CHAOTIFICATION METHODS FOR ENHANCING ONE-DIMENSION DIGITAL CHAOTIC MAPS FOR APPLICATIONS IN CRYPTOGRAPHY

MOATSUM KHALIF ODUH ALAWIDA

UNIVERSITI SAINS MALAYSIA

2020

CHAOTIFICATION METHODS FOR ENHANCING ONE-DIMENSION DIGITAL CHAOTIC MAPS FOR APPLICATIONS IN CRYPTOGRAPHY

by

MOATSUM KHALIF ODUH ALAWIDA

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

March 2020

ACKNOWLEDGEMENT

First and foremost, I have to thank Allah for somehow to help me and make everything going from hard into easy. I would like to thank my supervisor Prof Azman Samsudin for his patience and continued support during my study, he gave me all the cognitive and advisory support all the time about contributions and writing. These few words do not meet the size of appreciation and respect for him. Also, I would like to thank my co-supervisor Dr Je Sen Teh for his continued help in discussing ideas and research papers. I would like to extend my special thanks to the Dean and all staff members of the School of Computer Science, USM. There is no word to express my deep feelings to my lovely mother, wife, sisters, brothers, and my little daughters (Lenda and Lama) for their feeling and hopes.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
ApEn	Approximate Entropy
BRA	Bit Reversal Approach
CC	Correlation Coefficient
CD	Correlation Dimension
CDF	Cumulative Distribution Function
CML	Coupled Map Lattice
DCFSA	Deterministic Chaotic Finite State Automata
DES	Data Encryption Standard
DFA	Deterministic Finite Automata
DFM	Deterministic Finite Machine
DUH	Deviation from the Uniform Histogram
FCD	Fuzzy correlation Dimension
FNN	False Nearest neighbors
FuzzyEn	Fuzzy Entropy
GSE	Global Shannon Entropy
HCS	Hybrid Chaotic System
HD	High-Dimension
IEEE	Institute of Electrical and Electronics Engineers

LCT	Logistic-Control-Tent
LE	Lyapounv Exponent
LLE	Largest Lyapounv Exponent
LSE	Local Shannon Entropy
MAC	Message Authentication Code
MD5	Massage Digest Five
NFA	Non-Deterministic Finite Automata
NIST	National Institute of Standards and Technology
NPCR	Number of Pixels Change Rate
PRBG	Pseudo Random bit Generator
PRNG	Pseudo Random Number Generator
PSCS	Parametric Switching Chaotic System
RSA	Pubic-key encryption algorithm
SampEn	Symplectic Entropy
SE	Shannon Entropy
SMN	Stat-Mapping Network
SymEn	Symplectic Entropy
TLM	Tent-Logistic Map
TM-DFSM	Tent Map-Deterministic Finite State Machine
TRNG	True Random Number Generator
UACI	Unified Average Changing Intensity

USM	Universiti Sains Malaysia
1D	One-Dimension

KAEDAH KECAMUKAN MENINGKATKAN KEUPAYAAN PETA CAMUK DIGITAL SATU DIMENSI UNTUK APLIKASI KRIPTOGRAFI

ABSTRAK

Peta camuk digital satu dimensi menjadi semakin popular dalam bidang kriptografi kerana kedua-duanya mempunyai banyak persamaan dan mempunyai struktur yang mudah. Walau bagaimanapun, peta ini mempunyai banyak kelemahan yang telah dikenal pasti yang menyumbang secara negatif terhadap keselamatan algoritma kriptografi yang menggunakannya. Oleh itu, menambahbaikkan peta camuk digital satu dimensi dari segi kecamukan dan sifat statistik akan menyumbang terhadap penambahbaikan kepada algoritma kriptografi yang berasaskan kecamukan. Banyak kaedah mempertingkatkan kecamukan telah dicadangkan untuk menangani isu-isu ini. Walau bagaimanapun, kebanyakan kaedah ini bergantung kepada sumber entropi luaran untuk meningkatkan ciri-ciri peta camuk satu dimensi. Dalam kajian ini, empat kaedah mempertingkatkan kecamukan yang baru telah dicadangkan untuk menangani isu-isu tersebut tanpa memerlukan sumber luaran. Kaedah pertama ialah automata terbatas deterministik yang dihibridisasi dengan peta camuk satu dimensi di bawah kawalan kaedah mempertingkatkan kecamukan yang sedia ada. Tujuan kaedah ini adalah untuk melemahkan isu degradasi dinamik dengan memanjangkan panjang kitaran. Untuk mempertingkatkan kerumitan dan memperluaskan julat parameter kecamukan, kaedah kedua dicadangkan berdasarkan kepada perubahan nilai keadaan kecamukan dengan memperbalikkan urutan bit pecahannya. Dengan menggabungkan kedua-dua kaedah pertama dan kedua, kaedah ketiga dicadangkan berdasarkan kepada peta camuk satu dimensi dan automata terbatas deterministik yang dikawal oleh permutasi bit. Kaedah keempat yang diperkenalkan adalah berasaskan kepada kaedah lata dan gabungan

beberapa kaedah lain sebagai rangka kerja mudah untuk membesarkan julat parameter camuk dan juga untuk meningkatkan prestasi camuk. Analisis teori dan penilaian prestasi camuk menunjukkan bahawa kaedah yang dicadangkan mempunyai panjang kitaran yang panjang (panjang kitaran $> 10^5$ pada ketepatan bit 10^{-8}), tahap tidak-linear yang lebih tinggi (purata entropi simpangan pada tahap lebih-kurang 0.824), tahap kerumitan yang lebih baik (purata entropi fuzzy pada tahap lebih-kurang 1.87), dan julat parameter camuk yang lebih besar (parameter kawalan $r \in (0,\infty)$) berbanding dengan kaedah-kaedah baru lain yang telah dicadangkan. Peta camuk ini kemudiannya akan digunakan dalam reka bentuk algoritma kriptografi baru (enkripsi imej, fungsi hash, penjana nombor/bit pseudo-rawak). Analisis keselamatan dan prestasi menunjukkan bahawa algoritma penyulitan imej camuk yang dicadangkan sangat terjamin keselamatannya seperti yang dibuktikan oleh skor purata piksel (NPCR) dengan skor purata sehingga 99.65% dan skor nilai perubahan intensiti tergabung (UACI) dengan skor sehingga 33.45%. Dari segi keselamatan dan prestasi algoritma, algoritma yang dicadangkan juga melampaui prestasi algoritma-algoritma penyulitan imej camuk yang lain. Sejumlah analisis yang dilakukan pada kajian fungsi hash camuk baru ini telah menunjukkan bahawa fungsi yang dicadangkan mempunyai sifat statistik yang baik dengan perubahan bit dan kebarangkalian $\bar{B} = 64.127$ dan $P = 50.09$ masing-masing, rintangan perlanggaran dengan perlanggaran sifar $WN(0) = 9403$, dan secara amnya mempunyai prestasi statistik yang lebih baik jika dibandingkan dengan fungsi hash camuk sedia ada yang lain. Penjana nombor rawak camuk telah dicadangkan dan hasil statistik menunjukkan bahawa penjana yang dicadangkan mempunyai keselamatan yang lebih baik daripada penjana camuk yang sedia ada, seperti yang ditunjukkan yang mana penjana yang dicadangkan telah lulus semua 15 sub-ujian NIST SP 800-22.

