Ain Shams University
University College of Women
for Art, Science and Education
Mathematics Department

A NOVEL METHOD FOR THE USAGE OF CHAOS THEORY-BASED CRYPTOGRAPHY

THESIS
SUBMITTED IN PARTIAL
FULFILLMENT OF REQUIREMENTS
FOR THE DEGREE
OF
MASTER OF SCIENCE
(PURE MATHEMATICS)
BY

Lina Ahmed Sayed Khamis

Mathematics Department
University College of Women for
Art, Science and Education
Ain Shams University

SUPERVISORS

Prof. Dr. Salwa Kamal Abd-El-Hafiz
Professor of Engineering Mathematics
Faculty of Engineering
Cairo University

Prof. Dr. Gamal Ali Fouad Ismail
Professor of Pure Mathematics
University College of Women for
Art, Science and Education
Ain Shams University

2014

Ain Shams University
University College of Women for Art, Science and Education
Mathematics Department

M.Sc. Thesis
(PURE MATHEMATICS)

Title of thesis:

A NOVEL METHOD FOR THE USAGE OF CHAOS THEORY-BASED CRYPTOGRAPHY

Thesis supervisors:

Prof. Dr. Salwa Kamal Abd-El-Hafiz
Professor of Engineering Mathematics
Faculty of Engineering
Cairo University

Prof. Dr. Gamal Ali Fouad Ismail
Professor of Pure Mathematics
University College of Women
for Art, Science and Education
Ain Shams University

Ain Shams University
University College of Women for Art, Science and Education
Mathematics department

COURSES

The student has passed the following courses in partial fulfillment of requirements for M.Sc. Degree:

1. Numerical Analysis. 3h per week.
2. Differential Equation. 3h per week.
3. Difference Equation. 3h per week.
4. Control Theory. 3h per week.
5. Special Course. 3h per week.

Head of Mathematics Department

بسم الله الرحمن الرحيم

"قالوا ربنا لا علم لنا إلا ما علمتنا إنك أنت العزيز الحكيم"

وما توفيقي إلا بالله عليه توكلت و إليه أنيب

Before I begin, I want to start with thanking my Lord "Allah" who is always guiding me and teaching me from his knowledge.

Lina Ahmed Sayed

Acknowledgment

First of all, I would like to express my thankfulness to my Lord "**ALLAH**" who taught me from his knowledge and guided me to achieve this work.

All achievements contained in this thesis should be owed to my supervisors: **Prof. Dr. Salwa Kamal** and **Prof. Dr. Gamal Ali**. It is their serious supervision and encouragement to help me overcome many difficulties during this work.

Also I would like to give the most sincere thanks to my parents, specially my father (RIP) whom I hoped to be with me, whose teaching and education gave me great courage and confidence. I would like to thank my beloved husband for his continuous support and care for me.

Finally, I don't forget to thank the stuff members of Mathematics Department for interest and facilities they offered me.

CONTENTS

Chapter 4
A Novel Image Encryption Method

ABSTRACT

Lina Ahmed Sayed Khamis. Master of Science dissertation of Pure Mathematics, on Chaos Based Cryptography. University College of Women for Art, Science and Education, Ain Shams University.

The main purpose of this thesis is to study Chaos Theory.

This thesis is divided into five chapters:

In the **First Chapter**, we introduce the basics of Chaos Theory discussing dynamical properties for the most popular models. We also give an overview on cryptography in a historical view and its two types symmetric and asymmetric keys.

In **Chapter Two**, we illustrate the common properties for chaos and cryptography. Then we introduce chaos based cryptography in a literature review starting by English text encryption and then image encryption.

In **Chapter Three**, we discuss the evaluation criteria that are required to analyze the randomness properties. Then, we compare some statistical properties of four chaotic generators and use each of them in a simple block cipher to compare their ciphertexts randomness. The map with best chaotic behaviour returns the best randomized ciphertext than the other maps. In a secure crypto-system, the use of a good chaotic generator with desirable dynamical statistical properties is the most important.
The results have been accepted by

"*Journal of Scientific Research-In Science*", 31, 2014.

In **Chapter Four**, we design a novel method to encrypt a colored image by using the maps of better randomness properties. We perform the criteria we illustrated in Chapter 3, getting a highly secured ciphered image and an efficient encryption method.
These results have been published in

"*International J. of Computers & Technology*", 3(1) (2014) 4110-4117.

Finally, we illustrate the conclusions of our work and suggest some ideas for our future work.

Keywords: Chaos, bifurcation, plaintext, ciphertext, stream cipher, block cipher, symmetric key, asymmetric key, image encryption.

SUMMARY

There has been a considerable amount of research in the field of nonlinear dynamical systems and chaos theory and many attempts have been made to find the possible applications of the concepts derived from these fields. One of the applications of chaos theory has been in the design of cryptosystems. These two fields share interesting similarities which make the fusion very natural. Chaotic systems are characterized by their extreme sensitivity to initial conditions and seemingly random behavior, which enable the design of a good cryptographic system with many desirable properties.

