

People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
UNIVERSITY MOHAMED KHIDER, BISKRA
FACULTY of EXACT SCIENCES and NATURAL and LIFE SCIENCES
DEPARTMENT OF MATHEMATICS



Dissertation Submitted in Partial Execution of the
Requirements of the Degree of

Master in "Applied Mathematics"

Option: *Analysis*

Submitted and Defended By

TERKI Hania

Title :

Self Excited and Hidden Attractors

Jury Committee Members :

Dr. CHEMCHAM Madani	UMKB	President
Pr. MENACER Tidjani	UMKB	Supervisor
Dr. GHEDJEMIS Fatiha	UMKB	Examiner

18 June 2023

Dedicace

I dedicate this Master's thesis to my dear father and my beloved mother

To each of my brothers, and to my family

To all my friends and colleagues

To Department of Mathematics and its doctors and professors.

THANKS

To begin with, I want to express my thanks and gratitude to **Allah** for giving me the courage and strength to do this simple work.

I would like to thank my supervisor **Pr.MENACER Tidjani**, for giving me the opportunity to work on this project, for his great scientific and moral support, and for the suggestions and encouragement he gave me during my project. Carrying out my thesis under his supervision was a great honor and a real pleasure for me.

My sincere thanks to the jury members **Dr.CHEMCHAM Madani** and **Dr.GHEDJEMIS Fatiha** who agreed to judge my work.

I extend my sincere gratitude to all of the teachers in our department who have consistently given their all to give us a top-notch education. And also, all thanks to the administrative staff of the department.

Many thanks also to **Mr.Vladimir Vagaytsev**, who supported me by obtaining important information on this subject.

I want to express my sincere and great thanks to all the members of my small and large family and to all my friends for their support and encouragement.

Contents

Dedicace	i
THANKS	ii
Table of Contents	iii
List of Figures	vi
List of Tables	vii
Introduction	1
1 Dynamical Systems and Chaos	3
1.1 Dynamical System	3
1.2 Definition of Dynamical System	3
1.3 Classification of Dynamical Systems	4
1.4 Examples of Dynamical Systems	6
1.5 Flows	7
1.6 Equilibrium Point	7
1.6.1 Equilibrium Points of Continuous Dynamical System:	7
1.6.2 Fixed Points of Discrete Dynamical System:	8
1.7 The Stability	8
1.7.1 Stability in the sense of Lyapunov:	8

1.7.2	The asymptotically stability	9
1.7.3	The exponentially stability	9
1.8	Theory of Bifurcations	9
1.9	Attractors	10
1.9.1	Types of Attractors	10
1.10	Chaos	11
1.10.1	Characteristics of Chaos	13
2	Self Excited and Hidden Attractors	14
2.1	Self-Excited Attractors	15
2.2	Hidden Attractors	16
2.2.1	Analytical–numerical procedure for hidden attractors localization	16
2.2.2	Hidden Attractor Localization in Chua’s System	22
3	Application:Chaos-Based Cryptographic	29
3.1	Various kinds of multistability behaviors	32
3.2	Chaos-based PRNG	32
3.2.1	What is the PRNG?	32
3.2.2	Lyapunov exponents and Kaplan-Yorke dimension	34
3.2.3	Sample Entropy	35
	Conclusion	38
	Bibliography	39
	Annex :Program in MATLAB	41
3.3	Lorenz System	41
3.4	MACS System	41

Annex B: Abbreviations and Notation

43

List of Figures

1.1 Chaotic Attractor of Lorenz	12
2.1 ALGORITHM FOR LOCALIZING CHUA ATTRACTORS	27
2.2 Equilibria, saddles manifolds, hidden attractor localization.	28
3.1 Two coexisting attractors of case 1	31
3.2 Three coexisting attractors of case 1	32
3.3 Three coexisting attractors of case 1	33
3.4 Four coexisting attractors of case 2	33
3.5 Two coexisting chaotic attractors of case 3	34
3.6 The flowchart of generating PRNG	37

List of Tables

1.1 Classification of Dynamical Systems	6
3.1 Details of the attractors shown in figs	35

Introduction

Dynamical systems have received great attention because of their wide applications in the real world in various fields. These systems can range from simple models of physical systems, such as the motion of a pendulum, to more complex models of biological, chemical, and ecological systems.

One of the fundamental concepts in the study of dynamical systems is attractors. The study of attractors in dynamical systems has a long and rich history, dating back to the early 20th century. Attractors were initially studied in the context of simple linear systems, and they were found to exhibit stable, predictable behavior.

In the latter half of the 20th century, researchers began to study more complex nonlinear systems, and they discovered that these systems could exhibit much more complex and interesting behavior. The most prominent of which is the Lorenz system proposed by him in 1963, which opened the door to the study of chaotic systems. We can classify chaotic attractors into two categories: self-excited attractors and hidden attractors.

Self-excited attractors were first discovered in the 1970s by the mathematician Anatoly Zhabotinsky, who was studying a chemical reaction system known as the Belousov-Zhabotinsky reaction. Zhabotinsky observed that the system exhibited spontaneous oscillations, which he hypothesized were due to the presence of a self-excited attractor. This was a surprising result, as self-excited attractors were not thought to exist in chemical systems at the time.

In the 1990s, researchers began to study the phenomenon of hidden attractors. Hidden

attractors were discovered in a variety of nonlinear systems, including electronic circuits, biological models, and mechanical systems.

The study of self-excited and hidden attractors has since become an active and rapidly evolving field of research, with applications in a wide range of areas, including chaos-based cryptography and secure communications.

We will divide our work into three chapters. **The first chapter** summarizes general concepts about dynamic systems, such as types of dynamic systems, stability, bifurcations, and flows, and then we will define attractors and chaos as a prelude to the second chapter. The subject's main focus is in **the second chapter**, in which we will address the definition and examples of each of the self-excited and hidden attractors. We will also introduce the analytical-numerical procedure for hidden attractors localization, we will support it with a numerical example titled "Hidden Attractor Localization in Chua's System".

One of the popular applications of our topic is cryptography, which is a new application under development. That is why, in **chapter three** we will highlight the applications of attraction analysis in the field of cryptography.

We will study the sensitivity of the initial values and parameters of the three-dimensional system known as the multi-attribute chaotic system (MACS), we will use this system to generate PRNG, and we will finally check its effectiveness if it passes all the statistical tests.

Chapter 1

Dynamical Systems and Chaos

1.1 Dynamical System

Dynamical systems are our models of reality; they are how we describe the world around us, especially how things change and coevolve in time, so dynamical systems are fundamentally linked to time and how systems change in time.

They are our models for the evolving world around us, so they describes the rich behavior of maxing fluids; and how we build models that we would use to design rockets and land them; we use dynamical systems to understand the brain disease networks; and social networks.

1.2 Definition of Dynamical System

Definition 1.2.1 *A dynamical system is a mathematical formalization for any fixed rule which describes the dependence of the position of a point in some ambient space on a parameter.* [3]

Let $\mathbf{x} = \mathbf{x}(t) \in \mathbb{R}^n$ and $t \in I \subseteq \mathbb{R}$.

The dynamic system is usually written in the following form

$$\frac{d\mathbf{x}}{dt} = f(\mathbf{x}, t, \mu), \quad (1.1)$$

where $f(\mathbf{x}, t, \mu)$ is sufficiently smooth function defined on some subset $\mathbb{R}^n \times \mathbb{R} \times \mathbb{R}^m$. The variable t is interpreted as time, and the function $f(\mathbf{x}, t, \mu)$ is generally nonlinear. The variable μ is vector of parameters.

1.3 Classification of Dynamical Systems

Dynamical system can be:

1. **Discrete Dynamical System:** The rule is applied at discrete times (the natural numbers \mathbb{N} or the integers \mathbb{Z}). The system is typically specified by a set of equations, such as difference equations (or maps). In this case, the dynamical system can be solved by iterative calculation.

In other words

$$\mathbf{x}_{n+1} = f(\mathbf{x}_n) = f(f(\mathbf{x}_{n-1})) = \dots$$

In the form

$$\mathbf{x}_{n+1} = f(\mathbf{x}_n) = f^2(\mathbf{x}_{n-1}) = \dots$$

2. **Continuous Dynamical System:** Is essentially the limit of discrete systems with smaller and smaller updating times Δt ($t \in I \subseteq \mathbb{R}$), it is represented by differential equations.

The continuous system written as

$$\frac{d\mathbf{x}}{dt} = \dot{\mathbf{x}} = f(\mathbf{x}, t), \quad \mathbf{x} \in \mathbb{R}^n, t \in \mathbb{R}.$$

3. **Linear Dynamical System:** The function f must satisfy two properties: additivity ($f(\mathbf{x} + \mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y})$) and homogeneity ($f(a\mathbf{x}) = af(\mathbf{x})$).
4. **Nonlinear Dynamical System:** Is described by a nonlinear function. It does not satisfy the previous basic properties. Nonlinear systems are harder to solve than linear systems. They are important in describing phenomena; examples include physical science, biology, ecology, and chemistry.
5. **Deterministic Dynamical System:** Is one which behavior is entirely predictable (its entire future course and its entire past are uniquely determined by its state at the present time).[\[6\]](#)
6. **Stochastic Dynamical System:** Is one in which behavior cannot be entirely predicted; it's also called non deterministic.

There is another type called a semi-deterministic dynamical system (determined but not uniquely).