CHAOTIFICATION METHODS FOR ENHANCING ONE-DIMENSION DIGITAL CHAOTIC MAPS FOR APPLICATIONS IN CRYPTOGRAPHY

ABSTRACT

Digital one-dimensional chaotic maps are becoming increasingly popular in the area of cryptography due to their commonalities and their simple structures. However, these maps have well-known drawbacks which contribute negatively towards the security of the cryptographic algorithms that utilize them. Thus, enhancing digital one-dimensional chaotic maps in terms of their chaoticity and statistical properties will contribute towards the improvement of chaos-based cryptography. Many chaotification methods have been recently proposed to address these issues. However, most of these methods are dependent on an external entropy source to enhance the characteristics of one-dimensional chaotic maps. In this study, four novel chaotification methods are proposed to address these issues without the need of external entropy sources. The first method hybridizes deterministic finite state automata with one-dimensional chaotic maps under control the existing chaotification methods. The aim of this method is to weaken dynamical degradation issue through prolonging cycle length. To increase chaotic complexity and enlarge chaotic parameter range, the second method is proposed based on modifying chaotic state values by reversing the order of their fractional bits. To take advantage of the first two proposed methods, the third method is proposed based on a one-dimensional chaotic map and deterministic finite state machine under the control of bitwise permutations. The fourth method is introduced based on cascade and combination methods as a simple framework to enlarge the chaotic parameter range and to enhance chaotic performance. Theoretical analysis and chaotic performance evaluation indicate that the proposed methods have

long cycle lengths (cycle length $> 10^5$ at bit precision 10^{-8}), higher nonlinearity (average symplectic entropy of approximately 0.824), better complexities (average fuzzy entropy of approximately 1.87), and larger chaotic parameter ranges (control parameter $r \in (0,\infty)$) as compared to other recently proposed chaotification methods. The new chaotic maps are then used in the design of new cryptographic algorithms (image encryption, hash function, pseudo random number/bit generator). Security and performance analysis indicate that the proposed chaotic image encryption algorithms are highly secure as indicated by average number of pixels change rate (NPCR) scores of up to 99.65% and unified average changing intensity (UACI) values of up to 33.45%. The proposed algorithms also surpass existing chaotic image encryption algorithms in terms of security and performance. A number of analysis performed on the new chaotic hash function indicates that the proposed function has a good statistical properties with average bit changes and probabilities of $\bar{B} = 64.127$ and $P = 50.09$ respectively, collision resistance with zero collisions of $W_N(0) = 9403$, and generally has better statistical performance when compared to the other existing chaotic hash functions. Chaotic random number generators are proposed and the statistical results shows that the proposed generator has better security than existing chaotic generators, as indicated by the passing of all the 15 sub-tests of NIST SP 800-22.

CHAPTER 1

INTRODUCTION

1.1 Overview

Natural and non-natural phenomena such as the weather, fluid dynamics, lasers and climate can produce chaotic behaviors (Raymond, 1997; Xubin et al., 1993). Chaotic behaviors can be studied by using mathematical paradigms, known as chaotic systems. Chaotic systems possess the following common characteristics: sensitivity to slight changes to control parameters and initial conditions, topological mixing property, dense periodic trajectories and unpredictability. Each initial condition is highly capable of determining the nature of the chaotic trajectory. Any random small change to the initial condition leads to a completely different trajectory. Due to these important characteristics, chaos theory is widely studied in many fields, such as engineering, economics, geology, physics, biological, chemical, meteorology, mathematics, politics, robotics, philosophy, cryptography, algorithmic trading and secure communications (Ji et al., 2018; Kyrtsou and Labys, 2007; Radek and Radmila, 2016; Strogatz, 2018; Wu et al., 2014).

The first chaotic system was introduced by E. N. Lorenz to study the change of weather (Edward, 1963). Thereafter, a lot of chaotic systems have been proposed to study various kinds of phenomena such as population (Robert, 2004), kneading operation (Ronald, 1997), Arnold's cat map (Igorevich and André, 1968), etc. The chaotic systems can be one dimensional (1D) or high dimensional (HD) and can be divided into two classes: continuous-time and discrete-time chaotic systems. Continuous-time

chaotic systems is usually defined by a differential equations such as partial or ordinary differential equation. Examples of continuous-time systems include Lu chaotic attractor (Jinhu and Guanrong, 2002), Chua circuit (Leon et al., 1993), Lorenz system (Edward, 1963) and oscillating circuits (Bao et al., 2017). In contrast, discrete-time chaotic systems usually take the method of iterated functions to generate chaotic behaviors and defined by a difference equations. Examples of discrete-time systems include sine map, tent map and logistic map.

A discrete chaotic system is implemented on finite precision machines, such as computers. It generates chaotic behavior in the bounded space, which is called pseudo-chaos or digital chaos. A digital chaos map has dynamical characteristics, with low chaotic complexity compared to the chaotic system that is implemented on the analog circuit (Erivelton et al., 2019). An analog chaotic system is extremely complex, hard to predict, and unstable. However, an analog chaotic system requires the development of an electronic circuit to each chaotic system to generate chaotic behavior. Furthermore, due to the fact that cryptography handles digital data, the analog chaotic system is not appropriate for cryptographic applications.

With fast growth of communication technology, it is vital to protect private data from unauthorized access. Information security offers five basic principles to protect data, which are confidentiality, authentication, integrity, non-repudiation, access control, and availability. Cryptography is a science related to the achievement of these security principles. As a result, a number of different cryptographic algorithms have been proposed to suit different security applications.

