



*People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific
Research*

Larbi Tébessi University - Tébessa

Faculty of Exact Sciences and Natural and Life Sciences

Department: Mathematics

End-of-study disseration for obtaining the master degree

Field: Mathematics

Option: Mathematics

Speciality: Dynamical Systems and Its Applications

Titled by :

*Chaos in famous discrete dynamical
systems and its application in cryptography*

Presented By:

Zidane Belghit

Devant le jury :

Gasri Ahlem

Prof Larbi Tébessi University

Président

Diab Zouhair

M.C.A Larbi Tébessi University

Examine

Boukhalfa ElHafsi

M.C.B Larbi Tébessi University

Supervisor

Academic Year: 2025/2026

Dedication

Above all, I owe my deepest gratitude to my father, *Djamel Belghit*. No one could ever imagine the sacrifices he made or the love he gave me. His belief in me has always been and continues to be the fuel that keeps me going. This thesis is as much his as it is mine. I hope it makes you proud of me, as I have always been proud to be your son.

A special mention goes to the one who gives selflessly without ever expecting anything in return, to the first teacher, the best friend, the quiet supporter, and the eternal source of love. Thank you, Mom. I love you.

I am also deeply grateful to my brothers for their endless, unconditional love, care, and support. This achievement belongs to all of us.

Acknowledgments

In the name of Allah, the Most Gracious, the Most Merciful.

Alhamdulillah for His countless blessings.

I am sincerely thankful for the guidance and support I have received from *El Hafsi Boukhalfa*, my supervisor.

I would like to thank the staff of the Department of Mathematics at the University of Cheikh Larbi Tebessi – Tebessa, for welcoming me into a hardworking environment and providing the necessary academic support to complete this research.

To my colleagues and friends, thank you for making each day enjoyable.

Abstract

Chaos is a rich and modern field of research, linked to other disciplines such as information security, cryptography, and computer science.

This is why we are entreing this area of applied mathematics.

The objective of this work is based on the general problem of searching chaos in nonlinear dynamical system, more specifically, we are interested in discrete nonlinear dynamical systems, whose formulation are given by recurrent function with a set of bifurcation parameters, where a small perturbation to the inintial conditions results in a large discrepancy between long term observation; this is where the notion of unpredictability takes place.

Keywords: Chaos, discrete dynamical systems, nonlinear systems, bifurcation parameters, unpredictability, initial conditions.

Resumé

Le chaos est un domaine de recherche riche et moderne, étroitement lié à d'autres disciplines telles que la sécurité de l'information, la cryptographie et l'informatique.

C'est pourquoi nous avons choisi d'explorer ce domaine des mathématiques appliquées.

L'objectif de ce travail repose sur le problème général de l'étude du chaos dans les systèmes dynamiques non linéaire, plus précisément, nous intéressons aux systèmes dynamiques non linéaires discrets, dont les formulations sont définies par des fonctions récurrentes associées à un ensemble de paramètres de bifurcation, dans de tels systèmes, une faible perturbation des conditions initiales peut entraîner une divergence significative du comportement à long terme; c'est là qu'apparaît la notion d'imprévisibilité.

Mots clés : Chaos, systèmes dynamiques discrets, systèmes non linéaires, paramètres de bifurcation, imprévisibilité, conditions initiales

ملخص

الفوضى مجال بحثي غني وحديث، يرتبط ارتباطاً وثيقاً بتخصصات أخرى كأمّن المعلومات والتشفير وعلم الحاسوب، وهذا ما دفعنا إلى استكشاف هذا الفرع من الرياضيات التطبيقية. يقوم هدف هذا العمل على الإشكالية العامة لدراسة الفوضى في الأنظمة الديناميكية اللاخطية، وبشكل أدق، نهتم بالأنظمة الديناميكية اللاخطية المتقطعة، التي تُصاغ معادلاتها بواسطة دوال تكرارية مرتبطة بمجموعة من معاملات التشعب. وفي مثل هذه الأنظمة، قد يؤدي اضطراب طفيف في الشروط الابتدائية إلى تباعد ملحوظ في السلوك على المدى البعيد، وهنا تبرز مفهوم عدم القدرة على التنبؤ. الكلمات المفتاحية: الفوضى، الأنظمة الديناميكية المتقطعة، الأنظمة اللاخطية، معاملات التشعب، عدم القدرة على التنبؤ، الشروط الابتدائية.

List of Figures

2.1	Saddle-Node Bifurcation Diagram	16
2.2	Transcritical Bifurcation Diagram	16
2.3	Pitchfork Bifurcation Diagram	17
2.4	Period-Doubling Bifurcation Diagram	17
2.5	Neimark-Sacker Bifurcation Diagram with Prey Refuge Effect	18
2.6	Crisis Bifurcation Diagram	18
4.1	Logistic Map Attractor for $r = 3.9$	24
4.2	Logistic Map – First 100 Iterations of x_n	25
4.3	Logistic Map Bifurcation Diagram for $x_0 = 0.4$	26
4.4	Logistic Map : Lyapunov Exponent Evolution	26
4.5	Hénon Strange Attractor for $a = 1.4, b = 0.3$	27
4.6	Hénon Map – First 100 Iterations of x_n	28
4.7	Hénon Map – First 100 Iterations of y_n	28
4.8	Bifurcation diagram of Henon map	30
4.9	Hénon Map : Lyapunov Exponent Evolution	31
4.10	Lozi Strange Attractor for $a = 1.7, b = 0.5$	32
4.11	Lozi Map – First 100 Iterations of x_n	33
4.12	Lozi Map – First 100 Iterations of y_n	33
4.13	Lozi Map : Bifurcation diagram	35
4.14	Lozi Map : Lyapunov Exponent Evolution	36
4.15	first 50 iteration	37
4.16	Bifurcation diagram of system (4.26) for a with $b = 0.6$	41
4.17	Bifurcation diagram of system (4.26) for b with $a = -1$	41
4.18	Evolution of Lyapunov exponent E_1	42
4.19	Grayscale levels	43
4.20	MATLAB programe for encrypting a grayscale image	44
4.21	Original image	45
4.22	Encrypted image	45

Contents

Dedication	1
Acknowledgments	2
Abstract	3
Resumé	4
	5
Introduction	9
1 Preliminaries on Discrete Dynamical Systems	10
1.1 General Concepts	10
1.1.1 Discrete Dynamical Systems	10
1.1.2 Orbits	10
1.1.3 Equilibrium Points	11
1.1.4 Periodic Orbits of Order p (p-Cycles)	11
1.1.5 Phase Space	11
1.2 Stability	11
1.2.1 Lyapunov Stability and Asymptotic Stability	12
1.2.2 Linearization	12
1.2.3 Nature of Equilibrium via Linearization	13
1.2.4 Lyapunov Function	13
1.3 Summary	14
2 Bifurcation Concepts	15
2.1 Definition of Bifurcation	15
2.2 Fundamental Types of Bifurcations	15
2.2.1 Saddle-Node (Tangent) Bifurcation	15
2.2.2 Transcritical Bifurcation	16
2.2.3 Pitchfork Bifurcation	16
2.2.4 Period-Doubling Bifurcation	17
2.2.5 Neimark-Sacker Bifurcation	18
2.2.6 Crisis Bifurcation	18
2.3 Summary	18
3 Road to Chaos	19
3.1 A brief history of chaos	19
3.2 Definition of chaos	20