7. **Autonomous Dynamical System:** The right-hand side of the equation [\(1.1\)](#) is explicitly time independent, for example

$$\alpha\dot{x} + \beta x = 0, \quad \alpha, \beta > 0.$$

8. **Nonautonomous Dynamical System:** The right-hand side of the equation [\(1.1\)](#) is explicitly time dependent, for example

$$\alpha\dot{x} + \beta x = f \cos(\omega t), \quad \alpha, \beta > 0,$$

where f is amplitude of driving force, and ω is frequency of driving force.

Either	Or
Discrete	continuous
Linear	Nonlinear
Deterministic	Stochastic
Autonomous	Nonautonomous

Table 1.1: Classification of Dynamical Systems

Remark 1.3.1 *We will take care of our studies with continuous, deterministic and non-linear dynamical systems.*

1.4 Examples of Dynamical Systems

- Ordinary Differential Equations: This is the general form of the ordinary differential equation

$$\dot{x} = f(x, t)$$

$$\dot{x} = \frac{tx^2}{3} = f(x, t), \quad \text{is non-autonomous}$$

$$\dot{x} = \frac{x}{3} = f(x), \quad \text{is autonomous}$$

- The free pendulum: The pendulum is usually subject to gravity, with an acceleration g . The gravitational force is pointing vertically downward with strength mg and has a component $-mg \sin \varphi$ along the circle described by the point mass. Here φ is the deflection, the distance of the point mass from the "rest position" ($\varphi = 0$), measured along the circle of all its possible positions, then is $l\varphi$.

So, the equation of motion of the pendulum is:

$$\varphi'' = -\frac{g}{l} \sin \varphi.$$

This means that the evolutions are given by the functions $t \mapsto \varphi(t)$ that satisfy the

equation of motion of the pendulum. [2]

1.5 Flows

Consider the dynamical system:

$$\dot{\mathbf{x}} = f(x, t) \quad \mathbf{x} \in U \subseteq \mathbb{R}^n, t \in I \subseteq \mathbb{R}. \quad (1.2)$$

The flow of (1.2) is defined by $\phi_t(\mathbf{x}) : U \rightarrow \mathbb{R}^n$, where $\phi_t(\mathbf{x}) = \phi(t, \mathbf{x})$ is a smooth vector function of $\mathbf{x} \in U \subseteq \mathbb{R}^n$ and $t \in I \subseteq \mathbb{R}$ satisfying the equation:

$$\frac{d}{dt}\phi_t(\mathbf{x}) = f(\phi_t(\mathbf{x}), t),$$

for all t such that the solution through \mathbf{x} exists and $\phi(0, \mathbf{x}) = \mathbf{x}$. [6]

1.6 Equilibrium Point

The equilibrium points of a system play an important role in describing the properties of the system, they are also known as a critical point, a fixed point, or a stationary point.

1.6.1 Equilibrium Points of Continuous Dynamical System:

A point is an equilibrium point of the flow generated by an autonomous system

$\dot{\mathbf{x}} = f(\mathbf{x}), \mathbf{x} \in \mathbb{R}^n$ if and only if $\phi(t, \mathbf{x}) = \mathbf{x}$ for all $t \in \mathbb{R}$. Consequently, in a continuous system, this gives $\dot{\mathbf{x}} = 0 \Rightarrow f(\mathbf{x}) = 0$.

For nonautonomous systems equilibrium point can be defined for a fixed time interval.

Flows on a line may have no fixed points ($\dot{x} = 4$), only one fixed point ($\dot{x} = x + 3$), finite number of fixed points ($\dot{x} = x^2 - 1$, two fixed points), or an infinite number of fixed points ($\dot{x} = \sin x$). [6]

1.6.2 Fixed Points of Discrete Dynamical System:

Consider a discrete dynamical system

$$\mathbf{x}_{k+1} = f(\mathbf{x}_k), k \in \mathbb{Z},$$

a is called fixed point if:

$$a = f(a).$$

For example:

$$\mathbf{x}_{k+1} = r\mathbf{x}_k, k \in \mathbb{Z},$$

to find the fixed points we solve the following equation:

$$a = ra,$$

$$a(1 - r) = 0,$$

$$\begin{cases} r \neq 1 & a = 0 \text{ (only one fixed point)} \\ r = 1 & 0 \times a = 0 \text{ (infinite number of fixed points)} \end{cases}$$

1.7 The Stability

The question of stability is significant because a real-world system is constantly subject to small perturbations. Stability means that the system does not change too much under small perturbations. Therefore, a steady state observed in a realistic system must correspond to a stable fixed point.

1.7.1 Stability in the sense of Lyapunov:

A fixed point, say \mathbf{x}_0 is said to be stable in the sense of Lyapunov if for a given $\varepsilon > 0$, there exists a $\delta > 0$ depending upon ε such that for all $t > t_0$, $\|\mathbf{x}(t) - \mathbf{x}_0(t)\| < \varepsilon$, whenever

$\|\mathbf{x}(t_0) - \mathbf{x}_0(t_0)\| < \delta$, where $\|\cdot\| : \mathbb{R}^n \rightarrow \mathbb{R}$ denotes the norm of a vector in \mathbb{R}^n . Otherwise, the fixed point is called unstable.

1.7.2 The asymptotically stability

\mathbf{x}_0 is said to be asymptotically stable in the sense of Lyapunov if it is Lyapunov stable and $\lim_{t \rightarrow \infty} \|\mathbf{x}(t) - \mathbf{x}_0(t)\| = 0$.

1.7.3 The exponentially stability

\mathbf{x}_0 is said to be exponentially stable in the sense of Lyapunov if it is asymptotically stable and there exist $\alpha, \beta > 0$, $\|\mathbf{x}(t) - \mathbf{x}_0(t)\| \leq \alpha \|\mathbf{x}(t_0) - \mathbf{x}_0(t_0)\| e^{-\beta t}$, for all $t \geq 0$.

1.8 Theory of Bifurcations

The name "bifurcation" was first introduced by the French mathematician Henri Poincaré in 1885. Bifurcation theory is a useful and widely studied subfield of dynamical systems [\[1\]](#)

In dynamical systems, a bifurcation occurs when a small smooth change made to the parameter values of a system causes a sudden "qualitative" or topological change in its behavior.

The study of bifurcation is concerned with how structural change occurs when the parameter(s) are changing. The point at which bifurcation occurs is known as the bifurcation point. The diagram of the parameter values versus the fixed points of the system is known as the bifurcation diagram. It's very useful in understanding the dynamical behavior of a system.

Bifurcations associated with a single parameter are called 1-codimension bifurcations, and bifurcations associated with two parameters are known as 2-codiemension bifurcations. [\[6\]](#)

1.9 Attractors

Now we turn to an important part of dynamical systems, the "attractor".

In 1963, Edward Lorenz studied and simplified a remarkable system of three differential equations, which represented a flow in three-dimensional space:

$$\begin{cases} \frac{dx}{dt} = a(y - x), \\ \frac{dy}{dt} = x(b - z) - y, \\ \frac{dz}{dt} = xy - cz. \end{cases}$$

The divergence of the flow has a constant negative value, so that any volume shrinks exponentially with time. Moreover, there exists a bounded region in \mathbb{R}^3 into which every trajectory becomes eventually trapped. Therefore, all trajectories tend to a set of measure zero, called attractors.

At first, the Lorenz system was used to treat weather prediction phenomena, and it was developed later by Lanford (1975) and Pomeau (1976), and it has become widely used and has many applications in reality.

Definition 1.9.1 *Attractors are portions or subsets of the phase space of a dynamical system towards which the system tends to evolve towards it, whatever it's starting conditions.*

1.9.1 Types of Attractors

There are three states of attractors:

Fixed-point Attractor

A fixed point attractor is the simplest state of an attractor. This attractor is represented by a particular point in phase space.

A fixed point attractor is classified as a regular attractor, and it corresponds to a very limited range of possible behaviors of the system.

Periodic Attractor

Also called a limit cycle attractor, it consists of a periodic movement between two or more values.

Moreover, periodic attractor is also classified as a regular attractor. Compared to the fixed point attractor, it represents more possibilities for the behavior of the system.

Strange Attractor

The term strange attractor was coined by David Ruelle and Floris Takens in 1971 in their article entitled "On the Nature of Turbulence" (to describe the attractor resulting from a series of bifurcations of a system describing fluid flow).

Strange attractors are more complicated than others, we have now moved on to the chaotic attractors.

Strange attractors are complex geometric shapes that characterize the evolution of chaotic systems. After a period of time, all points in the phase space (which belong to the basin of attraction to the attractor) give trajectories that tend to form the strange attractor.

The strange attractor has the following properties:

1. It shows sensitivity to initial conditions.
2. The dimensions of the attractor are fractal, not integer.

1.10 Chaos

Back to meteorologist Edward Lorenz, who first described the chaotic motion in atmospheric flows in the year 1963. When plotting the solution structure in a three-dimensional Euclidean space, we see that it resembles the surface of two wings of a butterfly, known as a strange attractor with fractional dimension.

The sensitive dependence of dynamical evolution on an infinitesimal change of initial conditions is called "the butterfly effect". In 1972, Lorenz wondered about the butterfly effect: "Does the flap of a butterfly's wings in Brazil set off a tornado in Texas?", and he said that it was difficult to predict the long-range climate conditions correctly. Then he summed up the concept of chaos with the following statement: "Chaos: When the present determines the future, but the approximate present does not approximately determine the future."