Digital chaos has been used in different applications, such as watermarking, optimization, cryptography. Cryptography and chaos have many common characteristics, such as unpredictability, sensitivity to slight change to initial condition or control parameter, random-like behavior, ergodicity, and uniform distribution. Thus, chaotic maps are used as a source of diffusion and confusion in several chaotic cryptographic algorithms such as image encryption, hash function, and pseudo-random number generator (PRNG). Furthermore, the control parameters and the initial conditions of the chaotic maps are used as the key in a lot of chaotic cryptographic algorithms. 1D and HD chaotic maps are widely used to design new chaotic cryptographic algorithms during the last decades. 1D chaotic maps, such as unimodal maps, have attracted many researchers because they are simple mathematical equations and do not require more time to implement them.

1.2 Motivation

Chaos-based cryptography has several benefits compared to conventional cryptography, it is easy to expand the keyspace and swap the internal chaotic maps for different data encryption purposes. Besides, conventional cryptography shown to be unsuitable for fast encryption of bulky data such as color images encryption and video encryption (Chen et al., 2012; Luo et al., 2015; Zhang and Wang, 2015). In image encryption, the popular conventional symmetric algorithms such as DES, AES, and others are not suitable for image encryption due to the special characteristics of images such as large data capacity, and strong redundancy with high correlations between adjacent pixels (Li et al., 2018; Niyat et al., 2017). On the other hand, a digital chaotic map is more suitable for image encryption, which can remove the correlation and provides good

confusion and diffusion on the large data. As a consequence, many chaos-based image encryption algorithms have been proposed, and there are also many issues that have not yet been addressed (Ghadirli et al., 2019).

Many various cryptographic algorithms have adopted 1D chaotic maps in their proposed designs (Hou et al., 2017; Hua and Zhou, 2018), because the maps can be defined by simple mathematical equations which are easily coded into computer instructions. The security of chaotic cryptographic algorithms is derived from the adopted chaotic maps, whereby the chaotic characteristics are obviously reflected in algorithms. For instance, the initial condition and control parameter are always used in the design of the key in the chaotic ciphers, a small change to these parameters leads to a new independent chaotic cipher. Despite its simplicity and ease of implementation, 1D chaotic behaviors suffer from many security challenges such as limited chaotic range and small cycle length. This leads to a lot of research that studies 1D chaotic behaviors. Thus, these challenges attracted many researchers to propose new solutions to avoid security loopholes (Arroyo et al., 2008; Lingfeng and Suoxia, 2015; Nagaraj et al., 2008; Shujun et al., 2004). Many studies examine the impact of directly applying 1D chaotic maps in the cryptographic algorithms without modifications or enhancements. They found that these algorithms suffered from different security loopholes, such as relatively small keyspace, low complexity behavior, and unable to withstand different types of attacks.

Based on the cryptanalytic algorithm, many proposed cryptographic algorithms based on 1D chaotic maps are found to be insecure (Ponnain and Chandranbabu, 2016; Wang et al., 2018; Yong et al., 2017). The selection of 1D chaotic map is considered the

main challenge of chaotic cryptographic algorithms. Hence, many novel chaotification methods have been recently proposed to enhance the existing 1D chaotic maps (Deng et al., 2015a; Hua and Zhou, 2018; Hua et al., 2015; LingFeng et al., 2014). They all contributed towards better chaos performance, which better reflects on the security of chaotic cryptographic algorithms. Therefore, despite these new methodologies, chaos-based cryptography is still in its infancy and has yet to be adopted for general purpose usage. Thus, there is still a lot of potential work to be done in the area before chaos-based cryptography is widely accepted for cryptographic use.

1.3 Problem Statement

In recent decades, chaotic cryptographic applications have attracted many interests from researchers due to the common properties shared between cryptography and chaotic behavior. Thus, the chaotic cryptography is regarded as a new direction alongside traditional cryptography. Many chaotic cryptography algorithms have been designed to protect the different multimedia types (Alvarez and Li, 2006; Ghadirli et al., 2019). Existing 1D chaotic maps, which generally includes unimodal maps, are simple mathematical equations and easy to execute on a computer. They were therefore selected to be used in the design of many chaotic cryptographic algorithms. Unfortunately, these algorithms are unable to resist different types of well-known attacks (Feng et al., 2019; Li et al., 2013; Ponnain and Chandranbabu, 2016; Wang et al., 2018; Zhao et al., 2012). The main defect behind these weak algorithms is the adopted 1D chaotic maps which are known to have security loopholes.

In digital chaos, the dynamical degradation phenomenon arises when the chaotic systems are implemented on finite precision computing devices such as on computers. One of the causes of dynamical degradation is the truncation process. Using truncation functions such as flooring, rounding, and fixing on each chaotic iteration, the truncated chaotic points approach each other. After a certain number of the iterations, the chaotic trajectory lies in a cycle. When a chaotic trajectory generates a small cycle length, the chaotic points are repeated and have many negative properties such as non-uniform distribution, low linear complexity, low ergodicity and the strong correlation of chaotic trajectory. 1D chaotic maps rapidly degrade after a small number of iterations as compared to their HD counterparts and have small cycle lengths (Chengqing et al., 2019; Chunlei et al., 2019; Deng et al., 2015b; Liu and Miao, 2017; Liu et al., 2017b).

In chaotic complexity, 1D chaotic maps have simple mathematical definitions that produce chaotic behavior, in which chaotic behavior is the main source of security for chaotic cryptographic algorithms. Unfortunately, 1D chaotic maps generate low chaotic behaviors (low complexity) that are easy to attack. Low chaotic complexity arises as simple patterns and simple attractors in chaotic behaviors. Thus, the given or extracted points of a chaotic trajectory can be easily used to estimate parameters of 1D chaotic map such as initial condition and control parameter. For example, the logistic map is one of the unimodal maps and has a critical point for each control parameter (Arroyo et al., 2008). A critical point is the largest point of trajectory and always indicates to control parameter such as $0.5 \rightarrow 4,\ 0.25 \rightarrow 3.75,\ 0.225 \rightarrow 3$ and so on. Furthermore, the recent estimation technologies, coupled with lightweight complexity analysis can quickly identify the 1D chaotic maps parameters (Arroyo et al., 2013; Chengqing et al., 2019; Wang et al., 2009). These estimation techniques include op-

timization algorithms (He et al., 2007; Jiang et al., 2015; Tang and Guan, 2009), gray codes, symbolic dynamics (Arroyo et al., 2009a), return map (Adrian, 2008) and phase space reconstruction (Hamza, 2017). Identification of the control parameter and estimation of the initial condition leads to identifying the key in the chaotic cryptographic algorithms.

