable equilibrium. The MACS generates various types of coexisting behaviors, hence it would be very suitable in cryptographic applications if the initial values and parameters are chosen from the regions of coexisting chaotic attractors. Using the Lyapunov exponents and Sample Entropy, we examine the initial values of MACS that show coexisting chaotic attractors. Consequently, we use MACS to generate PRNG that can pass all statistical tests.

Chapter 8: This chapter summarizes all the contributions that were made in this thesis, along with some potential future works.

BIBLIOGRAPHY

Ahmad, M. and Alam, M. S. (2009). A new algorithm of encryption and decryption of images using chaotic mapping. International Journal on computer science and engineering, 2(1):46 50.

Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S.-C., and Hassan, Z. (2014). Pseudo random number generator based on quantum chaotic map. Communications in Nonlinear Science and Numerical Simulation, 19(1):101 111.

Alvarez, G. and Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. International journal of bifurcation and chaos, 16(08):2129 2151.

Ana-Cristina, D. and Boriga, R. (2015). A new chaotic dynamical system and its usage in a novel pseudorandom number generator with a linear feedback register structure. Proc. Romanian Acad. Ser. A Math. Phys. Tech. Sci. Inf. Sci, 16:357 366.

Angeli, D., Ferrell, J. E., and Sontag, E. D. (2004). Detection of multistability, bifurcations, and hysteresis in a large class of biological positive-feedback systems. Proceedings of the National Academy of Sciences, 101(7):1822 1827.

Arecchi, F., Meucci, R., Puccioni, G., and Tredicce, J. (1982). Experimental evidence of subharmonic bifurcations, multistability, and turbulence in a q-switched gas laser. Physical Review Letters, 49(17):1217.

Arroyo, D., Alvarez, G., Amigó, J. M., and Li, S. (2011). Cryptanalysis of a family of self-synchronizing chaotic stream ciphers. Communications in Nonlinear Science and Numerical Simulation, 16(2):805 813.

Arroyo, D., Rhouma, R., Alvarez, G., Li, S., and Fernandez, V. (2008). On the security of a new image encryption scheme based on chaotic map lattices. Chaos: An Interdisciplinary Journal of Nonlinear Science, 18(3):033112.

Baier, G. and Klein, M. (1990). Maximum hyperchaos in generalized hénon maps. Physics Letters A, 151(6-7):281 284.

Banks, J., Brooks, J., Cairns, G., Davis, G., and Stacey, P. (1992). On devaney s definition of chaos. The American mathematical monthly, 99(4):332 334.

Baptista, M. (1998). Cryptography with chaos. Physics letters A, 240(1-2):50 54.

Brown, R. and Chua, L. O. (1996). Clarifying chaos: Examples and counterexamples. International Journal of Bifurcation and Chaos, 6(02):219 249.

Cao, C., Sun, K., and Liu, W. (2018). A novel bit-level image encryption algorithm based on 2d-licm hyperchaotic map. Signal Processing, 143:122 133.

Casas-García, K., Téllez, L. Q., Carrillo-Moreno, S., Flores-Godoy, J., and Anaya, G. F. (2016). Asymptotically stable equilibrium points in new chaotic systems. Nova Scientia, 8(16):41 58.

Chai, X., Gan, Z., Chen, Y., and Zhang, Y. (2017). A visually secure image encryption scheme based on compressive sensing. Signal Processing, 134:35 51.

Chen, A., Lu, J., Lu, J., and Yu, S. (2006). Generating hyperchaotic lu attractor via state feedback control. Physica A: Statistical Mechanics and its Applications, 364:103 110.

Chen, C. P., Zhang, T., and Zhou, Y. (2012). Image encryption algorithm based on a new combined chaotic system. In 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pages 2500 2504. IEEE.

Chen, G., Mao, Y., and Chui, C. K. (2004). A symmetric image encryption scheme based on 3d chaotic cat maps. Chaos, Solitons Fractals, 21(3):749 761.

Chen, G. and Shi, Y. (2006). Introduction to anti-control of discrete chaos: theory and applications. Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, 364(1846):2433 2447.

Chen, G. and Ueta, T. (1999). Yet another chaotic attractor. International Journal of Bifurcation and chaos, 9(07):1465 1466.