3.3	Tools for quantifying and measuring chaos	20
3.3.1	Lyapunov exponents	20
3.3.2	Bifurcation diagram	22
3.3.3	Fractal Dimensions	23
3.4	Summary	23
4	Famous discrete dynamical systems	24
4.1	Logistic Map	24
4.1.1	Fixed point and stability	25
4.1.2	Bifurcation diagram	26
4.1.3	Chaos in Logistique map	26
4.2	Henon map	27
4.2.1	Fixed points and stability	29
4.2.2	Bifurcation study	30
4.2.3	Chaos in Henon map	31
4.3	Lozi Map	32
4.3.1	Fixed points and stability	34
4.3.2	Bifurcation diagram	35
4.3.3	Chaos in Lozi map	36
4.4	Boukhalfa map	37
4.4.1	Fixed Points stability	38
4.4.2	Period Doubling	40
4.4.3	Bifurcation diagram	41
4.4.4	Chaos in boukhalfa map	42
4.5	Application of chaotic maps in crypto-graphy	43
4.5.1	Definition of a grayscale image	43
4.5.2	Grayscale levels	43
4.5.3	The importance of using the Boukhalfa map	44
4.5.4	MATLAB code explanation	44
4.6	Summary	45
	Conclusion and Open Perspectives	46

Introduction

Chaos theory is considered one of the most important branches of modern mathematics. Although it is closely related to several highly abstract areas such as topology, measure theory, and number theory, it also has a wide range of practical applications in real life, including biology, cryptography, economics, weather forecasting, and other complex systems. This is mainly due to the ability of chaotic models to generate seemingly random behavior, despite being governed by deterministic laws, when certain parameter values are chosen.

The concept of chaos is inherently relative and multifaceted, as there is no single universally accepted definition that fully captures all of its characteristics [1]. Over the years, researchers have proposed various definitions of chaos, each emphasizing different aspects of the complex and unpredictable behavior observed in natural and mathematical systems. This diversity arises from the fact that the theory of chaos was developed through the study of real-world phenomena where seemingly random behavior often emerges from deterministic laws.

As research in Chaos Theory advanced and computer technology experienced rapid development, the practical applications of chaotic systems expanded far beyond their original role in the study of nonlinear dynamical phenomena. Researchers discovered that many properties of chaotic systems, such as their apparent randomness, sensitivity to initial conditions, ergodicity, and unpredictability, closely resemble the characteristics required for modern cryptographic algorithms [8].

In this context, this thesis is organized into four main interconnected chapters.

first chapter is devoted to the study of discrete dynamical systems, including fundamental definitions, rules of dynamical evolution, as well as the concepts of fixed points and their stability.

second chapter deals with the concept of bifurcation, presenting its main types and its role in the emergence of chaotic behavior.

third chapter addresses the concept of chaos and its methods of quantification and characterization, using mathematical tools that allow distinguishing chaotic behavior from regular dynamics.

fourth chapter provides a comprehensive study of the most important chaotic maps, along with a practical application involving the encryption of a grayscale image using a chaotic map, in order to demonstrate the effectiveness of these models in the field of cryptography and information security.

Chapter 1

Preliminaries on Discrete Dynamical Systems

This chapter establishes the foundational concepts necessary for the study of discrete dynamical systems. It introduces the mathematical formulation of such systems, their orbits, and the classification of equilibrium and periodic behavior. Stability is rigorously treated through Lyapunov methods and linearization, including the Hartman–Grobman theorem. These preliminaries are essential for understanding chaotic behavior in later chapters.

1.1 General Concepts

This section presents the core mathematical elements of discrete dynamical systems, including their formal definition, orbit structure, and the classification of fixed and periodic points. It also introduces the notion of phase space as the framework within which system evolution is visualized and analyzed. These concepts are foundational for characterizing dynamical behavior across parameter regimes.

1.1.1 Discrete Dynamical Systems

Definition 1.1. [6] Consider a system of recurrent algebraic equations

$$x_{k+1} = f(x_k; \Gamma), \quad k \in \mathbb{N}, \quad (1.1)$$

which defines a discrete dynamical system where $x_k \in \mathbb{R}^n$ is the state vector at the k -th iteration, $\Gamma \in \mathbb{R}^m$ (with $m \geq 1$) is the parameter vector, and f is the nonlinear recurrence function which dictates the dynamics of the system.

1.1.2 Orbits

Definition 1.2. [6] The orbit of a point x_0 under the system (1.1) is given by:

$$O(x_0) = \{x_0, f(x_0), f^2(x_0), f^3(x_0), \dots\}. \quad (1.2)$$

defined as the phase trajectory and originated from x_0 .

1.1.3 Equilibrium Points

Definition 1.3. [6] Consider x^* An equilibrium (or fixed) point of the system that satisfies

$$f(x^*) = x^*. \quad (1.3)$$

Remark. Graphically, equilibrium points are intersections of the curve $y = f(x)$, with the bisector $y = x$.

1.1.4 Periodic Orbits of Order p (p-Cycles)

Definition 1.4. [6] A point $x \in X$ is a periodic orbit of period p if

$$f^p(x) = x, \quad (1.4)$$

where p is the smallest positive integer satisfying this condition.

The set

$$\{x, f(x), f^2(x), \dots, f^{p-1}(x)\}, \quad (1.5)$$

which forms a p -cycle.

Remark. Periodic orbits are fundamental in bifurcations and the transition to chaos.

1.1.5 Phase Space

Definition 1.5. [6] Consider a discrete dynamical system $f : X \rightarrow X$, where the set $X \subseteq \mathbb{R}^d$ represents the phase space, and each point $x \in X$ represents the system's complete state. The evolution of the system is described by the orbit

$$\mathcal{O}(x_0) = \{x_n\}_{n \in \mathbb{N}}, \quad x_{n+1} = f(x_n), \quad x_0 \in X. \quad (1.6)$$

Remark. The phase space encodes all possible orbits under the iteration of f , including fixed points, periodic orbits, and a periodic (chaotic) trajectories.

1.2 Stability

This section addresses the stability properties of equilibrium points in discrete systems. It includes formal criteria for Lyapunov and asymptotic stability, linearization techniques via the Jacobian matrix, and the use of Lyapunov functions for nonlinear stability analysis. These tools are critical for assessing the robustness of system trajectories under perturbations and form the basis for detecting bifurcations and chaotic behavior.