Basically, chaotic parameter region is an important factor in chaotic cryptography algorithms, it represents the keyspace of algorithms and provides high flexibility in algorithm designs. Thus, a large chaotic parameter range is the most crucial for chaotic cryptographic algorithms. Unfortunately, 1D chaotic maps have limited chaotic parameter ranges and discontinuous behaviors, with many periodic windows of non-chaotic behaviors. Therefore, chaotic cryptographic algorithms based on 1D chaotic maps have a small keyspace, can be attacked by brute force (Dhivya et al., 2016; Hua and Zhou, 2016a; Zhou et al., 2014).

To sum up, the main vulnerabilities of 1D chaotic maps are caused by several issues such as:

1. 1D chaotic maps suffer from dynamical degradation at a rapid rate.
2. Easy to estimate control parameters and initial conditions.
3. Limited and discontinuous chaotic parameter ranges.

In the past few years, many chaotification methods such as cascade, switching and perturbation have been proposed to enhance the existing chaotic maps (Deng et al., 2015a; Hua et al., 2018b). Most of the proposed methods require an external entropy

source to enhance a simple 1D chaotic map. These sources may include a continuous chaotic system, a random number sequence, or additional digital chaotic maps. These techniques adversely affect the efficiency of the resulting maps. In addition, the external entropy source itself may suffer from statistical defects. Rather, a chaotification method should be simple, without needing an external source to generate excellent chaotic behaviors.

1.4 Research Objective

Based on the issues highlighted in the problem statement, the major objectives of this study is to propose novel chaotification methods to enhance the existing 1D chaotic maps and to design new chaotic cryptographic algorithms based on each of the proposed methods. Therefore, the goals of this research are as stated below:

1. To reduce the effect of the dynamical degradation of 1D digital chaotic maps by hybridized 1D chaotic map and deterministic finite state automata (DFA).

2. To enhance the chaotic complexity of 1D chaotic maps by reversal order fraction bits of chaotic point.

3. To expand the chaotic parameter range of 1D digital chaotic maps by hybridized cascade and combination method in the simple framework.

4. To design secure and practical cryptographic algorithms based on each of the proposed chaotification methods.

1.5 Research Scope

This study focuses on proposing novel chaotification methods to enhance the existing 1D chaotic maps and to improve the security of chaotic cryptographic algorithms. The new and existing digital 1D chaotic maps are examined based on the proposed chaotic benchmarks in the past two decades. This study uses the discrete chaotic maps such as unimodal maps (logistic, sine, and tent maps) and Henon map in the proposed chaotification methods. Other chaotic maps that are not included in the scope will not be used in this study.

In order to investigate the security and flexibility of the proposed chaotification methods, new chaotic cryptographic algorithms following the proposed methods are designed such as digital image encryption, hash function, PRNG and PRBG. Hence, symmetric cryptographic algorithms, block cipher, cryptographic hash functions and pseudo random generator included in the scope of this thesis. Other cryptographic branches such as asymmetric, stream cipher, lightweight cipher did not include in the scope of this thesis.

1.6 Research Contribution

According to the objectives of this study, four novel chaotification methods are introduced. Each one of these methods can generate many new chaotic maps. Furthermore, each proposed method is used in designing new chaotic cryptographic algorithm. Thus, the research contributions of this study can be categorized into two groups, chaotic maps and cryptographic algorithms. The basic contributions in a chaotic maps are as below:

1. Deterministic chaotic finite state automata (DCFSA) configurations using DFA with existing 1D chaotic maps under different existing chaotification methods.

2. Bit reversal approach (BRA) method based on reversal bit and fixed-point standard.

3. Tent map-deterministic finite state machine (TM-DFSM) based on tent map and DFSM under bit-wise permutations.

4. hybrid chaotic system (HCS) based on simple hybrid method between cascade and combination systems.

Also, the second group of contributions of this study focuses on multiple ways to design new chaotic cryptographic algorithms. Each proposed chaotification method is adopted in the design of a new algorithm. On a whole, the second group of contributions can be listed as below:

1. New image encryption algorithm based on TM-DFSM to create flexible keyspace and achieve high security.

2. New image encryption algorithm based on HCS to generate high sensitivity imagecipher to a small change to key or plain-image.

3. New hash function based on DCFSA to achieve high collision resistance and performance.

4. PRNG based on the application of the HCS method to investigate new chaotic maps and achieve uniform distribution.

5. PRBG based on the application of BRA method to investigate new chaotic maps in secure cryptographic applications.

The novel methods and new algorithms are evaluated in terms of security, flexibility and speed performance, which will be described and discussed in detail in the following chapters.

1.7 Research Process

The methodology applied in this study is conducted in five phases. First, the existing literature of 1D chaotic maps and chaotic cryptographic algorithms are studied to exhibit the shortcomings and difficulties. The weaknesses of 1D chaotic maps are listed and studied. In addition, the comparison of the existing chaotification methods is introduced to identify the research gap of these methods. The main issues of the chaotic cryptographic algorithms are studied and highlighted. These algorithms include chaotic image encryption, chaotic hash function and chaos-based pseudorandom number generator (PRNG).

In the second phase, based on internal entropy sources, novel chaotification methods are proposed to produce many new chaotic maps. To showcase the chaotic performance of the proposed methods, theoretical analysis based on cycle analysis and Lyapunov exponent (LE) are introduced and several experiments (including bifurcation diagram, LE, Shannon entropy (SE), Fuzzy entropy (FuzzyEn), Fuzzy Correlation Dimension (FCD), and cycle analysis) are performed in the third phase. These measurements are carefully selected to study different security aspects such as chaotic parameter sensitivity, ergodicity, chaotic range, strangeness, nonlinearity and complex-

ity. Meanwhile, decision and comparison to other existing chaotification methods are introduced in the same phase.

In the fourth phase, new chaotic cryptographic algorithms based on the different new chaotic maps that generated from the proposed chaotification methods are designed. For example, new chaotic image encryption was proposed based on the new chaotic maps to fulfill the security requirements and addressing defects that were discussed in Chapter 2. Finally, the experimental evaluation and performance analysis of the new chaotic cryptographic algorithms are reported in the fifth phase, whereby the results are compared to other chaotic cryptographic algorithms. These experimental evaluations are widely used in the chaos-based cryptographic primitive domains. Table 1.1 provides a summary of the five phases of the research steps and Figure 1.1 shows an overview of the steps involved in this study .