Chen, J., Zhu, Z.-l., Zhang, L.-b., Zhang, Y., and Yang, B.-q. (2018). Exploiting self-adaptive permutation–diffusion and dna random encoding for secure and efficient image encryption. Signal Processing, 142:340 353.

Chen, W., Zhuang, J., Yu, W., and Wang, Z. (2009). Measuring complexity using fuzzyen, apen, and sampen. Medical Engineering Physics, 31(1):61 68.

Chenaghlu, M. A., Jamali, S., and Khasmakhi, N. N. (2016). A novel keyed parallel hashing scheme based on a new chaotic system. Chaos, Solitons Fractals, 87:216 225.

Costa, M., Peng, C.-K., Goldberger, A. L., and Hausdorff, J. M. (2003). Multiscale entropy analysis of human gait dynamics. Physica A: Statistical Mechanics and its applications, 330(1-2):53 60.

Dăscălescu, A.-C., Boriga, R. E., and Diaconu, A.-V. (2013). Study of a new chaotic dynamical system and its usage in a novel pseudorandom bit generator. Mathematical Problems in Engineering, 2013(Article ID 769108):10 pages.

Deng, H. and Wang, Q. (2016). Radio frequency identification encryption via modified two dimensional logistic map. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 10(6):1191 1195.

Dudkowski, D., Jafari, S., Kapitaniak, T., Kuznetsov, N. V., Leonov, G. A., and Prasad, A. (2016). Hidden attractors in dynamical systems. Physics Reports, 637:1 50.

Elaydi, S. N. (2007). Discrete chaos: with applications in science and engineering. Chapman and Hall CRC, Texas, 2nd edition.

Elhadj, Z. and Sprott, J. (2008). The effect of modulating a parameter in the logistic map. Chaos: An Interdisciplinary Journal of Nonlinear Science, 18(2):023119.

Enayatifar, R., Sadaei, H. J., Abdullah, A. H., Lee, M., and Isnin, I. F. (2015). A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. Optics and Lasers in Engineering, 71:33 41.

Feudel, U., Grebogi, C., Hunt, B. R., and Yorke, J. A. (1996). Map with more than 100 coexisting low-period periodic attractors. Physical Review E, 54(1):71.

Feudel, U., Kurths, J., and Pikovsky, A. S. (1995). Strange non-chaotic attractor in a quasiperiodically forced circle map. Physica D: Nonlinear Phenomena, 88(3-4):176 186.

Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and chaos, 8(06):1259 1284.

Galias, Z. and Tucker, W. (2013). Numerical study of coexisting attractors for the hénon map. International Journal of Bifurcation and Chaos, 23(07):1330025.

Garcia, A. and Stichtenoth, H. (2006). Topics in geometry, coding theory and cryptography, volume 6. Springer Science Business Media, Dordrecht.

Gotz, M., Kelber, K., and Schwarz, W. (1997). Discrete-time chaotic encryption systems. i. statistical design approach. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 44(10):963 970.

Graham, R. and Tél, T. (1984). Existence of a potential for dissipative dynamical systems. Physical review letters, 52(1):9 12.

Grove, E. A. and Ladas, G. (2004). *Periodicities in nonlinear difference equations*, volume 4. Chapman and Hall CRC, Florida.

Guam, P. (1987). Cellular automaton public key cryptosystems. Complex Systems, 1:51 56.

Haken, H. (1975). Analogy between higher instabilities in fluids and lasers. Physics Letters A, 53(1):77 78.

Hale, J. K. and Koçak, H. (1991). Dynamics and bifurcations. Springer, New York, 1st edition.

He, D., He, C., Jiang, L.-G., Zhu, H.-w., and Hu, G.-r. (2001). Chaotic characteristics of a one-dimensional iterative map with infinite collapses. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48(7):900 906.

Heng-Jian, L. and Jia-Shu, Z. (2010). A novel chaotic stream cipher and its application to palmprint template protection. Chinese Physics B, 19(4):040505.

Hénon, M. (1976). A two-dimensional mapping with a strange attractor. Communications in Mathematical Physics, 50(1):69 77.

Hirsch, M. W., Smale, S., and Devaney, R. L. (2012). *Differential equations,* dynamical systems, and an introduction to chaos. Academic press, Waltham, 3rd edition.