Chaotic nonlinear dynamics is of great importance in the current era, as it has wide applications in computer science, physics, chemistry, biology, and industry... Chaos theory received great attention in the twentieth century. Scientists at the time defined it as follows: "Chaos is the unpredictability".

Numerical localization of chaotic attractor in Lorenz system

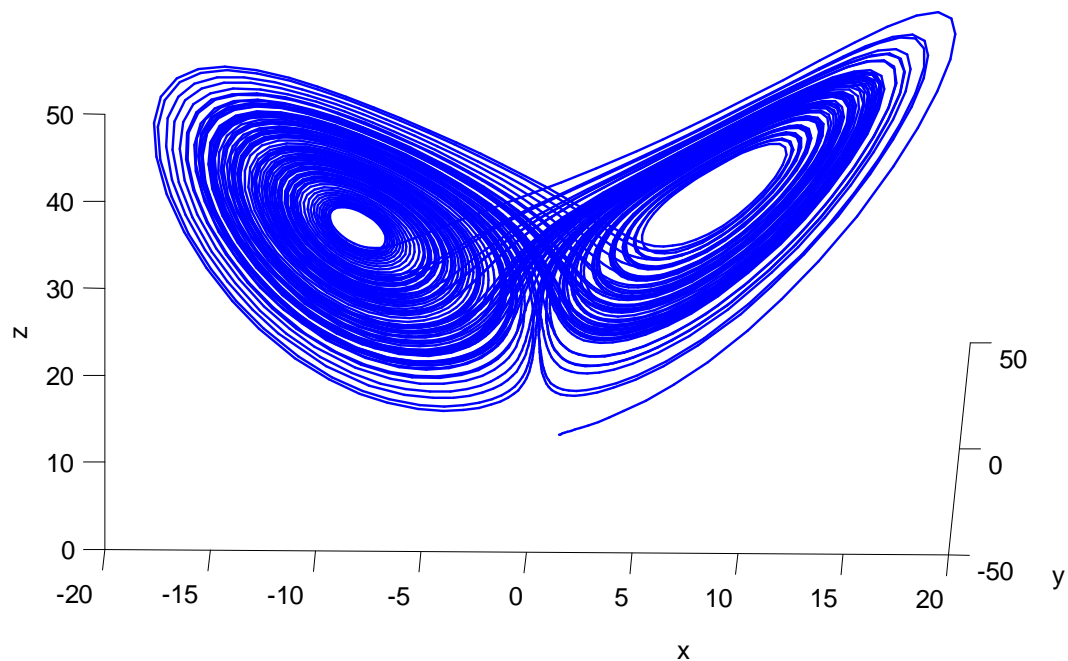


Figure 1.1: Chaotic Attractor of Lorenz

Definition 1.10.1 *There is still no valid definition of chaos, but we can say that it is the study of systems that have a very complex evolution.*

1.10.1 Characteristics of Chaos

Among the most important characteristics of chaos are the following:

1. **The nonlinearity:** A chaotic system is a nonlinear dynamical system. The system is linear, it cannot be chaotic.
2. **The sensitivity to the initial conditions:** A small change in the initial conditions of a system can lead to radically different behavior in its final state.
3. **The unpredictable:** This is due to sensitivity to initial conditions.
4. **Strange attractor:** We defined it earlier.
5. **The determinism:** Although the time evolution obeys strict deterministic laws, the system seems to behave according to its own free will. [\[6\]](#)
6. **The Fractal Structure:** There are connections with chaos and fractal objects.

Chapter 2

Self Excited and Hidden Attractors

The theory of nonlinear dynamical systems is one of the fastest growing branches of applied mathematics. After Lorenz proposed the first simple three-dimensional chaotic system, chaos theory categorized itself as an important branch of nonlinear dynamics, it has a broad range of applications in chemistry, ecology, secure communication systems, image and sound encryption, etc.

We can classify chaotic attractors into two categories: self-excited attractors and hidden attractors.

In April 1992, a fighter jet crashed while descending. The cause of the crash was a flight control software error that failed to prevent a pilot-induced oscillation. Despite the fact that the pilot was not injured, a crash like this revealed the fundamental requirement to investigate such peculiar oscillations in the aircraft's control system. Such attractors are generally known as hidden attractors.

In 2010, the two scientists Kuznetsov and Leonov presented their research on finding a chaotic hidden attractor in a generalized circle of Chua (for the first time), followed by the discovery of a chaotic hidden attractor in a classical circle of Chua in 2011 (by the scientist Leonov's). Hidden attractants were later found in Lorenz type systems, chaotic flows, and others.

So what is the definition of both self-excited and hidden attractants? And how are hidden attractants found?

2.1 Self-Excited Attractors

Definition 2.1.1 *An attractor is called a self-excited attractor if its basin of attraction intersects with any open neighborhood of an unstable equilibrium point.* [13]

Self-excited attractors can be localized numerically by a standard computational procedure, in which, after a transient process, a trajectory started from a point of unstable manifold in the neighborhood of equilibrium, reaches an attractor and identifies it.

Consider classical examples of visualization of self-excited oscillations:

Example 2.1.1 *[Rayleigh's string oscillator]*

In 1990, Rayleigh discovered that in a two-dimensional nonlinear dynamical system can arise undamped vibrations without external periodic action (limit cycles).

Consider the localization of the limit cycle in the Rayleigh system

$$\ddot{x} - (a - b\dot{x}^2)\dot{x} + x = 0,$$

for $a = 1, b = 0.1$, a limit cycle is localized by two trajectories, attracting to the limit cycle.

Example 2.1.2 *[Lorenz system]*

Consider Lorenz system

$$\begin{cases} \frac{dx}{dt} = a(y - x), \\ \frac{dy}{dt} = x(b - z) - y, \\ \frac{dz}{dt} = xy - cz. \end{cases}$$

For classical parameters $a = 10, b = \frac{8}{3}, c = 28$, the Lorenz attractor is self-excited with respect to all three equilibria and could have been found using the standard computational procedure.

2.2 Hidden Attractors

Definition 2.2.1 *Hidden attractors have a basin of attraction that does not intersect with any open neighborhoods of equilibria.* [11]

Remark 2.2.1 *From a computational point of view, hidden attractors can be classified into three categories: hidden attractors with stable equilibrium points, hidden attractors with no equilibrium points, and hidden attractors with infinitely many equilibrium points.*

2.2.1 Analytical–numerical procedure for hidden attractors localization

The following stages are a description of the algorithm used to detect hidden attractors in Leonov’s works:

Step 1

Consider the system

$$\frac{d\mathbf{x}}{dt} = M\mathbf{x} + q\psi(r^T\mathbf{x}), \mathbf{x} \in \mathbb{R}^n, \quad (2.1)$$

where M is a constant $n \times n$ -matrix, q, r are constant n -dimensional vectors, $\psi(\sigma)$ is a piecewise-continuous scalar function, and $\psi(0) = 0$.

Step 2

Define a coefficient of harmonic linearization h in such a way that the matrix (suppose that such h exists)

$$M_0 = M + hqr^T, \quad (2.2)$$

has a pair of purely imaginary eigenvalues $\pm i\omega_0$ ($\omega_0 > 0$) and the rest of its eigenvalues

have negative real parts. Then system (2.1) can be rewritten as

$$\frac{d\mathbf{x}}{dt} = M_0\mathbf{x} + q\varphi(r^T\mathbf{x}), \quad (2.3)$$

where $\varphi(\sigma) = \psi(\sigma) - h\sigma$.

Step 3

Introduce a finite sequence of functions $\varphi^0(\sigma), \varphi^1(\sigma), \dots, \varphi^m(\sigma)$ in such a way that the graphs of neighboring functions $\varphi^j(\sigma)$ and $\varphi^{j+1}(\sigma)$ slightly differ from one another ($j = 0, \dots, m - 1$), the function $\varphi^0(\sigma)$ is small, and $\varphi^m(\sigma) = \varphi(\sigma)$.

Taking into account the smallness of the function $\varphi^0(\sigma)$ we can use and justify mathematically strictly the method of harmonic linearization (the describing function method) for the system

$$\frac{d\mathbf{x}}{dt} = M_0\mathbf{x} + q\varphi^0(r^T\mathbf{x}), \quad (2.4)$$

and determine a stable nontrivial periodic solution $\mathbf{x}^0(t)$. Then for the localization of an attractor of the original system (2.3) we shall numerically follow the transformation of this periodic solution with increasing j . All the points of this stable periodic solution are located in the domain of attraction of the stable periodic solution $\mathbf{x}^1(t)$ of the system

$$\frac{d\mathbf{x}}{dt} = M_0\mathbf{x} + q\varphi^j(r^T\mathbf{x}), \quad (2.5)$$

with $j = 1$, or when passing from (2.4) to system (2.5) with $j = 1$, we observe the instability bifurcation destroying periodic solution. It is possible to find $\mathbf{x}^1(t)$ numerically in the first case, starting a trajectory of system (2.5) with $j = 1$ from the initial point $\mathbf{x}^0(0)$.

Starting from the initial point, after the transient process, the computational procedure reaches the periodic solution $\mathbf{x}^1(t)$ and computes it (here it should be considered a suffi-

ciently large computational interval $[0, T]$).

After the computation of $\mathbf{x}^1(t)$ it is possible to obtain a periodic trajectory $\mathbf{x}^2(t)$ of system (2.5) with $j = 2$ starting from the initial point $\mathbf{x}^2(0) = \mathbf{x}^1(T)$.