In Chapter 1, we introduce the basics of Chaos Theory. Chaos is an advanced field of mathematics that involves the study of dynamical systems which are easy to find in science represented in the form of mathematical systems changing over time. Dynamical systems are classified into two types: the first one is the discrete–time dynamical system, which takes the current state as input and updates the situation by producing a new state as output, and it is defined by a “map” such as Logisic map, Piece-Wise linear chaotic map and Hénon map . The other type is the continuous–time dynamical system, defined by a “flow” such as Lorenz system and R□ssler system.

Modern telecommunication networks, and especially the internet and mobile-phones networks, have tremendously extended the limits and possibilities of communications and information transmissions. Cryptography is the best solution against the unauthorized use of the information. Encryption is the process of hiding a message and Decryption is the reverse process to obtain the original message. A

plaintext is a message that is required to be hidden, and it could be a stream of bits, a text file, a stream of digitized voice, digital image or video, etc. Ciphertext is an encrypted message. A fundamental issue of all kinds of cryptosystems is the key. Shannon in 1949 through his celebrated paper [37] stressed out the importance of diffusion and confusion for a cryptosystem to be accepted. Diffusion means spreading out of the influence of a single plaintext character over many ciphertext characters so as to hide the statistical structure of the plaintext. Confusion is to complicate dependence of ciphertext statistics compared to that of plaintext. Modern cryptography could be divided into two categories. The first is the symmetric-key cryptosystem which uses the same key both for encryption and decryption and is very fast. The second is the asymmetric-key cryptosystem (public key cryptosystem) which uses different key pair to encrypt and decrypt, the encryption key is made to be public while the other part of the key for decryption is kept private. Also there are two classes of ciphers, stream ciphers and block ciphers.

In Chapter 2, we illustrate the common properties between chaos and cryptography. A lot of work has been done in the past in the field of chaos based encryption, with simple chaotic systems being used. At the beginning, chaos based cryptography was used to encrypt English texts such as Baptista's method [8], cross coupled chaotic map method [31]and the block cipher introduced in 1999 [34]. But with the rapid development in technology, many recent researches are performed to encrypt images.

A chaotic system is characterised by the seemingly random behavior, as the behavior of a single output (or a state variable) of a chaotic system varies randomly. Suitable metrics are needed to investigate the degree of randomness. However, few standards address

statistical analysis techniques that should be employed in practice. In fact, an ideal cipher should be robust against any statistical attacks. In order to evaluate the security of cryptosystems, the histogram, correlation coefficients, entropy test, mean absolute and square errors tests, differential attack tests and the National Institute of Standards and Technology (NIST) tests are performed.

In Chapter 3, we compare some statistical properties of one dimensional maps which are the logistic and the piecewise linear chaotic maps, two dimensional normalized Hénon map by only considering the variation of x or y with iterations and a continuous time Lorenz three dimensional system. We conclude that the PieceWise Linear Chaotic Map (PWLCM) has showed better randomness. Then, we use each of them in a simple block cipher to compare their ciphertexts randomness. We get the best randomized ciphertext by using the PWLCM than the other maps. In a secure cryptosystem, the use of a good chaotic generator with desirable dynamical statistical properties is the most important.

In Chapter 4, we introduce a new scheme to encrypt an image. Its idea is to generate from one initial condition several chaotic initial conditions, by the first chaotic map, e.g., logistic map, for another chaotic map, e.g., PWLCM. Then, we use the resultant chaotic sequences of the second map in both forms, the binary form and the real number form, and apply it to diffuse and confuse the image. Also, we introduce a delay element to increase the security and a reverse order round to increase the cipher strength against brute force attacks. The cipher images show very good statistical analysis measure correlation, histogram distributions and differential attack measures.

Finally, we conclude from this work that the best chaotic behavior and digital randomness chaotic generator returns the best

randomized cipher. And we design a novel highly secured encryption scheme. We also suggest some possibilities of our future work.

Chapter 1

Introduction and Basic Concepts

1.1 Introduction

In this chapter, we will give some basic definitions and theorems for the basics of Chaos theory. Also, we will discuss the most popular models and their dynamical properties. The second section will be an overview on cryptography.

1.2 Basics of Chaos Theory

Dynamical systems are easy to be found everywhere in science and nature in the form of any mathematical system that changes over time. The electrical engineer may be concerned with the oscillatory output from non-linear circuits; the chemist /chemical engineer with the regular cycling of a chemical reaction; the biologist with the cycles of growth and decay in animal populations; the cardiovascular surgeon with the regular (and more so, irregular) beating of the human heart; the economist with the boom-bust cycles of the stock market; the physicist with the motion of a driven pendulum; the astronomer with the cyclical motion of the celestial bodies; and so on. Whatever dynamical system presented, chaos theory can be used to understand it.