Houtekamer, P. and Zhang, F. (2016). Review of the ensemble kalman filter for atmospheric data assimilation. Monthly Weather Review, 144(12):4489 4532.

Hu, H., Liu, L., and Ding, N. (2013). Pseudorandom sequence generator based on the chen chaotic system. Computer Physics Communications, 184(3):765 768.

Hua, Z., Jin, F., Xu, B., and Huang, H. (2018a). 2d logistic-sine-coupling map for image encryption. Signal Processing, 149:148 161.

Hua, Z., Zhou, B., and Zhou, Y. (2018b). Sine-transform-based chaotic system with fpga implementation. IEEE Transactions on Industrial Electronics, 65(3):2557 2566.

Hua, Z. and Zhou, Y. (2017). Design of image cipher using block-based scrambling and image filtering. Information Sciences, 396:97 113.

Hua, Z., Zhou, Y., and Chen, C. P. (2013). A new series-wound framework for generating 1d chaotic maps. In Digital Signal Processing and Signal Processing Education Meeting (DSP SPE), pages 118 123. IEEE.

Hua, Z., Zhou, Y., Pun, C.-M., and Chen, C. P. (2015). 2d sine logistic modulation map for image encryption. Information Sciences, 297:80 94.

Hubertus, F., Udwadia, F. E., and Proskurowski, W. (1997). An efficient qr based method for the computation of lyapunov exponents. Physica D, 101(1):1 16.

Ivancevic, V. G. and Ivancevic, T. T. (2008). Complex nonlinearity: chaos, phase transitions, topology change and path integrals. Springer Science Business Media, Heidelberg.

Jafari, S., Pham, V.-T., and Kapitaniak, T. (2016a). Multiscroll chaotic sea obtained from a simple 3d system without equilibrium. International Journal of Bifurcation and Chaos, 26(02):1650031.

Jafari, S. and Sprott, J. (2013). Simple chaotic flows with a line equilibrium. Chaos, Solitons Fractals, 57:79 84.

Jafari, S., Sprott, J., and Golpayegani, S. M. R. H. (2013). Elementary quadratic chaotic flows with no equilibria. Physics Letters A, 377(9):699 702.

Jafari, S., Sprott, J. C., and Molaie, M. (2016b). A simple chaotic flow with a plane of equilibria. International Journal of Bifurcation and Chaos, 26(06):1650098.

Jiang, D., Chen, Y., Gu, X., Xie, L., and Chen, L. (2017). Efficient and universal quantum key distribution based on chaos and middleware. International Journal of Modern Physics B, 31(2):1650264.

Kaffashi, F., Foglyano, R., Wilson, C. G., and Loparo, K. A. (2008). The effect of time delay on approximate sample entropy calculations. Physica D: Nonlinear Phenomena, 237(23):3069 3074.

Kanso, A. and Smaoui, N. (2009). Logistic chaotic maps for binary numbers generations. Chaos, Solitons Fractals, 40(5):2557 2568.

Kingni, S. T., Jafari, S., Pham, V.-T., and Woafo, P. (2017). Constructing and analyzing of a unique three-dimensional chaotic autonomous system exhibiting three families of hidden attractors. Mathematics and Computers in Simulation, 132:172 182.

Kocarev, L. (2001). Chaos-based cryptography: a brief overview. IEEE Circuits and Systems Magazine, 1(3):6 21.

Kocarev, L. and Lian, S. (2011). Chaos-based cryptography: theory, algorithms and applications, volume 354. Springer Science Business Media, Chennai.

Kong, W., Ding, J., Chai, T., and Sun, J. (2010). Large-dimensional multi-objective evolutionary algorithms based on improved average ranking. In 49th IEEE Conference on Decision and Control (CDC), pages 502 507. IEEE.

Kuznetsov, Y. A. (2013). Elements of applied bifurcation theory, volume 112. Springer Science Business Media, New York, 1st edition.

Layek, G. (2015). An introduction to dynamical systems and chaos. Springer, Bankura.

Lee, P.-H., Pei, S.-C., and Chen, Y.-Y. (2003). Generating chaotic stream ciphers using chaotic systems. Chinese Journal of physics, 41(6):559 581.