Proceeding this procedure and computing $\mathbf{x}^j(t)$, using the trajectories of system (2.5) with the initial data $\mathbf{x}^j(0) = \mathbf{x}^{j-1}(T)$. Or observe, at a certain step, the instability bifurcation destroying the periodic solution.

It turns out that for system (2.4) with such function $\varphi^0(\sigma)$, it is possible to justify rigorously the method of harmonic linearization and to determine the initial conditions under which system (2.4) has a stable periodic solution that is close to the harmonic one.

Step 4 (System reduction)

To define the initial point $\mathbf{x}^0(0)$ of starting periodic solution, the system (2.4) with the nonlinearity $\varphi^0(\sigma)$ is transformed by a linear nonsingular transformation $\mathbf{x} = HY$ to the form

$$\begin{aligned} \dot{y}_1 &= -\omega_0 y_2 + v_1 \varphi^0(y_1 + u_3^T Y_3), \\ \dot{y}_2 &= \omega_0 y_1 + v_2 \varphi^0(y_1 + u_3^T Y_3), \\ \dot{Y}_3 &= A_3 Y_3 + V_3 \varphi^0(y_1 + u_3^T Y_3). \end{aligned} \tag{2.6}$$

Here y_1, y_2 are scalars, Y_3 is $(n - 2)$ -dimensional vector; V_3 and u_3 are $(n - 2)$ -dimensional vectors, v_1 and v_2 are real numbers; A_3 is an $((n - 2) \times (n - 2))$ - matrix, all eigenvalues of which have negative real parts. Without loss of generality, it can be assumed that for the matrix A_3 there exists a positive number $d > 0$ such that

$$Y_3^T (A_3 + A_3^T) Y_3 \leq -2d |Y_3|^2, \quad \forall Y_3 \in \mathbb{R}^{n-2}. \tag{2.7}$$

Let us present a transfer function of system (2.4)

$$W_1(p) = r^T(M_0 - pI)^{-1}q = \frac{\eta p + \theta}{p^2 + \omega_0^2} + \frac{R(p)}{Q(p)}, \quad (2.8)$$

and the transfer function of system (2.6):

$$W_2(p) = \frac{-v_1 p + v_2 \omega_0}{p^2 + \omega_0^2} + u_3^T(A_3 - pI)^{-1}V_3. \quad (2.9)$$

Here η and θ are certain real numbers, $Q(p)$ is a stable polynomial of degree $(n - 2)$, $R(p)$ is a polynomial of degree smaller than $(n - 2)$. Suppose, the polynomials $Q(p)$ and $R(p)$ have no common roots.

From the equivalence of systems (2.4) and (2.6), it follows that the transfer functions of these systems coincide.

This implies the following relations

$$\eta = -v_1,$$

$$\theta = v_2 \omega_0,$$

$$u_3^T V_3 + v_1 = r^T q,$$

$$\frac{R(p)}{Q(p)} = u_3^T (A_3 - pI)^{-1} V_3.$$

Step 5 (Poincaré map for harmonic linearization in the noncritical case)

Consider system (2.6) with nonlinearity $\varphi^0(\sigma) = \varepsilon\varphi(\sigma)$ (ε is classical small positive parameter)

$$\begin{aligned} \dot{y}_1 &= -\omega_0 y_2 + v_1 \varepsilon \varphi(y_1 + u_3^T Y_3), \\ \dot{y}_2 &= \omega_0 y_1 + v_2 \varepsilon \varphi(y_1 + u_3^T Y_3), \\ \dot{Y}_3 &= A_3 Y_3 + V_3 \varepsilon \varphi(y_1 + u_3^T Y_3), \end{aligned} \quad (2.10)$$

where $\varphi(\sigma)$ is a piecewise-differentiable function with discontinuity points v_i .

Introduce the following description function

$$\phi(a) = \int_0^{2\pi/\omega_0} \varphi(\cos(\omega_0 t) a \cos(\omega_0 t)) dt. \quad (2.11)$$

The existence of a derivative of the describing function results in the following:

Theorem 2.2.1 [8] *Suppose that there exists a number $a_0 > 0$, $a_0 \neq |v_i|$ such that the conditions*

$$\phi(a_0) = 0, \quad v_1 \left. \frac{d\phi(a)}{da} \right|_{a=a_0} < 0$$

are satisfied. Then for sufficiently small $\varepsilon > 0$ system (2.10) has a periodic solution of the form

$$\begin{aligned} y_1(t) &= \cos(\omega_0 t) y_1(0) + O(\varepsilon), \\ y_2(t) &= \sin(\omega_0 t) y_1(0) + O(\varepsilon), \quad t \in [0, T] \\ Y_3(t) &= \exp(A_3 t) Y_3(0) + O_{n-2}(\varepsilon), \end{aligned}$$

with the initial data

$$y_1(0) = a_0 + O(\varepsilon),$$

$$y_2(0) = 0,$$

$$Y_3(0) = O_{n-2}(\varepsilon),$$

and with the period

$$T = \frac{2\pi}{\omega_0} + O(\varepsilon).$$

Here $O_{n-2}(\varepsilon)$ is an $(n - 2)$ -dimensional vector such that its components are $O(\varepsilon)$.

Corollary 2.2.1 [8] Suppose that there exists a number $a_0 > 0$, $a_0 \neq |v_i|$ such that the conditions

$$\phi(a_0) = 0, \quad \eta \left. \frac{d\phi(a)}{da} \right|_{a=a_0} > 0 \quad (\text{because } \eta = -v_1)$$

are satisfied. Then, for a sufficiently small $\varepsilon > 0$ system (2.4) with transfer function (2.8) and the nonlinearity $\varphi^0(\sigma) = \varepsilon\varphi(\sigma)$ has a T -periodic solution such that

$$r^T \mathbf{x}(t) = a_0 \cos(\omega_0 t) + O(\varepsilon),$$

$$T = \frac{2\pi}{\omega_0} + O(\varepsilon).$$

The previous theorem describes the procedure of the search for stable periodic solutions by the standard describing function method.

2.2.2 Hidden Attractor Localization in Chua's System

Consider the following smooth Chua's system

$$\begin{cases} \dot{x} = \alpha(y - x) - \alpha f(x), \\ \dot{y} = x - y + z, \\ \dot{z} = -(\beta y + \gamma z), \end{cases}$$

here the function

$$f(x) = m_1 x + (m_0 - m_1) \text{sat}(x), \quad \text{sat}(x) = \frac{1}{2}(|x + 1| - |x - 1|),$$

$$f(x) = m_1 x + \frac{1}{2}(m_0 - m_1)(|x + 1| - |x - 1|),$$

is called Chua's diode; it describes a nonlinear element of system.

$m_0, m_1, \alpha, \beta, \gamma$ are parameters of the classical Chua's system.

Write Chua's system in the form [\(2.1\)](#)

$$\frac{d\mathbf{x}}{dt} = M\mathbf{x} + q\psi(r^T\mathbf{x}), \quad \mathbf{x} \in \mathbb{R}^3, \quad (2.12)$$

Here

$$M = \begin{pmatrix} -\alpha(m_1 + 1) & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix},$$

$$q = \begin{pmatrix} -\alpha \\ 0 \\ 0 \end{pmatrix}, \quad r = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

$$\psi(\sigma) = (m_0 - m_1) \text{sat}(\sigma).$$

Introduce a coefficient h and a small parameter ε , and represent system (2.12) as

$$\frac{d\mathbf{x}}{dt} = M_0\mathbf{x} + q\varepsilon\varphi(r^T\mathbf{x}), \quad (2.13)$$

where

$$\begin{aligned} M_0 &= M + hqr^T \\ &= \begin{pmatrix} -\alpha(m_1 + 1) & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} + h \begin{pmatrix} -\alpha \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} -\alpha(m_1 + 1) & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} + h \begin{pmatrix} -\alpha & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} -\alpha(m_1 + 1 + h) & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix}, \end{aligned}$$

and

$$\begin{aligned} \lambda_{1,2}^{M_0} &= \pm i\omega_0, & \lambda_3^{M_0} &= -d, \\ \varphi(\sigma) &= \psi(\sigma) - h\sigma = (m_0 - m_1)\text{sat}(\sigma) - h\sigma. \end{aligned}$$

Using a nonsingular linear transformation $\mathbf{x} = HY$, it is possible to transform system

(2.13) into the form

$$\frac{dY}{dt} = AY + V\varepsilon\varphi(u^TY), \quad (2.14)$$

where

$$A = \begin{pmatrix} 0 & -\omega_0 & 0 \\ \omega_0 & 0 & 0 \\ 0 & 0 & -d \end{pmatrix}, \quad V = \begin{pmatrix} v_1 \\ v_2 \\ 1 \end{pmatrix}, \quad u = \begin{pmatrix} 1 \\ 0 \\ -\ell \end{pmatrix}.$$

The transfer function $W_A(p)$ of system (2.14) can be represented as

$$W_A(p) = \frac{-v_1 p + v_2 \omega_0}{p^2 + \omega_0^2} + \frac{\ell}{p + d}.$$