1.2.1 Lyapunov Stability and Asymptotic Stability

Definition 1.6. [15] Let $f: X \rightarrow X$ be a map on the metric space (X, d) , and let $x^* \in X$ satisfy $f(x^*) = x^*$.

1. **Lyapunov stability:**

$$\forall \varepsilon > 0 \exists \delta > 0 : d(x_0, x^*) < \delta \implies d(f^n(x_0), x^*) < \varepsilon \quad \forall n \geq 0.$$

2. **Asymptotic stability:** x^* is Lyapunov stable and

$$\exists \delta' > 0 : d(x_0, x^*) < \delta' \implies \lim_{n \rightarrow \infty} f^n(x_0) = x^*.$$

1.2.2 Linearization

Definition 1.7. [15] Let $f: U \subset \mathbb{R}^n \rightarrow \mathbb{R}^n$ be C^1 on an open U , and let $x^* \in U$ satisfy $f(x^*) = x^*$.

$$Df(x^*) = \left[\partial_j f_i(x^*) \right]_{1 \leq i, j \leq n},$$

is the linearization of f at x^* .

Proof. Let $x_{n+1} = f(x_n)$ with $f(x^*) = x^*$

By applying the first order Taylor expansion to f near the point x^* we obtain:

$$x_{n+1} = f(x^*) + Df(x^*)(x_n - x^*) + O(x_n^2). \quad (1.7)$$

By setting $v_n = x_n - x^*$, and assuming that $O(x_n^2)$ very small we obtain :

$$v_{n+1} = Df(x^*)v_n. \quad (1.8)$$

□

Theorem 1.1 (Hartman–Grobman). *Let $f: U \rightarrow \mathbb{R}^n$ be C^1 with fixed point x^* . If $Df(x^*)$ is hyperbolic (no eigenvalue on the unit circle), then there exist neighborhoods $V \ni x^*$, $W \ni 0$ and a homeomorphism $h: V \rightarrow W$ such that*

$$h(f(x)) = Df(x^*)h(x) \quad \forall x \in V.$$

and for the proof of the theorem, you can refer to [15]

1.2.3 Nature of Equilibrium via Linearization

Let $f: U \subset \mathbb{R}^n \rightarrow \mathbb{R}^n$ be C^1 and $x^* \in U$ a fixed point, $f(x^*) = x^*$. Denote $A = Df(x^*)$ and let its eigenvalues be $\{\lambda_i\}_{i=1}^n$. Then the linearized map $x_{k+1} = Ax_k$ determines the local behavior of the nonlinear system:

- **Hyperbolic Sink (Asymptotically Stable)** $\forall i, |\lambda_i| < 1$. All trajectories in a neighborhood converge exponentially to x^* .
- **Hyperbolic Source (Unstable)** $\forall i, |\lambda_i| > 1$. All nearby trajectories diverge exponentially from x^* .
- **Hyperbolic Saddle** $\exists i, j$ such that $|\lambda_i| < 1$ and $|\lambda_j| > 1$. Trajectories approach x^* along the stable eigenspace and diverge along the unstable one.
- **Non-Hyperbolic (Center or Indeterminate)** $\exists i$ with $|\lambda_i| = 1$. Linearization is inconclusive; higher-order terms or Lyapunov functions are required.

1.2.4 Lyapunov Function

Theorem 1.2. [11] *Let U be a neighborhood of the equilibrium x^* .*

$V: U \rightarrow \mathbb{R}$ is a Lyapunov function that satisfies:

1. **Positivity:** $V(x^*) = 0$ and $V(x) > 0$ for all $x \in U \setminus \{x^*\}$.
2. **Non-Increase Along Orbits:**

$$V(f(x)) - V(x) \leq 0 \quad \text{for all } x \in U. \quad (1.9)$$

If

$$V(f(x)) - V(x) < 0 \quad \text{for all } x \in U \setminus \{x^*\}, \quad (1.10)$$

then x^* is asymptotically stable.

Theorem 1.3 (Discrete-Time Lyapunov Stability). [11] *Consider a discrete system $x_{k+1} = Ax_k$, where $A \in \mathbb{R}^{n \times n}$. The system is globally asymptotically stable if and only if, for any positive definite matrix $Q \in \mathbb{R}^{n \times n}$, there exists a unique positive definite matrix $P \in \mathbb{R}^{n \times n}$ satisfying the Lyapunov equation:*

$$A^T P A - P + Q = 0. \quad (1.11)$$

The quadratic function

$$V(x) = x^T P x. \quad (1.12)$$

is a valid Lyapunov function, which proves the system's stability.

Example. Let the discret dynamical system :

$$\begin{cases} x_{n+1} = \frac{2026x_n}{1 + 2025x_n}, \\ x_0 = \frac{1}{2}. \end{cases} \quad (1.13)$$

Thus, the fixed point are : $\{0, 1\}$

$$|f'(0)| = 2026 > 1 \Rightarrow \text{unstable.}$$

$$|f'(1)| = \frac{1}{2026} < 1 \Rightarrow \text{asymptotically stable.}$$

Example. Let the 2D discret dynamical system difined by

$$\begin{cases} x_{n+1} = \frac{x_n}{1 + x_n^2 + y_n^2}, \\ y_{n+1} = \frac{y_n}{1 + x_n^2 + y_n^2}. \end{cases} \quad (1.14)$$

$(0, 0)$ the fixed point

Let $V(x, y) = x^2 + y^2$ a positive definite function

By applying the definition we find:

$$V(x_{n+1}, y_{n+1}) - V(x_n, y_n) = \frac{x_n^2 + y_n^2}{(1 + x_n^2 + y_n^2)^2} - x_n^2 - y_n^2. \quad (1.15)$$

Let $r_n^2 = x_n^2 + y_n^2$,

$$V(x_{n+1}, y_{n+1}) - V(x_n, y_n) = \frac{r_n^2}{(1 + r_n^2)^2} - r_n^2. \quad (1.16)$$

$$V(x_{n+1}, y_{n+1}) - V(x_n, y_n) = r_n^2 \left(\frac{1}{(1 + r_n^2)^2} - 1 \right). \quad (1.17)$$

Its clear here that the difference is negative, therefore the equilibrium point is stable.

1.3 Summary

In this chapter, we reviewed some of the basic concepts of discrete dynamical systems and their behavior, and this helped us analyze these systems. These ideas pave the way for the next chapter, where we explore comprehensive chaotic discrete dynamical systems, their mathematical properties, and their role in chaos theory.

Chapter 2

Bifurcation Concepts

Bifurcation theory studies the changes in a dynamical system's behavior when certain adjustments are made to its parameters. In discrete systems specifically, bifurcations lead to the appearance or disappearance of fixed points or periodic orbits, resulting in the onset of chaos.