Leonov, G., Kuznetsov, N., and Mokaev, T. (2015). Homoclinic orbits, and self-excited and hidden attractors in a lorenz-like system describing convective fluid motion. The European Physical Journal Special Topics, 224(8):1421 1458.

Leonov, G., Kuznetsov, N., and Vagaitsev, V. (2011). Localization of hidden chuas attractors. Physics Letters A, 375(23):2230 2233.

Leonov, G. A. and Kuznetsov, N. V. (2013). Hidden attractors in dynamical systems. from hidden oscillations in hilbert kolmogorov, aizerman, and kalman problems to hidden chaotic attractor in chua circuits. International Journal of Bifurcation and Chaos, 23(01):1330002.

Li, C., Sprott, J., and Thio, W. (2014). Bistability in a hyperchaotic system with a line equilibrium. Journal of Experimental and Theoretical Physics, 118(3):494 500.

Li, C., Sprott, J. C., Hu, W., and Xu, Y. (2017). Infinite multistability in a self-reproducing chaotic system. International Journal of Bifurcation and Chaos, 27(10):1750160.

Li, S.-J. (2003). Analyses and new designs of digital chaotic ciphers. PhD thesis, Xi an Jiaotong University.

Li, T.-Y. and Yorke, J. A. (1975). Period three implies chaos. The American Mathematical Monthly, 82(10):985 992.

Liang, W., Sun, X., Xia, Z., Sun, D., and Long, J. (2011). A chaotic ip watermarking in physical layout level based on fpga. Radioengineering, 20(1):118 125.

Liu, W., Sun, K., He, Y., and Yu, M. (2017). Color image encryption using three-dimensional sine icmic modulation map and dna sequence operations. International Journal of Bifurcation and Chaos, 27(11):1750171.

Liu, W., Sun, K., and Zhu, C. (2016). A fast image encryption algorithm based on chaotic map. Optics and Lasers in Engineering, 84:26 36.

Lorenz, E. N. (1963). Deterministic nonperiodic flow. Journal of the atmospheric sciences, 20(2):130 141.

Lu, J. and Chen, G. (2002). A new chaotic attractor coined. International Journal of Bifurcation and chaos, 12(03):659 661.

Lu, J., Chen, G., and Zhang, S. (2002). Dynamical analysis of a new chaotic attractor. International Journal of Bifurcation and chaos, 12(05):1001 1015.

Lyapunov, A. M. (1992). The general problem of the stability of motion. International journal of control, 55(3):531 534.

Ma, J., Chen, Z., Wang, Z., and Zhang, Q. (2015). A four-wing hyper-chaotic attractor generated from a 4-d memristive system with a line equilibrium. Nonlinear Dynamics, 81(3):1275 1288.

Martínez-Zerega, B. E., Pisarchik, A. N., and Tsimring, L. (2003). Using periodic modulation to control coexisting attractors induced by delayed feedback. Physics Letters A, 318(1-2):102 111.

Matthews, R. (1989). On the derivation of a chaotic encryption algorithm. Cryptologia, 13(1):29 42.

May, R. M. (1976). Simple mathematical models with very complicated dynamics. Nature, 261(85-93):459.

Mobayen, S., Volos, C. K., Kaçar, S., Çavuşoğlu, U., and Vaseghi, B. (2018). A chaotic system with infinite number of equilibria located on an exponential curve and its chaos-based engineering application. International Journal of Bifurcation and Chaos, 28(09):1850112.

Molaie, M., Jafari, S., Sprott, J. C., and Golpayegani, S. M. R. H. (2013). Simple chaotic flows with one stable equilibrium. International Journal of Bifurcation and Chaos, 23(11):1350188.

Nazarimehr, F., Rajagopal, K., Kengne, J., Jafari, S., and Pham, V.-T. (2018). A new four-dimensional system containing chaotic or hyper-chaotic attractors with no equilibrium, a line of equilibria and unstable equilibria. Chaos, Solitons Fractals, 111:108 118.

Ozkaynak, F. (2014). Cryptographically secure random number generator with chaotic additional input. Nonlinear Dynamics, 78(3):2015 2020.

Ozkaynak, F. (2018). Brief review on application of nonlinear dynamics in image encryption. Nonlinear Dynamics, 92(2):305 313.