Table 1.1: Research Process

Phase	Details
Performing literature study	Shortcomings of 1D chaotic maps. Comparing of the existing chaotification methods. Weaknesses of existing chaotic cryptographic algorithms.
Proposing	Proposing novel chaotification method.
Chaotic analysis	• Theoretical analysis. • Chaotic performance evaluations. • New experimental investigations. • Comparing to the existing 1D chaotic maps. • Comparing to some recent chaotification methods.
Designing algorithms	• Designing new chaotic cryptographic algorithms. • TM-DFSM-based image encryption. • HCS-based image encryption. • DCFSA-based hash function. • HCS-BASD PRNG.BRA-based PRBG.
Evaluating	• Designing experiments to analyze security • Measuring complexity computation. • Comparing to other chaotic cryptographic algorithms.

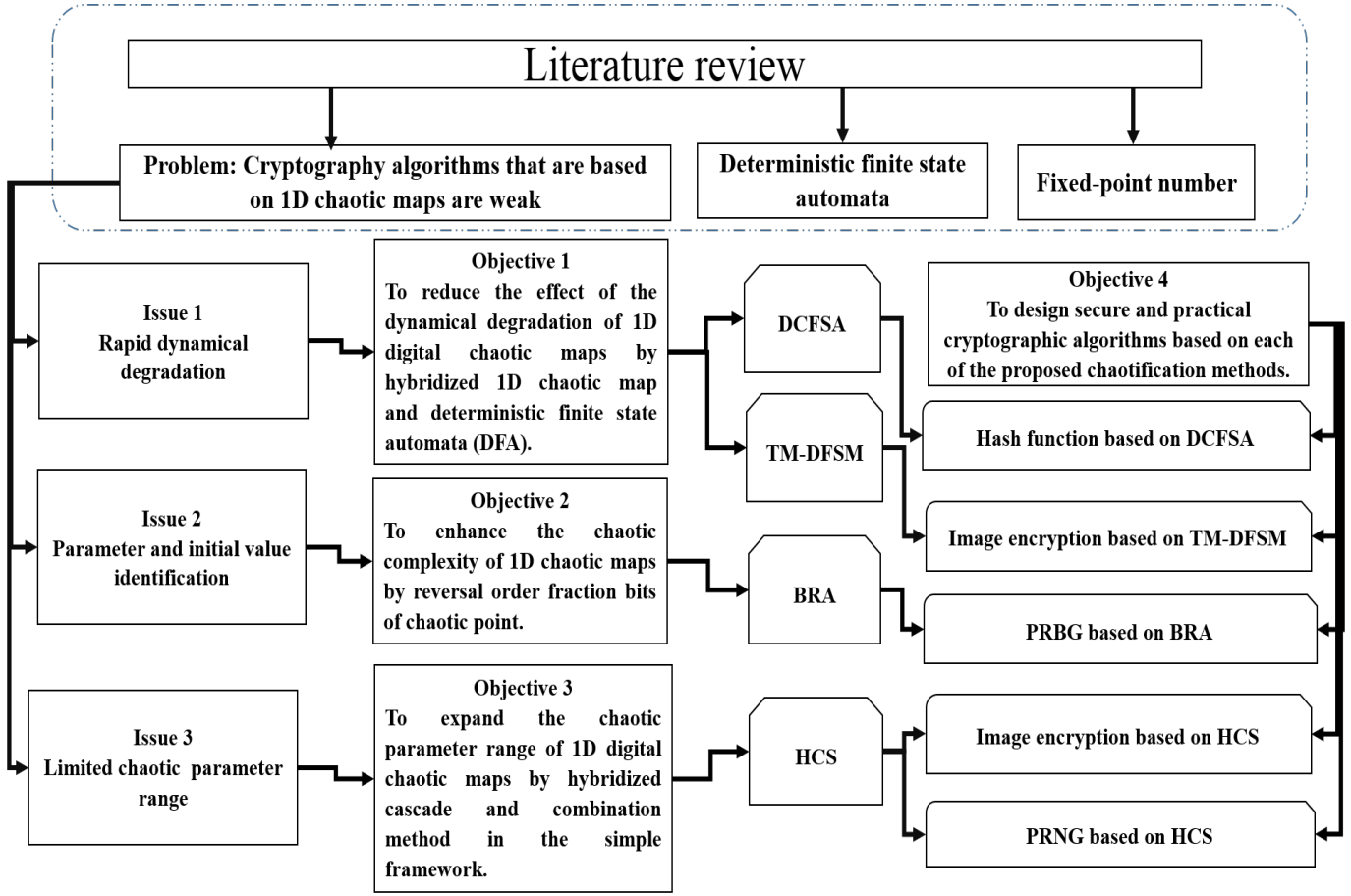

Figure 1.1: Research process

1.8 Outline of the Thesis

The thesis is organized into six chapters. Chapter 1 provides an overview of concepts, problems, methodology, and contributions of the research. Chapter 2 briefly reviews the closely related literature review, background and presents a description of the methods, concepts, and tools used in this thesis. Chapter 3 provides steps to build novel chaotification methods. Chapter 4 studies the chaotic behavior of the proposed methods under a set of investigations and discusses the chaotic results and the research outcomes. Chapter 5 provides new chaotic cryptographic algorithms with their evaluations and discusses the outcomes. Finally, Chapter 6 provides the conclusion and focuses on future research works.

CHAPTER 2

BACKGROUND AND LITERATURE REVIEW

2.1 Introduction

From thousands of years ago, the use of cryptography in protecting sensitive information in all spheres of life remain unprecedented. The rapid influence of information technology and telecommunications in our society implies that strong security requirement must be developed to fit and address new technological challenges for the protection of data at the state of rest, in transit or in use during exchange over public channels. Several cryptographic primitives have been employed in achieving security such as confidentiality, integrity, authentication, non-repudiation, access control and digital signature (Ljupco, 2001). The vast majority of cryptosystems are designed to be highly secure and fast especially when a bulk amount of data such as images, videos or audio data are being transferred. Traditional cryptography such as DES, AES, etc, has been developed and widely used for protecting confidential data. On the other hand, digital chaos has been adopted in designing many cryptographic algorithms. They are designed and developed alongside traditional cryptography to protect sensitive data against different types of attacks. Hence, chaotic cryptography has gained a good reputation as one of the most widely researched cryptographic algorithms and has been extensively used for securing sensitive information (Alvarez and Li, 2006).