Then, using the equality of transfer functions

$$W_A(p) = r^T (M_0 - pI)^{-1} q$$

of system (2.13) and system (2.14), one can obtain

$$\begin{aligned} h &= \frac{-\alpha(m_1 + m_1\gamma + \gamma) + \omega_0^2 - \gamma - \beta}{\alpha(1 + \gamma)}, \\ d &= \frac{\alpha + \omega_0^2 - \beta + 1 + \gamma + \gamma^2}{1 + \gamma}, \\ \ell &= \frac{\alpha(\gamma + \beta - (1 + \gamma)d + d^2)}{\omega_0^2 + d^2}, \\ v_1 &= \frac{\alpha(\gamma + \beta - \omega_0^2 - (1 + \gamma)d)}{\omega_0^2 + d^2}, \\ v_2 &= \frac{\alpha((1 + \gamma - d)\omega_0^2 + (\gamma + \beta)d)}{\omega_0(\omega_0^2 + d^2)}. \end{aligned} \tag{2.15}$$

Since system (2.13) transforms into system (2.14) by nonsingular linear conversion

$\mathbf{x} = HY$, therefore, the matrix H satisfies the following equations

$$A = H^{-1}M_0H, \quad V = H^{-1}q, \quad u^T = r^T H. \tag{2.16}$$

Having solved these matrix equations, one can obtain the transformation matrix

$$H = \begin{pmatrix} s_{11} & s_{12} & s_{13} \\ s_{21} & s_{22} & s_{23} \\ s_{31} & s_{32} & s_{33} \end{pmatrix},$$

where

$$\begin{aligned} s_{11} &= 1, & s_{12} &= 0, & s_{13} &= -\ell, \\ s_{21} &= m_1 + 1 + h, & s_{22} &= -\frac{\omega_0}{\alpha}, \\ s_{23} &= -\frac{\ell(\alpha(m_1 + 1 + h) - d)}{\alpha}, \\ s_{31} &= \frac{\alpha(m_1 + h) - \omega_0^2}{\alpha}, \\ s_{32} &= -\frac{\alpha(\beta + \gamma)(m_1 + h) + \alpha\beta - \gamma\omega_0^2}{\alpha\omega_0}, \\ s_{33} &= \ell \frac{\alpha(m_1 + h)(d - 1) + d(1 + \alpha - d)}{\alpha}. \end{aligned}$$

For small enough ε one can obtain the initial data

$$\mathbf{x}(0) = HY(0) = H \begin{pmatrix} a_0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} a_0 s_{11} \\ a_0 s_{21} \\ a_0 s_{31} \end{pmatrix}.$$

For the determination of initial data of starting solution for multistage procedure, one can obtain

$$x(0) = a_0, \quad y(0) = a_0(m_1 + 1 + h), \quad z(0) = a_0 \frac{\alpha(m_1 + h) - \omega_0^2}{\alpha}. \quad (2.17)$$

Consider system (2.13) with the parameters

$$\begin{aligned}
 \alpha &= 8.4562, \\
 \beta &= 12.0732, \\
 \gamma &= 0.0052, \\
 m_0 &= -0.1768, \\
 m_1 &= -1.1468.
 \end{aligned}
 \tag{2.18}$$

Now let us apply the above procedure of hidden attractors localization to Chua's system (2.12) with parameters (2.18). For this purpose, compute a coefficient of harmonic linearization and a starting frequency:

$$h = 0.2098, \quad \omega_0 = 2.0392.$$

Then, compute solutions of system (2.13) with nonlinearity $\varepsilon\varphi(x) = \varepsilon(\psi(x) - h(x))$, sequentially increasing ε from the value $\varepsilon_1 = 0.1$ to $\varepsilon_{10} = 1$ with step 0.1.

By (2.15) and (2.17), the initial data can be obtained

$$x(0) = 9.4287, \quad y(0) = 0.5945, \quad z(0) = -13.4705,$$

for the first step of multistage procedure.

For $\varepsilon_1 = 0.1$ after the transient process, the computational procedure arrives at a periodic solution close to the harmonic one. Further, with increasing parameter ε this periodic solution close to the harmonic one is transformed into a chaotic attractor.

Additionally, the set a hidden is calculated for the original Chua's system (2.12) using

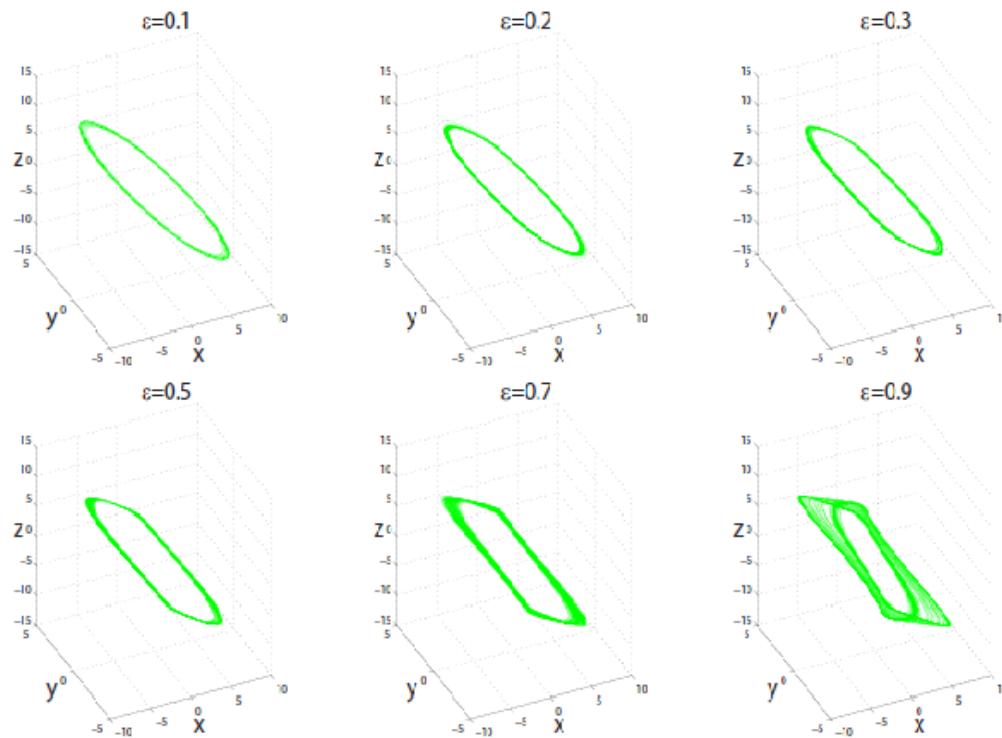


Figure 2.1: ALGORITHM FOR LOCALIZING CHUA ATTRACTORS

numerical methods and the sequential transformation $\mathbf{x}^j(t)$ with increasing parameter ε_j (figure 2.1).

The behavior of system trajectories in a neighborhood of equilibria is shown in figure 2.2). Here M_1^{st}, M_2^{st} are stable manifolds, M_1^{unSt}, M_2^{unSt} are unstable manifolds, F_0 is stable zero equilibrium, S_1, S_2 are two symmetric saddles, A_{hidden} is a hidden chaotic attractor (in green).

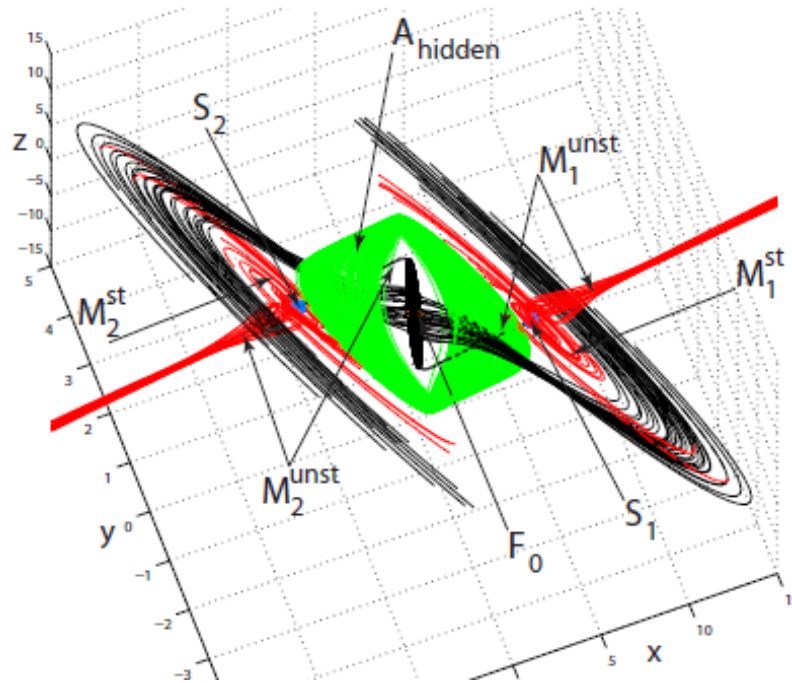


Figure 2.2: Equilibria, saddles manifolds, hidden attractor localization.

Chapter 3

Application: Chaos-Based Cryptographic

Researchers have focused a lot of effort on the localization and analysis of attractors in dynamical systems due to their wide possible application in various fields like cryptography, encryption, brain dynamics, the financial market, and many more.

In this chapter, we will highlight the applications of attraction analysis in the field of cryptography.

It has been observed in many recent studies that numerous properties of chaotic systems are similar to their counterparts in traditional cryptography. However, the sensitivity of the initial values and parameters of the chaotic systems used in cryptographic applications greatly influences the security levels of cryptographic schemes. Complex chaotic behaviors and high sensitivity to both initial values and parameters are characteristics of chaotic systems with coexisting attractors. These systems would therefore be appropriate for cryptography applications.