2.1 Definition of Bifurcation

Consider the discrete dynamical system:

$$x_{k+1} = f(x_k, \lambda), \quad k \in \mathbb{N}, \quad (2.1)$$

where $x \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$ is a parameter.

A **bifurcation** happens at a critical parameter value λ^* if there is an adjustment in the structure of the fixed points or periodic orbits of f .

2.2 Fundamental Types of Bifurcations

2.2.1 Saddle-Node (Tangent) Bifurcation

Definition 2.1. [3] Two fixed points (one stable, one unstable) merge and disappear. For the normal form

$$x_{k+1} = x_k + \lambda - x_k^2, \quad (2.2)$$

the conditions are:

- **Existence:** $f(x^*, \lambda^*) = x^*$.
- **Tangency:** $\frac{\partial f}{\partial x}(x^*, \lambda^*) = 1$.
- **Non-degeneracy:** $\frac{\partial^2 f}{\partial x^2}(x^*, \lambda^*) \neq 0$.

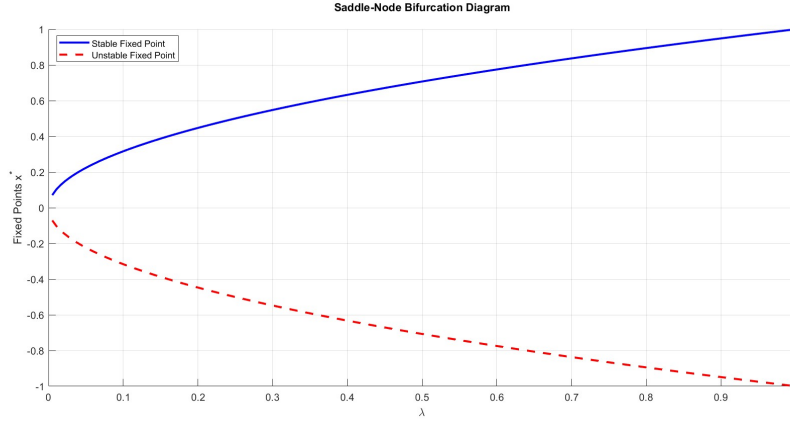


Figure 2.1: Saddle-Node Bifurcation Diagram

2.2.2 Transcritical Bifurcation

Definition 2.2. [3] Two fixed points exchange stability. The normal form is

$$x_{k+1} = x_k + \lambda x_k - x_k^2. \quad (2.3)$$

Here, fixed points exist at $x = 0$ and $x = \lambda$; as λ crosses zero, the stability properties of these fixed points are interchanged.

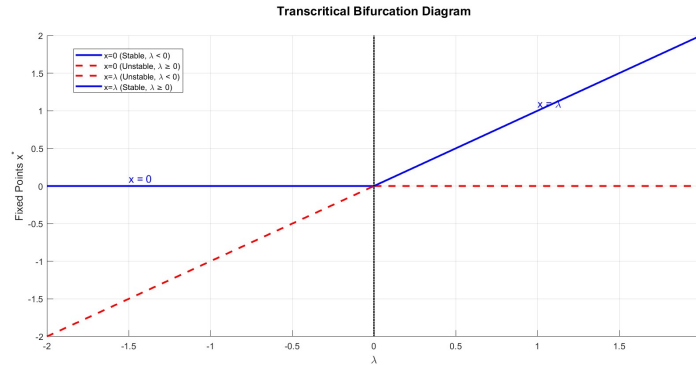


Figure 2.2: Transcritical Bifurcation Diagram

2.2.3 Pitchfork Bifurcation

Definition 2.3. [3] A pitchfork bifurcation happens in systems with symmetry. The normal form

$$x_{k+1} = x_k + \lambda x_k - x_k^3. \quad (2.4)$$

has these features:

- For $\lambda < 0$, the unique fixed point $x = 0$ is stable.
- For $\lambda > 0$, $x = 0$ becomes unstable and two new fixed points emerge at $x = \pm\sqrt{\lambda}$.

The bifurcation is termed **supercritical** if the new fixed points are stable, and **subcritical** if they are unstable.

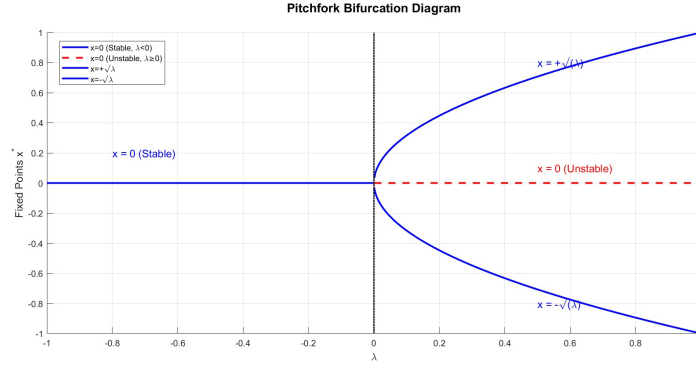


Figure 2.3: Pitchfork Bifurcation Diagram

2.2.4 Period-Doubling Bifurcation

Definition 2.4. [3] A period-doubling bifurcation happens when a fixed point (or periodic orbit) loses stability as an eigenvalue crosses -1 , leading to a new orbit with twice the period. For example, in the logistic map

$$x_{k+1} = \lambda x_k(1 - x_k), \quad (2.5)$$

this happens when

$$f'(x^*, \lambda^*) = -1. \quad (2.6)$$

2.2.4.1 remark

Successive period-doubling bifurcations can form a cascade that leads to chaos.

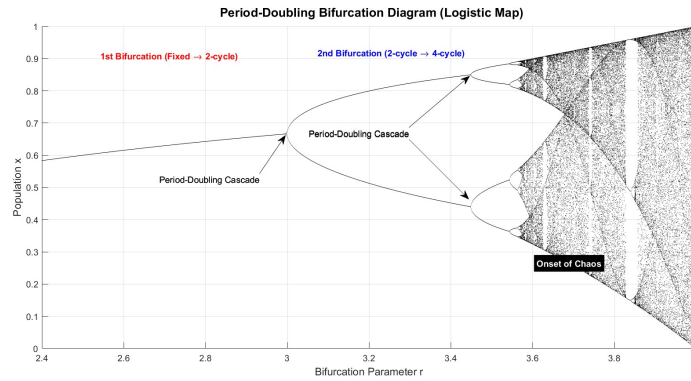


Figure 2.4: Period-Doubling Bifurcation Diagram

2.2.5 Neimark-Sacker Bifurcation

Definition 2.5. [14] The Neimark-Sacker bifurcation happens when a pair of complex conjugate eigenvalues of $Df(x^*, \lambda)$ cross the unit circle (with $|\mu| = 1$ and $\mu \neq \pm 1$). This transition gives rise to an invariant closed curve and quasiperiodic dynamics.