Shannon, in his principles of secure systems (Claude, 1949), did not formally use the word chaos in his theory but he referred to the meaning of chaos through his proposed design of secure cryptosystem which is based on mixing transformation and high

sensitivity to any slight change. Therefore, chaos is considered to be the source of entropy, diffusion and confusion in chaos-based cryptographic systems. Based on these features, in 1989, the first two digital chaotic cryptosystems was proposed (Matthews, 1989; Toshiki et al., 1991). In the past two decades, a large body of research has produced several enhanced versions of chaos-based cryptosystems (Belazi et al., 2019; Ghadirli et al., 2019; Nepomuceno et al., 2019; Pak and Huang, 2017). However, some of them are found to be not secure (Feng et al., 2019; Feng and He, 2018; Li et al., 2019; Wang et al., 2018). Several reasons around vulnerabilities of chaotic ciphers are found, most of them indicated that digital chaos has many limitations and challenges. Therefore, these weaknesses and countermeasures have made the digital chaos a very interesting area.

This chapter will study information related to chaotic maps which includes chaotic behaviors, examples of existing chaotic maps, quantifying chaotic tools, chaotic issues and methods, and chaotic cryptographic applications. In this chapter, the research gap in the existing chaotification methods will be highlighted, and the new concepts that will be used in the next chapters will be also described in this chapter.

2.2 Chaos and Properties

The phenomena known as the butterfly effect is one of the most well-known characteristics of chaos theory. Chaos can be considered as a type of nonlinear dynamical system, which provides a link between determinism and randomness. Formally, chaos is defined as an "aperiodic long-term behaviour in a deterministic system that exhibits sensitive dependence on initial conditions" with the chaotic signals exponentially di-

verging with time evolution (also known as the Lyapunov exponent (LE)). LE is used as a quantitative measure to identify a chaotic behavior.

Table 2.1: Chaos theory terms

Term	Definition
Dynamical system	A dynamical system is a paradigm representing the temporal evolution of particular mathematical rules from a specified initial state. The result of a dynamical system is vectors or time series.
Deterministic	The output point of a dynamic system is unique to the input point.
Chaotic system	Chaos is a nonlinear dynamic system that is composed of an iterated function, an initial condition, time and a control parameter to generate a data series.
Initial condition	Initial condition(s) is the initial input value(s) for a chaotic system. The initial value should be within the domain's phase space.
Control parameter	A real number that has the primary role in generating chaotic behavior.
Trajectory	A series of points generated by the iterative function. The points start from x_0 to x_n, where n is the n^{th} iteration of system. Trajectory is also known as the orbit of a chaotic system.
Phase space	It is the bound of the chaotic points, which limits them between two values, eg. $[0, 1]$.
Mixing property	A small change in an initial condition and control parameter can cause a considerable change in the chaotic behavior.
Ergodicity	Describes the chaotic trajectory in which the trajectory visits its all states in the phase space uniformly regardless of where it is initiated.

The system variable, control parameter and initial condition values of dynamical systems have a real, infinite phase space. However, when a dynamical system is realized on a computer, all these values are represented by points from a finite space. Chaotic trajectories that are generated by a nonlinear deterministic dynamical system is entirely unpredictable at high iterations (Rupak, 2011). Table 2.1 shows the conceptual terms that are often used in the chaos domain to pave a way for easy understanding for readers.

A nonlinear dynamical system is considered a chaotic system if it has the following properties:

- **Bounded**: The phase space of all possible system variables (states) along the trajectory should be bounded. This means that the system variables of the trajectory must remain between an upper limit and a lower limit. For example, the phase space for the logistic map is [0, 1].
- **Deterministic**: The system must be a deterministic function where an input uniquely determines an output.
- **Aperiodic**: A trajectory of a nonlinear dynamical system does not lie in periodic cycle or a fixed point.
- **Sensitivity**: Any slight change to initial conditions or/and control parameters in a nonlinear dynamical system will diverge exponentially and rapidly as time evolves. If the system has at least one positive LE, then such a system is considered as unpredictable and chaotic.

In order to study the properties of a nonlinear dynamical systems, the logistic map is used as an example. The logistic map was designed to model the population growth over time, in which the system can be represented by simple equation of a second degree nonlinear dynamical system. The logistic map is defined as:

$$x_{n+1} = r \times x_n \times (1 - x_n) \tag{2.1}$$

where r is the control parameter that ranges between $[0, 4]$ and x_n is a system variable in

the range of the phase space $[0,1]$. If r is chosen to be between 3.9 to 4, then the logistic map will produce the chaotic behavior, leading to a trajectory that is unpredictable, covers the entire phase space, and has random-like behavior.

The first condition of a chaotic map is it must be bounded. The logistic map is bounded between $[0,1]$ with a control parameter range of $r \in [0,4]$. The logistic map is also a deterministic function, whereby its outputs depend on its chaotic point and control parameter values. In order to verify the logistic map's trajectory fulfils the third condition, aperiodicity, the trajectory was simulated using Matlab. As shown in Figure 2.1, the trajectory of the logistic map moves randomly as time evolves. A detailed analysis on its aperiodicity can be found in (Li et al., 2005).

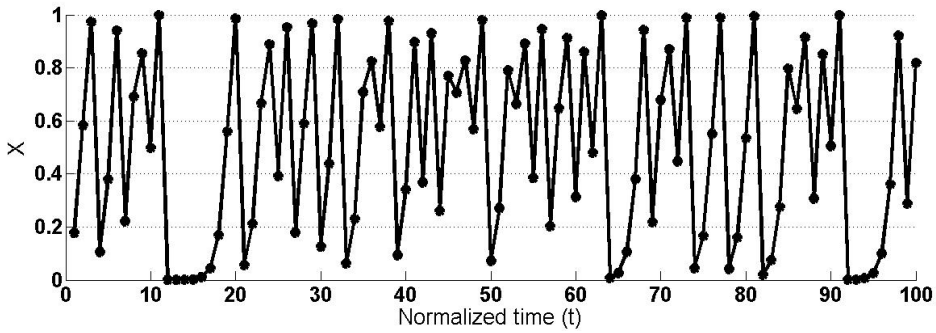

Figure 2.1: The trajectory of the logistic map

Finally, to demonstrate that the logistic map is sensitive to its initial condition and control parameter, two logistic trajectories $\{X_1, X_2\}$ were generated from two initials conditions that are extremely close to each other (x_a, x_b), with control parameter r being defined as $r = 4$. The difference in initial conditions is noted as ε. Let ε be equal to 10^{-8} and $\varepsilon = (|x_a - x_b|) = 10^{-8}$. In Figure 2.2, the two trajectories X_1 and X_2 diverge from each other after 20 iterations. Meanwhile, Figure 2.3 shows the two system variables $|x_a - x_b|$ diverging at an exponential rate as time elapses. The diverging

values start off with a positive slope before turning into a straight line on a log plot. This indicates that a small change in the initial conditions of the logistic chaotic map will completely generate a new chaotic trajectory.