We now introduce a new simple 3D chaotic system, named the multi-attribute chaotic system (MACS).

Mathematically, it is defined as

$$\begin{cases} \frac{dx}{dt} = -y, \\ \frac{dy}{dt} = x + \delta yz, \\ \frac{dz}{dt} = \sigma |f(x)| - by^2 - az - \mu, \end{cases} \quad (3.1)$$

where x, y and z are the state variables, and $a, b, \delta, \sigma, \mu$ are the constant parameters of the system, and $|f(x)|$ is given by either $|\cos(x)|$ or $|\sin(x)|$ (nonlinear controller).

The system is rotationally symmetric under the transformation $(x, y, z) \longrightarrow (-x, -y, z)$.

- **Case 1** $a, b, \delta, \sigma > 0, \mu = 0$ and $|f(x)| = |\cos(x)|$.

The equilibria can be obtained by solving the equations:

$$\begin{cases} -y = 0, \\ x + \delta yz = 0, \\ \sigma |\cos(x)| - by^2 - az = 0. \end{cases} \quad (3.2)$$

From the equations (3.2), case 1 of MACS has only one equilibrium with the following form:

$$Eq_1(0, 0, \frac{\sigma}{a}).$$

Type of system: Self-excited attractor with one unstable hyperbolic equilibrium.

- **Case 2** $b, \delta, \sigma > 0, a = \mu = 0$ and $|f(x)| = |\cos(x)|$.

The equilibria can be obtained by solving the equations:

$$\begin{cases} -y = 0, \\ x + \delta yz = 0, \\ \sigma |\cos(x)| - by^2 = 0. \end{cases} \quad (3.3)$$

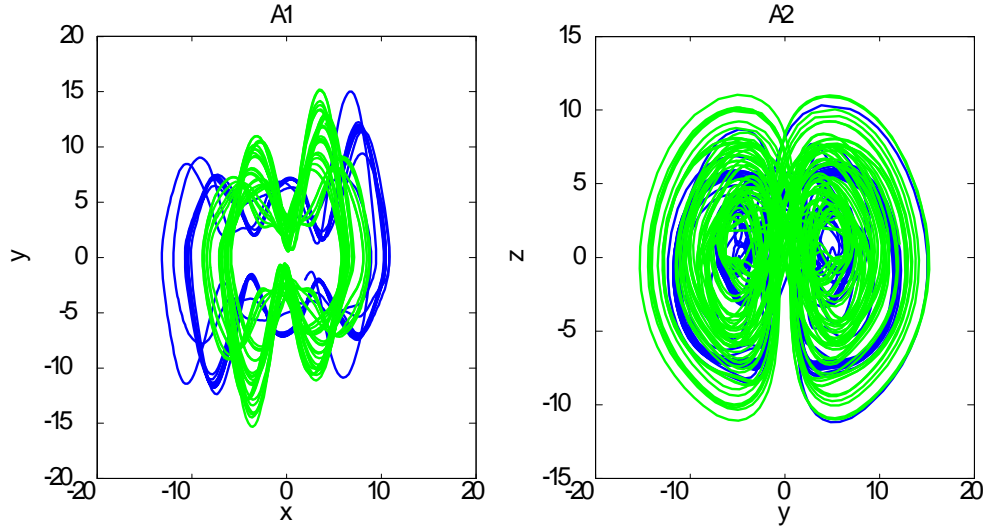


Figure 3.1: Two coexisting attractors of case 1

The last equation of system (3.3) is inconsistent since $\sigma > 0$. Thus, there is no equilibrium in system (3.3).

Type of system: Hidden attractor with no equilibrium.

- **Case 3** $b, \sigma, \mu > 0, a = \delta > 0$ and $|f(x)| = |\sin(x)|$.

The equilibria can be obtained by solving the equations:

$$\begin{cases} -y = 0, \\ x + \delta yz = 0, \\ \sigma |\sin(x)| - by^2 - \delta z - \mu = 0. \end{cases} \quad (3.4)$$

From the equations (3.4), one can observe that case 3 of MACS has only one equilibrium

$$Eq_2(0, 0, \frac{-\mu}{\delta}).$$

Type of system: Hidden attractor with one stable equilibrium.

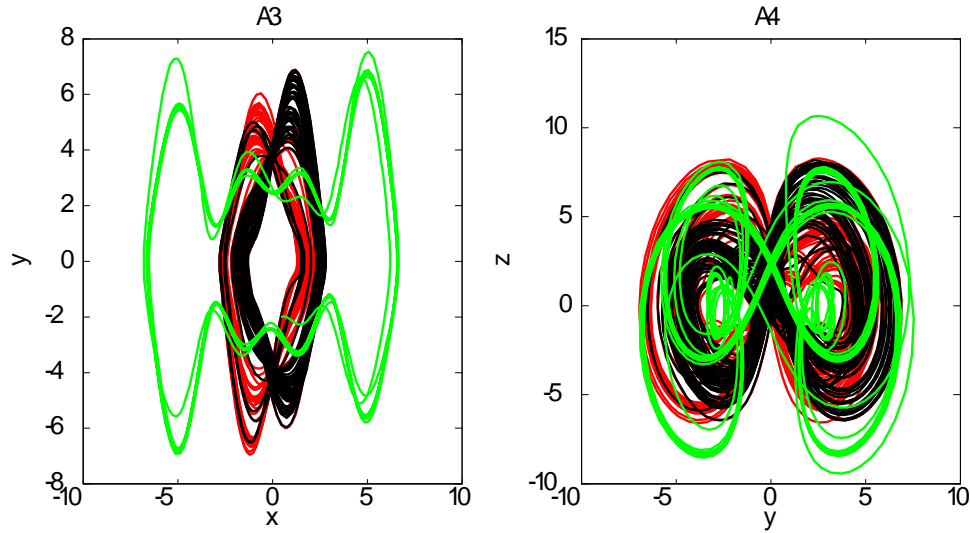


Figure 3.2: Three coexisting attractors of case 1

3.1 Various kinds of multistability behaviors

Multistability (coexisting) attractors basically mean that a system has two or more solutions simultaneously under the same set of parameters and different initial values.

Extremely multistability behaviors of self-excited and hidden attractors of the MACS are investigated using numerical simulations. [11]

We summarize the cases in the following table (3.1).

It can be inferred from the analysis above that the MACS is highly sensitive to initial values and parameters because we can observe the attractive and interesting multisubstance phenomenon of the three cases of the MACS.

3.2 Chaos-based PRNG

3.2.1 What is the PRNG?

A pseudo-random number generator (PRNG) is an algorithm that generates a sequence of numbers that appear to be random but are actually generated by a deterministic process. PRNG uses a deterministic algorithm to generate a sequence of numbers that has statistical

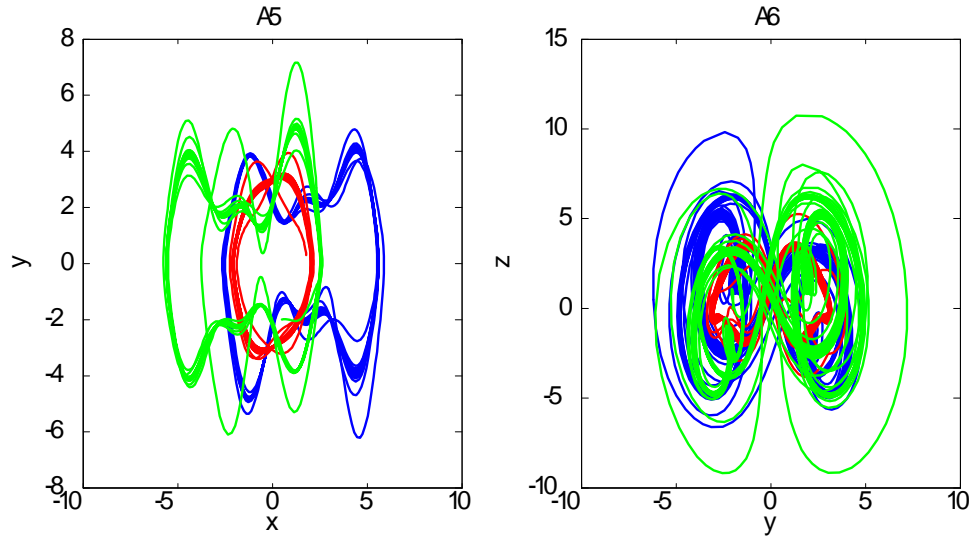


Figure 3.3: Three coexisting attractors of case 1

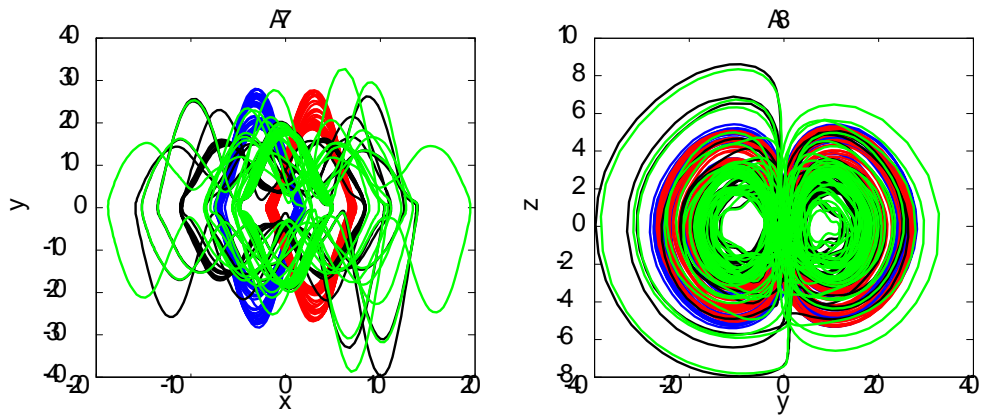


Figure 3.4: Four coexisting attractors of case 2

properties that are similar to true random numbers.