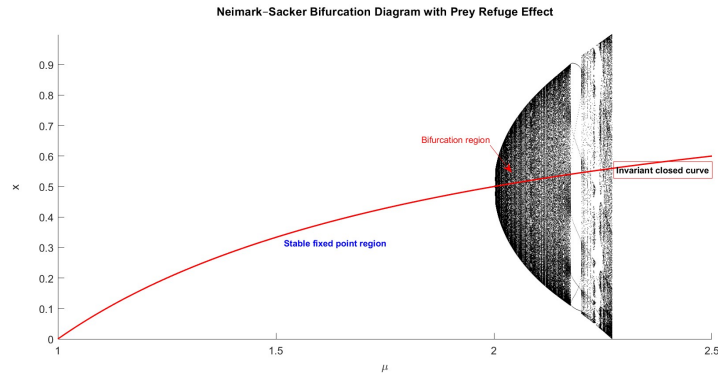


Figure 2.5: Neimark-Sacker Bifurcation Diagram with Prey Refuge Effect

2.2.6 Crisis Bifurcation

Definition 2.6. [14] A crisis bifurcation is a sudden change in the size or shape of a chaotic attractor as the parameter λ varies. It happens when the attractor collides with an unstable periodic orbit, causing a sudden chaos appearance or disappearance.

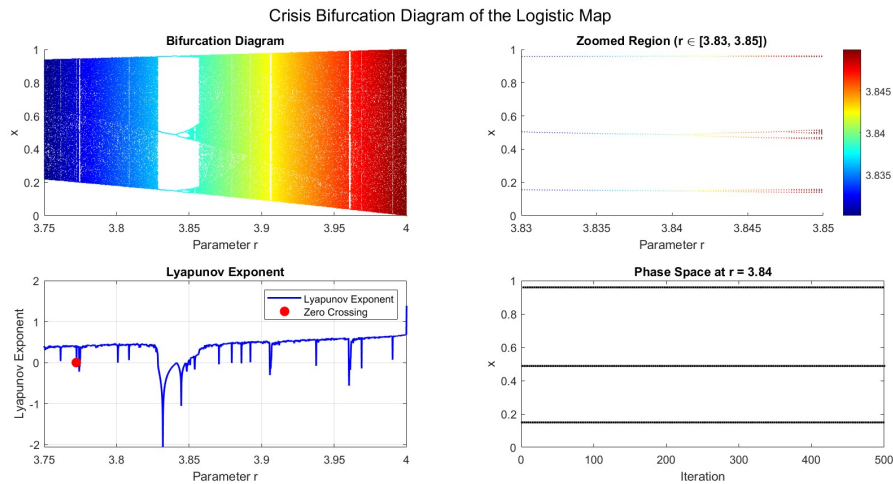


Figure 2.6: Crisis Bifurcation Diagram

2.3 Summary

In this chapter, we have introduced the concept of bifurcation in discrete dynamical systems, and we have studied the main types of bifurcations along with the conditions required for each type to occur.

Chapter 3

Road to Chaos

3.1 A brief history of chaos

The historical roots of chaos theory date back to the late nineteenth century with work of Henri Poincaré during his study of the three body problem in celestial mechanics, he discovered that deterministic systems can exhibit complex and non periodic behavior that is extremely difficult to predict over the long term thereby laying the foundation for the concept of sensitivity to initial conditions.

The first half of the twentieth century particularly the period between the two world wars witnessed a relative stagnation in the development of this field. This was due to the dominance of the classical deterministic world view, the absence of computational tools capable of analyzing complex nonlinear systems, and the redirection of scientific resources toward weapons production.

The real turning point came in 1963 with the American meteorologist Edward Lorenz, while simulating a simplified weather model, he discovered that a very small change in initial values could lead to drastically different outcomes what later became known as the butterfly effect, he also introduced the famous strange attractor that bears his name.

During the 1970s, the theory expanded mathematically, especially after Mitchell Feigenbaum discovered universal constants governed the period doubling phenomenon in nonlinear systems, Benoit Mandelbrot contributed to the development of fractal geometry, showing that many chaotic structures possess fractional dimensions and self similarity.

Beginning in the 1980s, chaos theory gained widespread recognition, particularly after the publication of *Chaos: Making a New Science* by James Gleick, it also became a major focus of research institutions such as the Santa Fe Institute, transforming from a specialized mathematical field into a multidisciplinary scientific framework.

From the 1990s, to the present, chaos theory has merged with complex systems science and has found broad application in physics, biology, economics, climate science, and network analysis, becoming an essential tool for understanding the complexity that characterizes many natural and human phenomena. [10]

3.2 Definition of chaos

Definition 3.1. [1] Let (X, d) be a metric space, and the map $f : X \rightarrow X$, where X is a set, is said to be chaotic if

1. f is transitive

For any two non-empty open sets $A, B \subset X$ there exists an integer $n > 0$ such that

$$f^n(A) \cap B \neq \emptyset. \quad (3.1)$$

2. The set of periodic points p is dense in X .

$\forall x \in X$ and $\forall U$, neighborhood of x $\exists p \in U$, and $n \in \mathbb{N}$ such that

$$f^n(p) = p. \quad (3.2)$$

3. f has sensitive dependence on initial condition.

A map is said to possess sensitive dependence on initial condition if there exists $\delta > 0$ then for all $x \in X$ and for all $\varepsilon > 0$ $n \in \mathbb{N}$ and $y \in X$ with $d(x, y) < \varepsilon \Rightarrow d(f^n(x), f^n(y)) > \delta$.

3.3 Tools for quantifying and measuring chaos

3.3.1 Lyapunov exponents

Many dynamical systems exhibit extreme sensitivity to initial conditions, a phenomenon known as the butterfly effect to distinguish such systems.

Alexander Lyapunov developed tools that allow us to measure the divergence between two trajectories of the same equation that start from very close initial conditions.

3.3.1.1 case of one dimensionnal discret systems

Theorem 3.1. [2] Let the discret dynamical system defined by:

$$x_{n+1} = f(x_n). \quad (3.3)$$

than f be a differentiable map, the Lyapunov exponent which measures sensitivity to initial conditions is given by:

$$\lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \ln |f'(x_i)|, \quad (3.4)$$

Proof. Let x_0 and x'_0 initial conditions, after repeating the composition N times we obtain:

$$x_N = f^N(x_0), \quad (3.5)$$

and

$$x'_N = f^N(x'_0), \quad (3.6)$$

so $\delta x_N = x_N - x'_N = f^N(x_0) - f^N(x'_0)$,

Applying the mean value theorem, we obtain:

$$\delta x_N = \frac{df^n(x_0)}{dx}(x_0 - x'_0) = \frac{df^n(x_0)}{dx}\delta x_0, \quad (3.7)$$

with

$$\frac{df^n(x_0)}{dx} = \prod_{i=0}^{N-1} f'(x_i)\delta x_0, \quad (3.8)$$

The philosophy of lyaponov states that the evolution of the solution is exponential with respect to the initial conditions, and this gives us:

$$\delta x_N = \prod_{i=0}^{N-1} f'(x_i)\delta x_0 = e^{\lambda N}\delta x_0, \quad (3.9)$$

so

$$e^{\lambda N} = \prod_{i=0}^{N-1} f'(x_i), \quad (3.10)$$

than

$$\lambda N = \sum_{i=0}^{N-1} |f'(x_i)| \Rightarrow \lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} |f'(x_i)|. \quad (3.11)$$