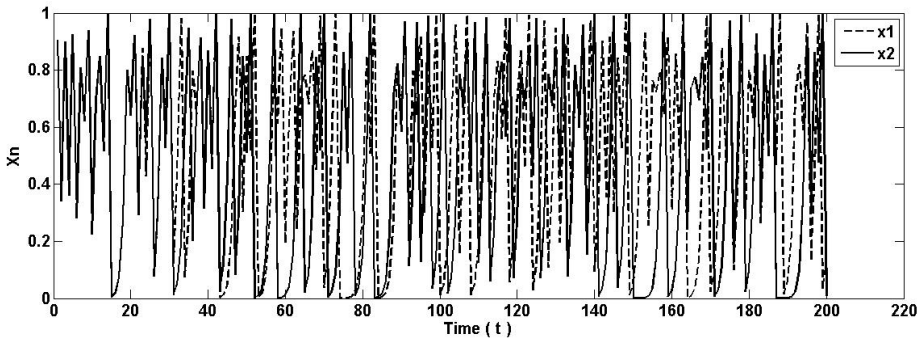

Figure 2.2: Two trajectories of two logistic maps that start from initial points that are close to each other

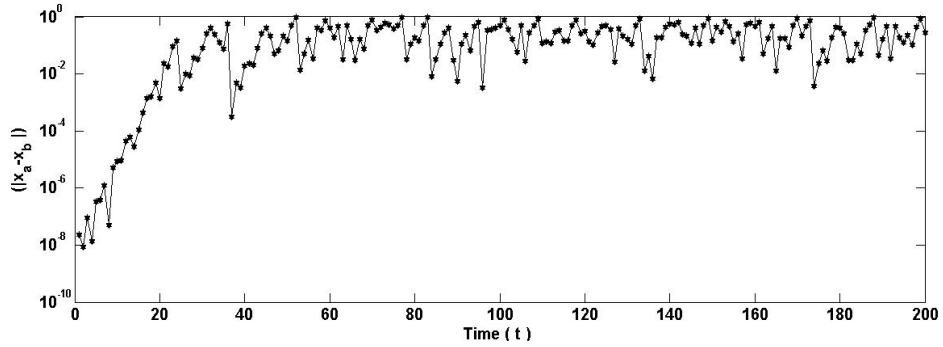

Figure 2.3: Exponential divergence of two trajectories of two logistic maps that start from initial points that are close to each other

To evaluate the sensitivity of a control parameter, a similar experiment is performed. The two trajectories are generated by using the same initial condition and but instead, a slight change to the control parameter is introduced. The exponential divergence of system variables is shown in each iteration. To summarise, chaotic systems are nonlinear deterministic dynamic systems, but not all of these systems are chaotic systems, as only some of the them have chaotic characteristics.

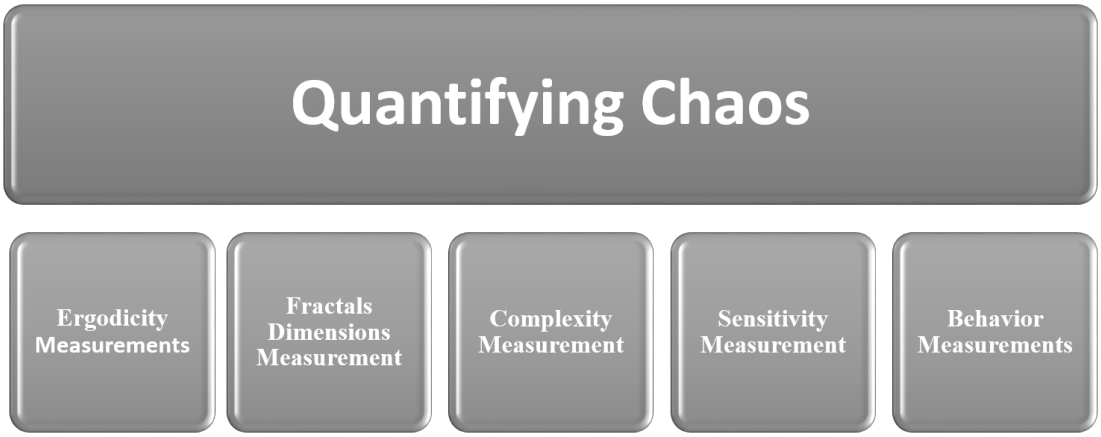

Figure 2.4: Quantifying chaos

2.3 Quantifying Chaos

To evaluate a nonlinear dynamical system and investigate its chaotic behavior along its control parameter range and phase space, there is a set of quantifiers that can be used. They cover different aspects of chaotic behaviors, and have been used in the domain of chaotic system by different researchers. These metrics are classified as shown in Figure 2.4.

2.3.1 Behavior Measurement

This section discusses the measures of chaotic behavior over its phase space and its relationship with control parameters, through the use of iteration function diagram and bifurcation diagram.

2.3.1(a) Iteration Function Diagram

In order to analyze the dynamic behavior for any of digital chaotic map (a chaotic system implemented with finite computing precision), and to describe the relationship between intputs and outputs along its phase space (attractor), the iteration function