The need for a pseudo-random number generator arises in many cryptographic applications; for example, common cryptosystems employ keys, auxiliary quantities used in generating digital signatures, and data hiding. If a chaotic system possesses certain characteristics, such as high sensitivity to initial values and parameters, good complexity performance, and high randomness, it can provide a good PRNG.

We noted above the high sensitivity of the MACS by producing various types of coexisting attractors by changing its initial values. Such systems might be inappropriate for

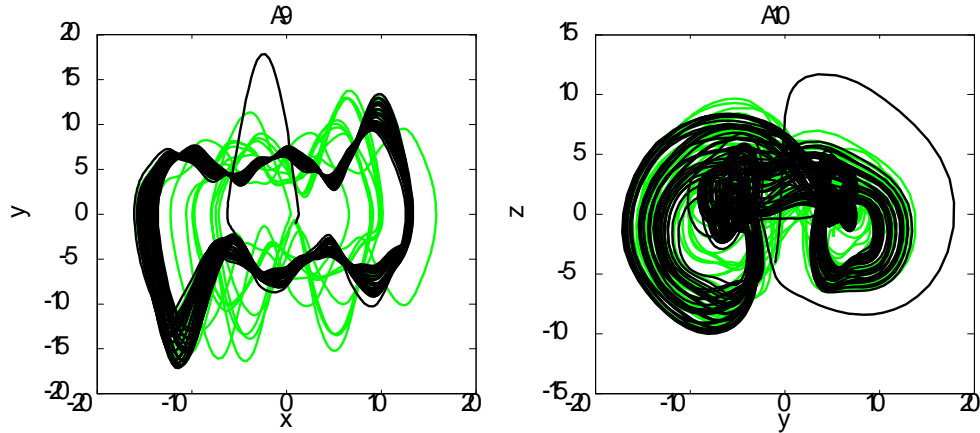


Figure 3.5: Two coexisting chaotic attractors of case 3

cryptographic applications if the PRNG generates from regions of coexisting chaotic with periodic attractors. It follows that we must identify the initial values and parameters that demonstrate coexisting chaotic attractors.

As an example, this section discusses how to construct a PRNG based on Case 2 of MACS.

3.2.2 Lyapunov exponents and Kaplan-Yorke dimension

To generate PRNG from case 2 of MACS, we need to determine the parameters that show coexisting chaotic attractors. We chose $\delta = 1.2$, which produces chaotic behavior for the given four initial values. However, to examine the broad range of initial values, the behavior case 2 versus varying one and two of initial values are investigated. The Largest Lyapunov exponents (LLE) and Kaplan-Yorke dimension versus varying one of the initial values between -5 and 5 are determined.

The LLE-based contour plots are also shown in the reference [11], where two of the initial values are simultaneously changing in the range of $[-5, 5]$ with a step size of 0.1 , while the other initial value is fixed at 1 .

These two results indicate that case 2 shows fractional dimension chaotic or coexisting chaotic attractors when one or even two of the initial values vary in the range of $[-5, 5]$.

Name	Parameters	Initial values	Attractor type	Figure
Case 1	$b = 0.47$	$(2, -2, -1)$ (blue)	limit cycle	3.1
		$(0.5, -2, 0)$ (green)	S-E C attractor	
Case 1	$b = 1.4$	$(1.8, 0.3, 0)$ (red)	S-E C attractor	3.2
		$(-1.8, 0.3, 0)$ (black)	S-E C attractor	
		$(0.5, -2, 0)$ (green)	limit cycle	
Case 1	$b = 1.93$	$(2, -2, -1)$ (blue)	limit cycle	3.3
		$(1.8, 0.3, 0)$ (red)	limit cycle	
		$(0.5, -2, 0)$ (green)	limit cycle	
Case 2	$\delta = 1.82$	$(1.8, 0.3, 0)$ (blue)	H C attractor	3.4
		$(-1.8, 0.3, 0)$ (red)	H C attractor	
		$(5, 0, -5)$ (black)	H C attractor	
		$(5, 3, -3)$ (green)	H C attractor	
Case 3	$b = 0.3$	$(1, -1, 1)$ (green)	H C attractor	3.5
		$(1, -1, -4)$ (black)	H C attractor	

Table 3.1: Details of the attractors shown in figs

3.2.3 Sample Entropy

There are numerous measures that can be used to quantify the complexity of a dynamical system, such as Sample Entropy, Approximate Entropy, and Multiscale Entropy. We select Sample Entropy (SamEn) because it has excellent properties of simplicity, robustness, and fast calculation.

The Sample Entropy (SampEn) algorithm is a statistical method used for measuring the complexity of a time-series signal.

Suppose that the time series $(y_i, i = 0, \dots, N-1)$ with a length of N . Here is the algorithm for computing the SampEn:

1) Phase-space reconstruction: for a given embedding dimension n and time delay τ , the reconstruction sequences are provided by

$$Y_i = \{y_i, y_{i+\tau}, \dots, y_{i+(n-1)\tau}\}, \quad y_i \in \mathbb{R}^n,$$

where $i = 1, \dots, N - n + \tau$.

2) Counting the vector pairs: let B_i be the number of vector Y_j , such that

$$d(Y_i, Y_j) \leq s, \quad i \neq j,$$

where s is the tolerance parameter, and $d(Y_i, Y_j)$ is defined by

$$d(Y_i, Y_j) = \max\{|y(i+k) - y(j+k)| : 0 \leq k \leq n-1\}.$$

3) Calculating probability: according to the obtained number of vector pairs, we can obtain

$$C_i^n(s) = \frac{B_i}{N-(n-1)\tau},$$

then calculate the probability by

$$\phi^n(s) = \frac{\sum_{i=1}^{N-(n-1)\tau} \ln(C_i^n(s))}{[N-(n-1)\tau]}.$$

4) Calculating SamEn: we can obtain $\phi^{n+1}(s)$ by repeating the above steps, then SamEn is given by

$$SamEn(n, s, N) = \phi^n(s) - \phi^{n+1}(s).$$

In our study, we fix $n = 2, \tau = 1$ and $s = 0.2 \times SD$ (SD is times standard deviation).

SamEn of case 2 with one of the initial values between -5 and 5 is determined.

The SamEn of case 2 is also shown in the reference [11], where two of the initial values vary in the range of $[-5, 0]$ and $[0, 5]$ with a step size of 0.03 .

The generation procedures of the PRNG are shown in figure(3.6), where a new algorithm based on case 2 is proposed. Reference [11] shows that the highest standards of statistical packages were used, which is NIST-800-22, and our PRNGs were able to pass all statistical tests.