□

3.3.1.2 case of multy dimensionnal discret systems

Theorem 3.2. [2] *Let the discret dynamical system difined by:*

$$x_{n+1} = f(x_n). \quad (3.12)$$

than $f : R^n \longrightarrow R^n$ be a differentiable map, the Lyapunov exponent which measures sensitivity to initial conditions is given by

$$\lambda_i = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \ln q_i(f^k(x_0)). \quad (3.13)$$

Proof. Let x_0 and x'_0 initial conditions ,than $x'_0 = x_0 + \delta_0$.

after repeating the composition N times we obtain:

$$x_N = f^n(x_0). \quad (3.14)$$

and

$$x'_N = f^n(x'_0). \quad (3.15)$$

By applying the first order taylor expansion to f^n in a neighborhood of x_0 , we obtain :

$$f^n(x'_0) = f^n(x_0) + Df^n(x_0)(x'_0 - x_0). \quad (3.16)$$

so

$$\delta x_N = Df^n(x_0)\delta x_0. \quad (3.17)$$

with :

$$Df^n(x_0) = Df(x_{N-1})...Df(x_1)Df(x_0). \quad (3.18)$$

Let

$$Df(x_i) = J(x_i). \quad (3.19)$$

so :

$$\delta x_N = \prod_{i=0}^{N-1} J(x_i) \delta x_0. \quad (3.20)$$

we replace : $\prod_{i=0}^{N-1} J(x_i)$, by $J^N(x_0)$.

if $J^N(x_0)$ diagonalisable, there existe an invertible matrix P than $D^N = P^{-1}J^N P$ with the eigen values $q_i(f^k(x_0))$.

we defined the p lyapunov exponents by:

$$\lambda_i = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \ln q_i(f^k(x_0)). \quad (3.21)$$

□

Dynamical Regime	Lyapunov Exponent Spectrum	Characteristic
Fixed Point	All $\lambda_i < 0$	Exponential convergence to a single equilibrium.
Periodic Orbit	One $\lambda_1 = 0$, and all others $\forall i > 1 : \lambda_i < 0$	Neutral direction along the cycle; contraction transverse to it.
Quasi-Periodic	k exponents $\lambda_1 = \lambda_2 = \dots = \lambda_k = 0$, rest < 0	Invariant k -torus; motion with k incommensurate frequencies.
Chaotic	Exactly one $\lambda_1 > 0$, all others ≤ 0	Sensitive dependence on initial conditions; strange attractor of fractal geometry.
Hyperchaotic	At least two $\lambda_1, \lambda_2 > 0$, rest ≤ 0	Two (or more) expanding directions; more complex attractor with higher information dimension.

Table 3.1: Lyapunov exponent conditions and their corresponding dynamical regimes.

3.3.2 Bifurcation diagram

Definition 3.2. [3] is a graphical tool used to study how the long term behavior of a dynamical system changes when a parametre varies.

the diagram allows us to observe

- sensitive dependence on initial conditions
- dense and irregular regions
- the emergence of periodic cycles

thus it enables us to verify all the conditions of Devany definition of chaos.

3.3.2.1 Role of Bifurcations in Chaos

Bifurcations are fundamental in the transition to chaos. For example, a cascade of **period-doubling** bifurcations lead to a chaotic regime, while **Neimark-Sacker** bifurcations introduce **quasiperiodic behavior** that results in complex, chaotic dynamics.

3.3.3 Fractal Dimensions

Fractal geometry will make you see everything differently, there is danger in reading further, you risk the loss of your childhood vision of clouds, forest, galaxies, leaves, feathers, flowers, rocks, torrents of water, carpets, bricks, and much else besides, never again will your interpretation of these things be quite the same.

Michael barnsley

Definition 3.3. [11] is a non-integer number used to measure the degree of complexity of a shape. it differs from the classical definition of dimension; it does not rely on linearly independent vectors, but rather on self-similarity.

Definition 3.4. [11] Let λ_i denote the lyapunov exponents ordered as $\lambda_1 \geq \lambda_2 \geq \dots$ and let j , be the largest index such that :

$$\sum_{i=1}^j \lambda_i \geq 0. \quad (3.22)$$

Then the Kaplan-Yorke dimension is defined by :

$$D_{KY} = j + \frac{\sum_{i=1}^j \lambda_i}{|\lambda_{j+1}|}. \quad (3.23)$$

3.3.3.1 fractals and chaos

In chaotic systems, the phase space is not filled in a regular manner, rather the trajectories accumulate on a set which gives rise to a fractal dimension, this fractal dimension is also considered a good measure of the intensity of chaos.

3.4 Summary

This chapter introduced the chaos tools. We discussed the definition of chaos, including sensitivity to initial conditions, topological mixing, and the density of periodic orbits. Lyapunov exponents were presented for measuring sensitivity, and their role in stability was clarified through the associated theorem, we examined fractal dimensions and strange attractors, linking them to Lyapunov exponents via the Kaplan-Yorke conjecture.

Chapter 4

Famous discrete dynamical systems

This chapter examines fundamental discrete-time chaotic maps that serve as canonical models in chaos theory. These include the Logistic, Hénon, Lozi, and Boukhalifa maps. Each system is analyzed through its defining equations, attractor geometry, bifurcation structure, and Lyapunov exponent evolution to highlight the onset and development of chaos in low-dimensional dynamics, in the end, we will take an example of one of the applications of chaos in cryptography.

4.1 Logistic Map

Definition 4.1. [6] The *Logistic map* is a discrete dynamical system, defined by :

$$x_{n+1} = rx_n(1 - x_n), \quad (4.1)$$

where:

- x_n is the state variable at time step n ,
- r is a real parameter that influences the system's behavior.

Strange Attractor Plot

The figure below presents the scatter plot of the Logistic map's strange attractor for the parameter value: $r = 3.9$

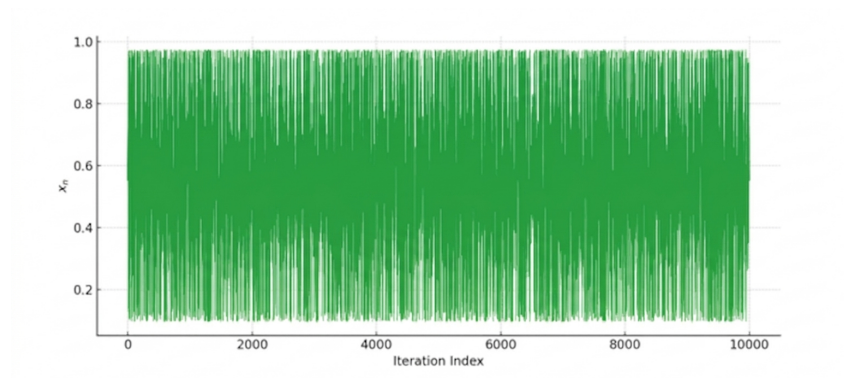


Figure 4.1: Logistic Map Attractor for $r = 3.9$.