Pak, C. and Huang, L. (2017). A new color image encryption using combination of the 1d chaotic map. Signal Processing, 138:129 137.

Pham, V.-T., Jafari, S., and Volos, C. (2017a). A novel chaotic system with heart-shaped equilibrium and its circuital implementation. Optik-International Journal for Light and Electron Optics, 131:343 349.

Pham, V.-T., Jafari, S., Volos, C., Vaidyanathan, S., and Kapitaniak, T. (2016). A chaotic system with infinite equilibria located on a piecewise linear curve. Optik-International Journal for Light and Electron Optics, 127(20):9111 9117.

Pham, V.-T., Volos, C., Jafari, S., and Kapitaniak, T. (2017b). Coexistence of hidden chaotic attractors in a novel no-equilibrium system. Nonlinear Dynamics, 87(3):2001 2010.

Pisarchik, A., Flores-Carmona, N., and Carpio-Valadez, M. (2006). Encryption and decryption of images with chaotic map lattices. Chaos: An Interdisciplinary Journal of Nonlinear Science, 16(3):033118.

Pisarchik, A. and Zanin, M. (2008). Image encryption with chaotically coupled chaotic maps. Physica D: Nonlinear Phenomena, 237(20):2638 2648.

Pisarchik, A. N. (2001). Controlling the multistability of nonlinear systems with coexisting attractors. Physical Review E, 64(4):046203.

Pisarchik, A. N. and Feudel, U. (2014). Control of multistability. Physics Reports, 540(4):167 218.

Qi, G., Chen, G., Du, S., Chen, Z., and Yuan, Z. (2005). Analysis of a new chaotic system. Physica A: Statistical Mechanics and its Applications, 352(2-4):295 308.

Rahimov, H., Babaei, M., and Farhadi, M. (2011). Cryptographic prng based on combination of lfsr and chaotic logistic map. Applied Mathematics, 2(12):1531.

Rajagopal, K., Akgul, A., Jafari, S., Karthikeyan, A., and Koyuncu, I. (2017). Chaotic chameleon: Dynamic analyses, circuit implementation, fpga design and fractional-order form with basic analyses. Chaos, Solitons Fractals, 103:476 487.

Richman, J. S. and Moorman, J. R. (2000). Physiological time-series analysis using approximate entropy and sample entropy. American Journal of Physiology-Heart and Circulatory Physiology, 278(6):H2039 H2049.

Richter, H. (2008). On a family of maps with multiple chaotic attractors. Chaos, Solitons Fractals, 36(3):559 571.

Robinson, C. (1998). Dynamical systems: stability, symbolic dynamics, and chaos. CRC press, London, 2nd edition.

Rossler, O. E. (1976). An equation for continuous chaos. Physics Letters A, 57(5):397 398.

Routh, E. J. (1877). A treatise on the stability of a given state of motion: particularly steady motion. Macmillan and Company, London.

Rozenbaum, E. B., Ganeshan, S., and Galitski, V. (2017). Lyapunov exponent and out-of-time-ordered correlators growth rate in a chaotic system. Physical review letters, 118(8):1 5.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., and Barker, E. (2001). A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Booz-Allen and Hamilton Inc Mclean Va.

Shannon, C. E. (1949). Communication theory of secrecy systems. Bell system technical journal, 28(4):656 715.

Shi, Y. and Chen, G. (2005). Chaotification of discrete dynamical systems governed by continuous maps. International Journal of Bifurcation and Chaos, 15(02):547 555.

Shi, Y., Yu, P., and Chen, G. (2006). Chaotification of discrete dynamical systems in banach spaces. International Journal of Bifurcation and Chaos, 16(09):2615 2636.

Shukla, P., Khare, A., Rizvi, M., Stalin, S., and Kumar, S. (2015). Applied cryptography using chaos function for fast digital logic-based systems in ubiquitous computing. Entropy, 17(3):1387 1410.

Singh, J. P., Rajagopal, K., and Roy, B. K. (2018). A new 5d hyperchaotic system with stable equilibrium point, transient chaotic behaviour and its fractional-order form. Pramana, 91(3):33.

Som, S. and Sen, S. (2013). A non-adaptive partial encryption of grayscale images based on chaos. Procedia Technology, 10:663 671.