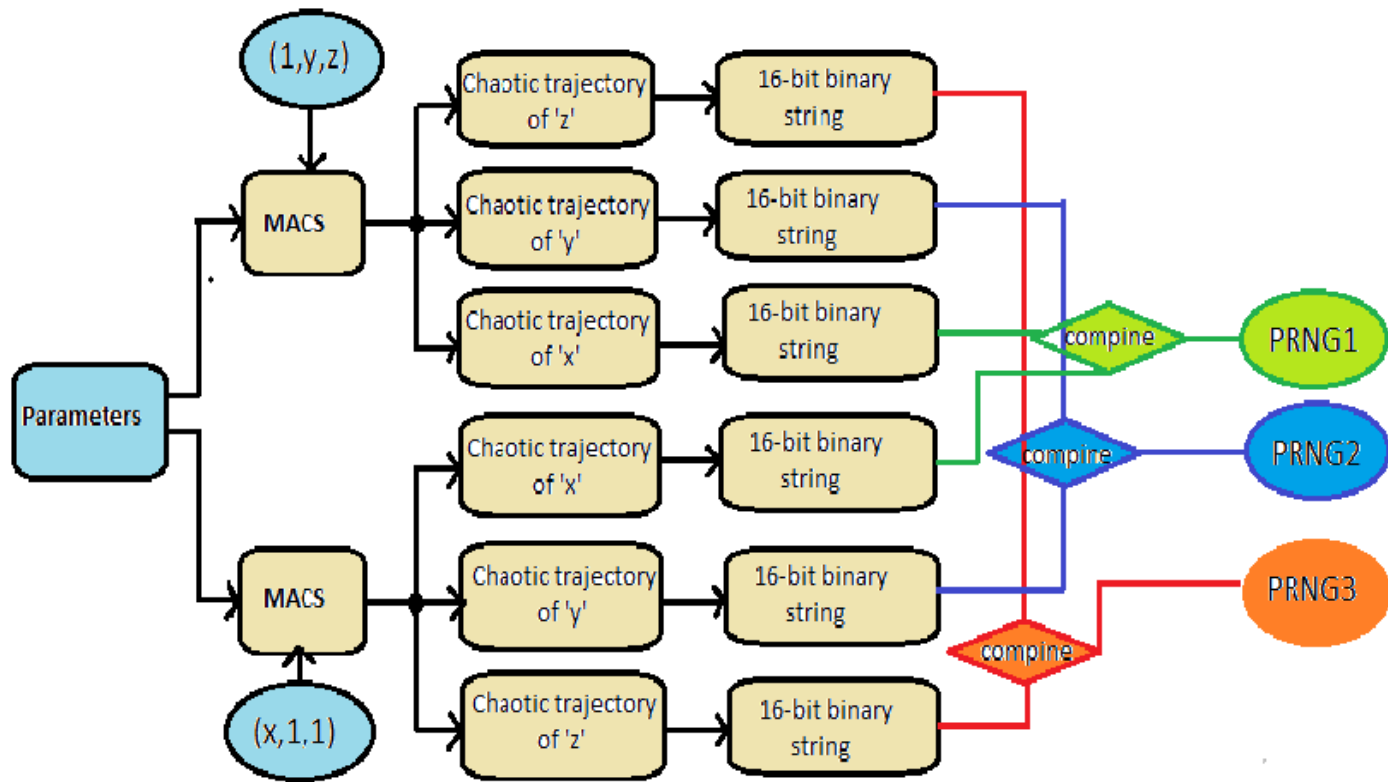


Figure 3.6: The flowchart of generating PRNG

Conclusion

This work has been divided into three chapters. **In the first chapter**, we introduced concepts about dynamical systems and their studies, we discussed the definition of dynamical system and its types, then we presented definitions of basic concepts in the study of dynamical systems: flows, equilibrium points, stability, and bifurcations. We also made it clear that the three-dimensional nonlinear systems would be highlighted. At the last step, we defined the concepts of attractors and chaos as a prelude to the second chapter. **In the second chapter**, which was titled "Self Excited and Hidden Attractors", we defined each of the self-excited and hidden attractors. Then, in five steps, we introduced the analytical-numerical procedure for hidden attractors localization. To explain the previous steps, we chose Chua's system as an applied example. Moving on to the real side, **in chapter three** we introduced one of the most important applications of self-excited and hidden attractors, which is cryptography. We introduced a three-dimensional system with parameters; after studying it, the system showed sensitivity to initial values and parameters, and it was chosen to generate PRNG. This chapter was provided with figures and diagrams, and the system proved its effectiveness by passing all the statistical tests.

While self-excited and hidden attractors have some limitations, their many positive points and applications make them a fascinating and important topic in dynamical systems theory. As a student studying self-excited and hidden attractors, I can share my future goals and aspirations for research in this field. I aspire to make new discoveries about the behavior of these systems as well as new applications in other fields.

Bibliography

- [1] Alligood, K. T., Sauer, T. D., Yorke, J. A., & Chillingworth, D. (1998). Chaos: an introduction to dynamical systems. *SIAM Review*, 40(3), 732-732.
- [2] Broer, H. W., & Takens, F. (2011). *Dynamical systems and chaos* (Vol. 172, pp. 133-133). New York: Springer.
- [3] Brown, R. (2018). *A modern introduction to dynamical systems*. Oxford University Press.
- [4] Deng, Q., Wang, C., & Yang, L. (2020). Four-wing hidden attractors with one stable equilibrium point. *International Journal of Bifurcation and Chaos*, 30(06), 2050086.
- [5] Efrem, R. (2017). AN EXAMPLE OF HIDDEN ATTRACTOR LOCALIZATION. *ROMAI Journal*, 13(2).
- [6] Layek, G. C. (2015). *An introduction to dynamical systems and chaos* (Vol. 449). New Delhi: Springer.
- [7] Leonov, G. A., & Kuznetsov, N. V. (2011). Analytical-numerical methods for investigation of hidden oscillations in nonlinear control systems. *IFAC Proceedings Volumes*, 44(1), 2494-2505.
- [8] Leonov, G. A., & 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.
- [9] Menacer, T., Lozi, R., & Chua, L. O. (2016). Hidden bifurcations in the multispiral Chua attractor. *International Journal of Bifurcation and Chaos*, 26(14), 1630039.
- [10] Nag Chowdhury, S., & Ghosh, D. (2020). Hidden attractors: A new chaotic system without equilibria. *The European Physical Journal Special Topics*, 229(6-7), 1299-1308.
- [11] Natiq, H., Said, M. R. M., Ariffin, M. R. K., He, S., Rondoni, L., & Banerjee, S. (2018). Self-excited and hidden attractors in a novel chaotic system with complicated multistability. *The European Physical Journal Plus*, 133, 1-12.
- [12] SAMBAS, A., MAMAT, M., & VAIDYANATHAN, S. (2018). A novel chaotic hidden attractor, its synchronization and circuit implementation. *Chaos*, 1, 2.
- [13] Zaamouche, F. (2022). *Attractors and bifurcations of chaotic systems (Doctoral dissertation)*.

Annex A: Programs in MATLAB

3.3 Lorenz System

```
sigma = 10;
beta = 8/3;
rho = 28;
x0 = [1;1;1];
tspan = [0,100];
dt = 0.01;
f=@(t,x) [sigma*(x(2)-x(1));...
x(1)*(rho-x(3))-x(2);...
x(1)*x(2)-beta*x(3)];
[t,x] = ode45(f,tspan,x0);
figure;
plot3(x(:,1),x(:,2),x(:,3),'b','LineWidth',1);
xlabel('x'); ylabel('y'); zlabel('z');
title('Numerical localization of chaotic attractor in Lorenz system');
```

3.4 MACS System

```
a=0.5;
b=.47
```

```
sigma = 17;
rho = .63;
u=0;
x01 = [2;-2;-1];
tspan = [0,200];
dt = 0.0001;
f=@(t,x) [-x(2);...
x(1)+rho*x(2)*x(3);...
sigma*abs(cos(x(1)))-b*x(2)^2-a*x(3)-u];
[t,x1] = ode45(f,tspan,x01);
x02 = [0.5;-2;0];
[t,x2] = ode45(f,tspan,x02);
subplot(1,2,1)
plot(x1(:,1),x1(:,2),'b','LineWidth',1);xlabel('x'); ylabel('y');
hold on
plot(x2(:,1),x2(:,2),'g','LineWidth',1);
xlabel('x'); ylabel('y');
subplot(1,2,2)
plot(x1(:,2),x1(:,3),'b','LineWidth',1);
xlabel('y'); ylabel('z');
hold on
plot(x2(:,2),x2(:,3),'g','LineWidth',1);
xlabel('y'); ylabel('z');
%This algorithm is for A1 and A2, and the rest is done in the same way.
```

Annex B: Abbreviations and Notation

\mathbb{R}^n	The set of real numbers power n .
\mathbb{R}	The set of real numbers.
\mathbb{Z}	The set of integers.
\mathbb{N}	The set of natural numbers.
S-E C	Self-excited chaotic.
H C	Hidden chaotic.

Abstract

There is still no valid definition of chaos, but we can say that it is the study of systems that have had a very complex evolution. Chaotic attractors are classified into two types: self-excited attractors and hidden attractors. We presented the objective of this Master's Thesis in three chapters: the first chapter summarizes definitions about dynamical systems; the second chapter provides definitions about self-excited attractors and hidden attractors; we introduced the analytical-numerical procedure for hidden attractors localization; the last chapter is interesting, that presents an important application that falls under the title "Chaos-Based Cryptographic", we have already proven the success of this cryptographic application.

Keywords: Dynamic systems, chaos, self-excited attractors, hidden attractors, cryptographic.

Résumé

Il n'y a toujours pas de définition valable du chaos, mais on peut dire que c'est l'étude de systèmes qui ont eu une évolution très complexe. Les attracteurs chaotiques sont classés en deux types : les attracteurs auto-excités et les attracteurs cachés. Pour atteindre notre objectif, le mémoire est divisé en trois chapitres : le premier chapitre résume les notions de base sur les systèmes dynamiques ; le deuxième chapitre fournit des définitions sur les attracteurs auto-excités et les attracteurs cachés et la différence entre eux; nous avons introduit la procédure analytique-numérique pour la localisation des attracteurs cachés ; le dernier chapitre est intéressant qui présente une application importante qui relève du titre "Chaos-Based Cryptographic", et nous avons déjà prouvé le succès de cet application de chiffrement.

Les mots clés : Les systèmes dynamiques, chaos, les attracteurs auto-excités, les attracteurs cachés, chiffrement.

الملخص

لا يوجد حتى الآن تعريف دقيق للفوضى، لكن يمكننا القول إنها دراسة الأنظمة التي كان لها تطور معقد للغاية. تصنف الجاذبات الفوضوية إلى فئتين: الجاذبات ذاتية الإثارة والجاذبات المخفية. للوصول إلى الهدف قسمنا هذه المذكرة إلى ثلاثة فصول: الفصل الأول يلخص المفاهيم الأساسية حول الأنظمة الديناميكية. يقدم الفصل الثاني تعريفات حول الجاذبات ذاتية الإثارة والجاذبات المخفية و الفرق بينهما. قدمنا طريقة تحليلية و عددية لتحديد الجاذبات المخفية؛ والفصل الأخير هو فصل مثير للاهتمام يقدم تطبيقاً مهماً يندرج تحت عنوان "التشفير القائم على الفوضى"، وقد أثبتنا بالفعل نجاح تطبيق التشفير هذا.

الكلمات المفتاحية : الأنظمة الديناميكية، الفوضى، الجاذبات ذاتية الإثارة، الجاذبات المخفية، التشفير.