The first 1,000 iterates are discarded as transients, and the subsequent 100,000 points are also plotted to show the strange attractor.

First 100 Iterations

The time series plot below shows the evolution of x_n over the first 100 iterations, starting from: $x_0 = 0.4$

The resulting sequence displays irregular, non-repeating fluctuations indicative of chaotic behavior.

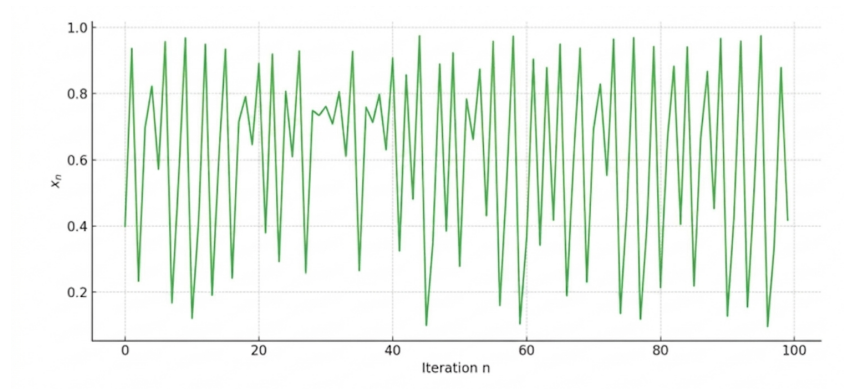


Figure 4.2: Logistic Map – First 100 Iterations of x_n

4.1.1 Fixed point and stability

We can obtain the fixed points of the Henon map by setting :

$$f_r(x) = x. \quad (4.2)$$

So

$$rx(1 - x) = x. \quad (4.3)$$

Thus, the fixed points are :

$$x_1 = 0, x_2 = \frac{r-1}{r}. \quad (4.4)$$

The stability of the fixed point depends on the absolute value of $f'(x) = r - 2rx$
Since

$$|f'(0)| = |r| = r. \quad (4.5)$$

The fixed point $x_1 = 0$ is stable when $r < 1$ and unstable when $r > 1$.

Again, since :

$$|f'(\frac{r-1}{r})| = |2 - r| < 1. \quad (4.6)$$

The fixed point $x_2 = \frac{r-1}{r}$ is stable when $1 < r < 3$ and unstable when $3 < r < 4$.

4.1.2 Bifurcation diagram

By varying the parameter r from 2.5 to 4.0 and fixing the initial condition: $x_0 = 0.4$, we obtain the bifurcation diagram by discarding the first 1,000 transient values and plotting the next 100 iterates of x_n for each r . This diagram demonstrates the period-doubling route to chaos.

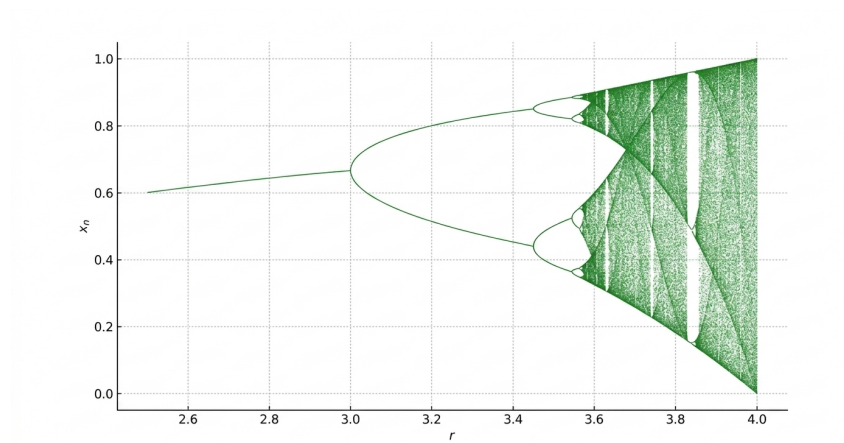


Figure 4.3: Logistic Map Bifurcation Diagram for $x_0 = 0.4$

4.1.3 Chaos in Logistique map

This visualization shows how the Lyapunov exponent changes as parameter r varies from 2.5 to 4.0. Note the transition to positive values (above the gray line) marking the onset of chaos, and the complex structure with periodic windows where the exponent dips below zero.

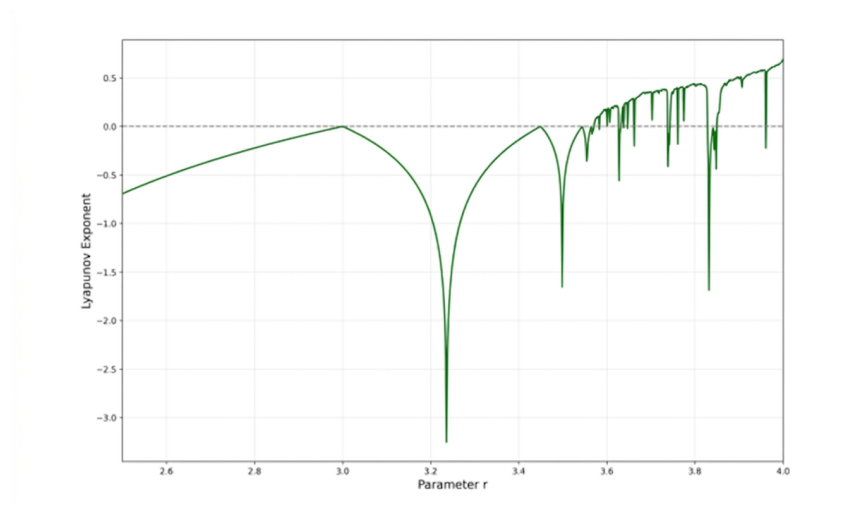


Figure 4.4: Logistic Map : Lyapunov Exponent Evolution

4.2 Henon map

Definition 4.2. [12] The Henon map it is a two-dimensional discret time dynamical system defined by the following expression :

$$\begin{cases} x_{n+1} = -ax_n^2 + y_n + 1, \\ y_{n+1} = bx_n. \end{cases} \quad (4.7)$$

where $a, b \in R$, a is parameter that controls the nonlinearity of the system , and b represents the role of dissipation .