Sprott, J. (2006). High-dimensional dynamics in the delayed hénon map. Electronic journal of theoretical physics, 3(12):19 35.

Sprott, J. and Munmuangsaen, B. (2018). Comment on a hidden chaotic attractor in the classical lorenz system. Chaos, Solitons Fractals, 113:261 262.

Stallings, W. (2006). Cryptography and Network Security, 4 E. Pearson Education India, Upper Saddle River, fifth edition.

Strogatz, S. H. (2018). Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering. CRC Press, Boca Raton, 2nd edition.

Sun, F., Liu, S., Li, Z., and Lu, Z. (2008). A novel image encryption scheme based on spatial chaos map. Chaos, Solitons Fractals, 38(3):631 640.

Tahir, F. R., Jafari, S., Pham, V.-T., Volos, C., and Wang, X. (2015). A novel no-equilibrium chaotic system with multiwing butterfly attractors. International Journal of Bifurcation and Chaos, 25(04):1550056.

Tang, Z., Song, J., Zhang, X., and Sun, R. (2016). Multiple-image encryption with bit-plane decomposition and chaotic maps. Optics and Lasers in Engineering, 80:1 11.

Van Tartwijk, G. H. and Agrawal, G. P. (1997). Nonlinear dynamics in the generalized lorenz-haken model. Optics communications, 133(1-6):565 577.

Wang, X., Pham, V.-T., Jafari, S., Volos, C., Munoz-Pacheco, J. M., and Tlelo-Cuautle, E. (2017). A new chaotic system with stable equilibrium: From theoretical model to circuit implementation. IEEE Access, 5:8851 8858.

Wang, X. F. and Chen, G. (2000). Chaotifying a stable map via smooth small-amplitude high-frequency feedback control. International Journal of Circuit Theory and Applications, 28(3):305 312.

Wang, X.-y. and Qin, X. (2012). A new pseudo-random number generator based on cml and chaotic iteration. Nonlinear Dynamics, 70(2):1589 1592.

Wei, Z. (2011). Dynamical behaviors of a chaotic system with no equilibria. Physics Letters A, 376(2):102 108.

Wei, Z. (2012). Complex dynamics of a new chaotic system without equilibria. In Chaos-Fractals Theories and Applications (IWCFTA), 2012 Fifth International Workshop on, pages 79 82. IEEE.

Wei, Z., Moroz, I., and Liu, A. (2014a). Degenerate hopf bifurcations, hidden attractors, and control in the extended sprott e system with only one stable equilibrium. Turkish Journal of Mathematics, 38(4):672 687.

Wei, Z., Moroz, I., Sprott, J., Akgul, A., and Zhang, W. (2017). Hidden hyperchaos and electronic circuit application in a 5d self-exciting homopolar disc dynamo. Chaos: An Interdisciplinary Journal of Nonlinear Science, 27(3):033101.

Wei, Z., Wang, R., and Liu, A. (2014b). A new finding of the existence of hidden hyperchaotic attractors with no equilibria. Mathematics and Computers in Simulation, 100:13 23.

Wei, Z. and Yang, Q. (2011). Dynamical analysis of a new autonomous 3-d chaotic system only with stable equilibria. Nonlinear Analysis: Real World Applications, 12(1):106 118.

Wei, Z. and Yang, Q. (2012). Dynamical analysis of the generalized sprott c system with only two stable equilibria. Nonlinear Dynamics, 68(4):543 554.

Wei, Z., Zhang, W., and Yao, M. (2015). On the periodic orbit bifurcating from one single non-hyperbolic equilibrium in a chaotic jerk system. Nonlinear Dynamics, 82(3):1251 1258.

Wei-Bin, C. and Xin, Z. (2009). Image encryption algorithm based on henon chaotic system. In 2009 International Conference on Image Analysis and Signal Processing, pages 94 97. IEEE.

Wheeler, D. D. and Matthews, R. A. (1991). Supercomputer investigations of a chaotic encryption algorithm. Cryptologia, 15(2):140 152.

Wiggins, S. (2003). Introduction to applied nonlinear dynamical systems and chaos, volume 2. Springer Science Business Media, New York, 2nd edition.