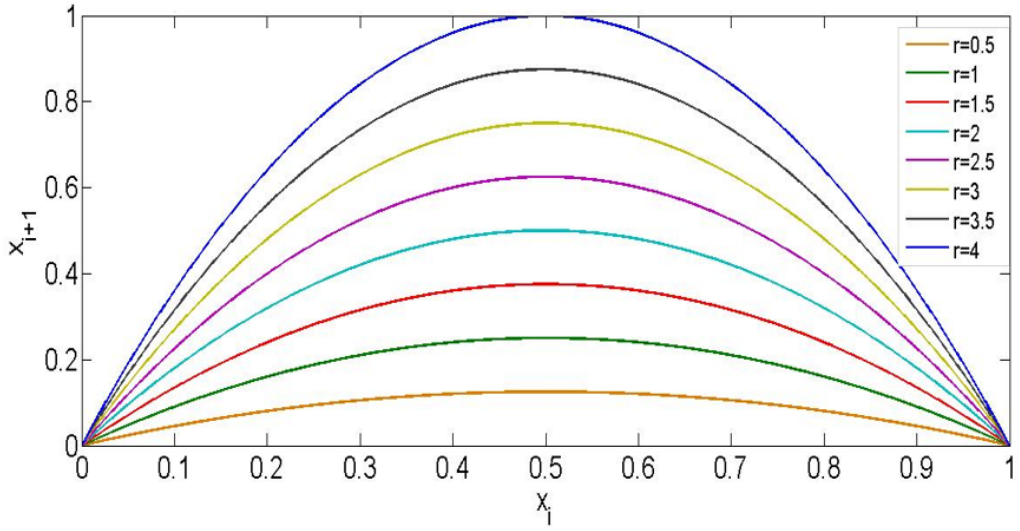

Figure 2.5: Iteration function associated to the logistic map

diagram (chaos attractor) has been used in many studies (Arroyo et al., 2008; Liu and Miao, 2017; Wu et al., 2014; Zhou et al., 2015). It also describes the complex geometric shape of the attractor. To plot an iteration function diagram, the input phase space is divided into a set of points. Two values (x_{n+1}, x_n) of a chaotic map f are selected, where $x_{n+1} = f(x_n)$. The control parameter is constant for all inputs (Zhou et al., 2015). Figure 2.5 illustrates the iteration function diagram for the logistic map, which is classified as a unimodal map. A unimodal map always has a critical point x_c in its phase space for each control parameter, and is monotonically increasing for $x_n < x_c$ while monotonically decreasing for $x_n > x_c$ (Arroyo et al., 2008). In fact, the iteration function diagram can distinguish the complex patterns from simple patterns in the phase space, which plays a significant role in the security benefits of chaos-based cryptography to withstand against statistical attacks (Liu and Miao, 2017).

2.3.1(b) Bifurcation Diagram

A bifurcation diagram always reveals interesting features of a nonlinear dynamic systems along a range of control parameter. These features include chaotic, non-

chaotic, periodic, fixed point, period doubling, blank windows, stable and unstable orbits (Ji et al., 2018; Martínez and Cantón, 2015). As an example, the bifurcation diagram of logistic map $f_L(x_0, r)$ with a control parameter $r \in [0,4]$ is shown in Figure 2.6 $f_L : [0,1] \rightarrow [0,1]$ which exhibits the distribution of system variables x_n for different parameter settings. Based on Figure 2.6, a detailed analysis of the logistic map's bifurcation diagram is as follows (Arroyo et al., 2008):

- The bifurcation diagram exhibits a stable fixed point equal to 0 for $r \in (0,1)$. It also exhibits a stable fixed point equal to $(r-1)/r$ for $r \in (1,3)$.
- The bifurcation diagram shows the doubling-period cascade region for $r \in (3, 3.57)$ which means that there exists periodic attractors of period $2m$ for $m = 1, 2, ..., m$, where m is the precision of the finite space used in a hardware implementation.
- For $r \geq 3.57$ the logistic map depicts chaotic behavior but with visible periodic windows. These regions are a mix between periodic and chaotic attractors but do not reach a strange attractor.

In short, the bifurcation diagram can be useful in studying how system variables are related to each control parameter, and can provide information about the behavior of chaotic maps with respect to changes to its control parameter. It identifies the chaotic parameter values for which the system has desired chaotic features, while also revealing undesired features which are unsuitable for chaotic cryptographic algorithms. Therefore, the bifurcation diagram is a good tool to identify asymptotic points for choosing best keys in chaos-based cryptography algorithms (Arroyo et al., 2009a; Shujun et al., 2004).

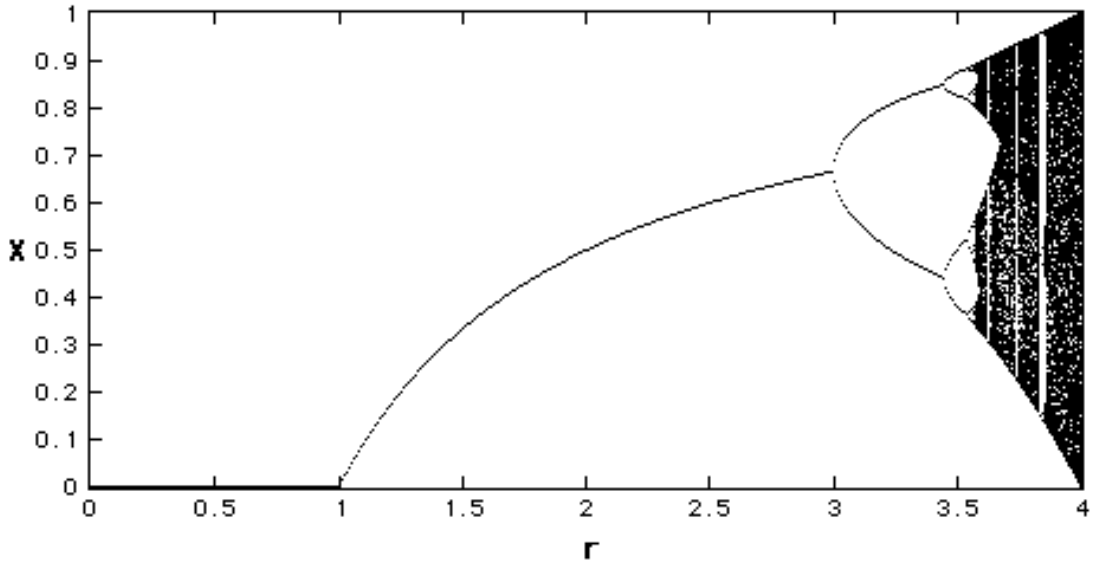

Figure 2.6: Bifurcation diagram for r between 0 and 4

2.3.2 Sensitivity Measurement

The butterfly effect is one of the most significant feature of a chaotic system. Its sensitivity to initial conditions and/or control parameters can provide unpredictable chaotic behavior, which is desirable in chaos-based cryptography. LE and correlation tests can be used for sensitivity measurements.

2.3.2(a) Lyapunov Exponent

LE is a quantitative measure to identify if a nonlinear dynamical system has chaotic behavior (Hua and Zhou, 2018; Jan et al., 2018; Wang and Wu, 2015). LE represents the average exponential rate for two trajectories that start from infinitesimally close points, that may diverge or converge as time elapses (Alan et al., 1985). Two trajectories start at x_0 and $x_0 + \varepsilon$, where ε is an infinitesimally small distance. If this distance enlarges exponentially with as time goes on, the value of the LE would be positive, indicating that the system is chaotic and unstable for a particular region. On the other hand, a negative LE value indicates that the system is attracted to a fixed point or a