Many people believe that 20^{th} century science will be remembered for three main theories: quantum mechanics, relativity, and chaos. Chaos theory is blanketing theory that covers all aspects of science. Hence, it shows up everywhere in the world today. It is a developing scientific discipline which is focused on the study of non-linear systems.

A dynamical system is concerned with making qualitative predictions about the behavior of systems, which evolve in time as parameters which control the system and the initial state of the system itself are varied (i.e., about the starting value and the rule itself). The computations associated with dynamical system are as follow. At first, they define the dynamical system by setting the initial conditions and the system parameters. Secondly, they define the equations for the system and solve them numerically. Then, gain a deeper understanding of the basins of attraction. Finally, iterate on this process to motivate choices of initial condition and parameters.

Dynamical systems are classified into two types. The first one is the discrete–time dynamical system [10, 17, 21], which takes the current state as input and updates

the situation by producing a new state as output. It is defined by a "map", $x_1 = f(x_0)$ where x_0 is the initial state at time $t = 0$ and x_1 is the first state resulting from x_0. The other type is the continuous–time dynamical system [10, 26, 29]. It is the limit of discrete systems with smaller updating times and the rule becomes a set of differential equations. It is defined by a "flow", $x(t) = f^t(x_0)$.

In the next two subsections, we will investigate discrete dynamical systems. These systems evolve through a series of discrete steps in time, and not continuously, in contrast to the continuous dynamical systems which we will deal with in the following subsection.

1.2.1 Basic definitions

Discrete dynamical systems evolve through time by the process of iteration, where the subsequent state of the system is determined by its present state. For example, consider a one dimension dynamical system whose state is given by the variable x where an updated value of x is produced solely from its present value, i.e., the value of x at a subsequent time (n+1) is a function only of its present state at time n, $x_{n+1} = f(x_n)$, where f maps the present value of x at time n to the next value at time n+1. The repeated iteration of relatively simple equations of this form may lead to both simple and complex model behaviors. We will observe some of the rich variety of behaviors that iterative processes may produce.

1.2.2 Discrete Dynamical Systems

Map is a function whose domain space (input space) and range space (output space) are the same. A map describes the time evaluation of a system by expressing its current state as a function of its previous state.

The **orbit** is defined as the sequence of values that satisfy the equation $x_n = f^n(x_0)$. Put simply the orbit of a point x_0 under a map f is the set of points $\{x_0, x_1, x_2, \ldots\}$, where the starting value x_0 is the initial value of the orbit.

There are different types of orbits:

The **fixed orbit**: Let us at first mention the definition of a **fixed point** (f. p.) as follows: p is a said to be a fixed point of a map f, if $p = f(p)$ (i.e., a point that is

mapped into itself); e.g., for $f(x) = x^2$, $x = 0$ and $x = 1$ is a fixed point. The fixed orbit is exhibited by x_0 that satisfies $x_0 = f(x_0)$. If the orbit converges to a fixed point, it will remain constant. As an example of the fixed orbit, with $f(x) = x^2$, 1 is a fixed point whose orbit is {1, 1, 1, …}.

The **eventually fixed orbit**: it is the orbit which becomes fixed after n iterations. For example, with $f(x) = x^2$, –1 is an eventually fixed point whose orbit is {-1, 1, 1, …}.

The **periodic orbit**: Let f be a map on $\mathcal{R}$, p is **period point** of period k if $f^k(p) = p$ and k is the smallest such integer. This type of orbit is shown by x_0 values that satisfy the equation $x_0 = f^n(x_0)$ where n is any positive integer. The lowest possible n for such an orbit is called the prime period of the orbit. If an orbit is prime period n, it can also be referred to as a period n orbit. An example of period 2 orbit, with $f(x) = x^2 - 1$, using –1 as x_0; the orbit is {–1, 0, –1, 0, …} , alternating between –1 and 0.

The **eventually periodic orbit**: as with eventually fixed orbits, eventually periodic points do not start off as periodic; however, after n iterations, their orbits become periodic. An example of an eventually periodic point can be seen in $f(x) = 1 - x^2$, using –1 as x_0; the orbit is {–1, 1, 0, 1, 0, 1, …}.

The **chaotic orbits**: these are of points that do not fit into any of the above categories, and they behave randomly. For example, the orbit of $x_0 = 0.4$ on $f(x) = 4x(1-x)$ is given by {0.4, 0.96, 0.1536, 0.9983954, 0.00640793, …}

The **Cobweb plot** or the **Graphical iteration** is a rough plot of an orbit for a map of real line. In which, we sketch the function f together with diagonal line $y = x$ (45^o line), at any intersection of $y = f(x)$ with the line $y = x$, the input x and the output $f(x)$ are identical for x, which is a fixed point. It will be discussed in the following sections.