Wolf, A., Swift, J. B., Swinney, H. L., and Vastano, J. A. (1985). Determining lyapunov exponents from a time series. Physica D: Nonlinear Phenomena, 16(3):285 317.

Wolfram, S. (1985). Cryptography with cellular automata. In Conference on the Theory and Application of Cryptographic Techniques, pages 429 432. Springer.

Wu, Y., Noonan, J. P., Yang, G., and Jin, H. (2012). Image encryption using the two-dimensional logistic chaotic map. Journal of Electronic Imaging, 21(1):013014.

Wu, Y., Zhou, Y., and Bao, L. (2014). Discrete wheel-switching chaotic system and applications. IEEE Transactions on Circuits and Systems I: Regular Papers, 61(12):3469 3477.

Xu, G., Shekofteh, Y., Akgul, A., Li, C., and Panahi, S. (2018). A new chaotic system with a self-excited attractor: entropy measurement, signal encryption, and parameter estimation. Entropy, 20(2):86.

Yang, T., Wu, C. W., and Chua, L. O. (1997). Cryptography based on chaotic systems. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 44(5):469 472.

Yicong, Z., Hua, Z., Pun, C.-M., and Chen, C. P. (2015). Cascade chaotic system with applications. IEEE transactions on cybernetics, 45(9):2001 2012.

Yu, M., Sun, K., Liu, W., and He, S. (2018). A hyperchaotic map with grid sinusoidal cavity. Chaos, Solitons Fractals, 106:107 117.

Yuan, H.-M., Liu, Y., Gong, L.-H., and Wang, J. (2017). A new image cryptosystem based on 2d hyper-chaotic system. Multimedia Tools and Applications, 76(6):8087 8108.

Zanin, M. and Pisarchik, A. N. (2014). Gray code permutation algorithm for high-dimensional data encryption. Information Sciences, 270:288 297.

Zeraoulia, E. (2012). Robust chaos and its applications, volume 79. World Scientific, Singapore.

Zhang, H. and Chen, G. (2004). Single-input multi-output state-feedback chaotification of general discrete systems. International Journal of Bifurcation and Chaos, 14(09):3317 3323.

Zhang, H., Wang, H., and Chen, W.-K. (2002). Oversampled chaotic binary sequences with good security. Journal of Circuits, Systems, and Computers, 11(02):173 185.

Zhang, S., Zeng, Y., Li, Z., Wang, M., and Xiong, L. (2018). Generating one to four-wing hidden attractors in a novel 4d no-equilibrium chaotic system with extreme multistability. Chaos: An Interdisciplinary Journal of Nonlinear Science, 28(1):013113.

Zhang, Y., Kong, G., and Yu, J. (2009). Critical curves and coexisting attractors in a quasiperiodically forced delayed system. Physics Letters A, 373(15):1341 1345.

Zhang, Y. and Xiao, D. (2014). An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Communications in Nonlinear Science and Numerical Simulation, 19(1):74 82.

Zheng, F., Tian, X.-j., Song, J.-y., and Li, X.-Y. (2008). Pseudo-random sequence generator based on the generalized henon map. The Journal of China Universities of Posts and Telecommunications, 15(3):64 68.

Zhongyun, H. and Zhou, Y. (2016a). Dynamic parameter-control chaotic system. IEEE Trans. Cybernetics, 46(12):3330 3341.

Zhongyun, H. and Zhou, Y. (2016b). Image encryption using 2d logistic-adjusted-sine map. Information Sciences, 339:237 253.

Zhou, N., Hu, Y., Gong, L., and Li, G. (2017). Quantum image encryption scheme with iterative generalized arnold transforms and quantum image cycle shift operations. Quantum Information Processing, 16(6):164.

Zhou, N., Pan, S., Cheng, S., and Zhou, Z. (2016). Image compression encryption scheme based on hyper-chaotic system and 2d compressive sensing. Optics Laser Technology, 82:121 133.

Zhou, Y., Bao, L., and Chen, C. P. (2014). A new 1d chaotic system for image encryption. Signal processing, 97:172 182.

Zhou, Y., Panetta, K., Agaian, S., and Chen, C. P. (2012). Image encryption using p-fibonacci transform and decomposition. Optics Communications, 285(5):594 608.