4.2.0.1 Strange Attractor Plot

The figure below presents the scatter plot of the Hénon attractor for

$$a = 1.4, \quad b = 0.3.$$

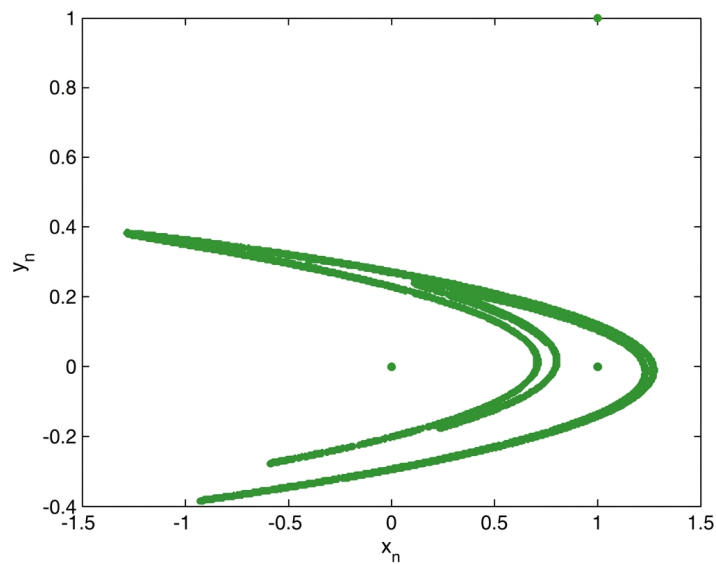


Figure 4.5: Hénon Strange Attractor for $a = 1.4$, $b = 0.3$.

4.2.0.2 First 100 Iterations

The time series of x_n over the first 100 iterations, starting from $(x_0, y_0) = (0, 0)$, reveals a non-repeating, irregular fluctuation indicative of chaotic dynamics:

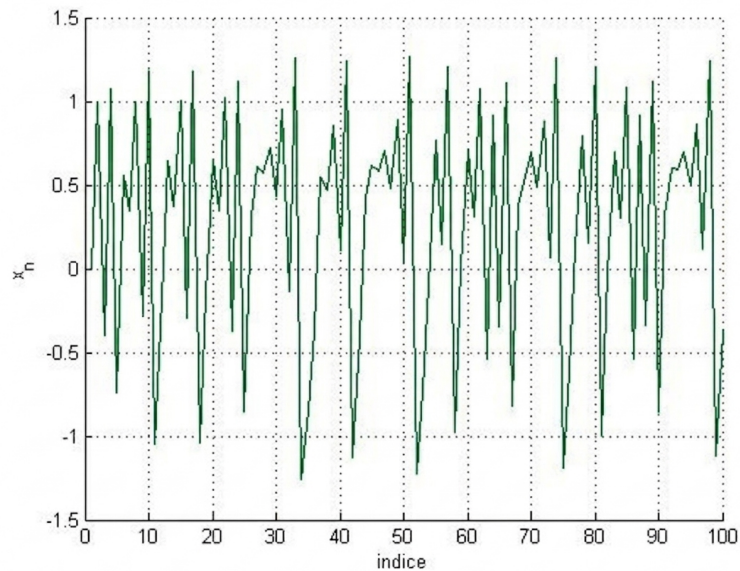


Figure 4.6: Hénon Map – First 100 Iterations of x_n

The time series of y_n over the first 100 iterations, starting from $(x_0, y_0) = (0, 0)$, reveals a non-repeating, irregular fluctuation indicative of chaotic dynamics:

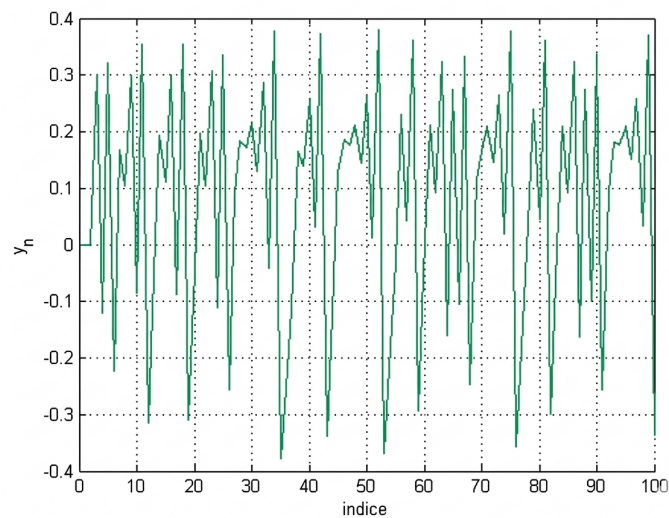


Figure 4.7: Hénon Map – First 100 Iterations of y_n

4.2.1 Fixed points and stability

We can obtain the fixed points of the Henon map by setting :

$$H_{a,b}(x, y) = (x, y). \quad (4.8)$$

so

$$\begin{cases} -ax^2 + y + 1 = x, \\ bx = y. \end{cases} \quad (4.9)$$

Then : $-ax^2 + (b-1)x + 1 = 0 \Rightarrow \Delta = (b-1)^2 + 4a$.

Here, we distinguish three different cases :

1. $\Delta < 0$: the equation has no real roots $\Rightarrow$ there are no fixed points.
2. $\Delta = 0$: the equation has a double root.

Thus, the fixed point are : $P = (\frac{b-1}{2a}, \frac{b(b-1)}{2a})$.

3. $\Delta > 0$: the equation has two distinct real roots.

Thus, the fixed points are :

$$P_1 = (\frac{b-1-\sqrt{\Delta}}{2a}, \frac{b(b-1-\sqrt{\Delta})}{2a}), P_2 = (\frac{b-1+\sqrt{\Delta}}{2a}, \frac{b(b-1+\sqrt{\Delta})}{2a}). \quad (4.10)$$

The Jacobian matrix of Henon map is :

$$J_{(x,y)} = \begin{pmatrix} -2ax & 1 \\ b & 0 \end{pmatrix}, \quad (4.11)$$

At the fixed point P_1 the characteristic polynomial is :

$$\lambda^2 + (b-1-\sqrt{\Delta})\lambda - b, \quad (4.12)$$

The eigenvalues are

$$\lambda_{1,2} = \frac{1-b+\sqrt{\Delta} \pm \sqrt{(b-1-\sqrt{\Delta})^2 + 4b}}{2}, \quad (4.13)$$

At the fixed point P_2 the characteristic polynomial is :

$$\lambda^2 + (b-1+\sqrt{\Delta})\lambda - b. \quad (4.14)$$

The eigenvalues are

$$\lambda_{1,2}^* = \frac{1-b-\sqrt{\Delta} \pm \sqrt{(b-1+\sqrt{\Delta})^2 + 4b}}{2}. \quad (4.15)$$

4.2.2 Bifurcation study

For : $a = \frac{-(b-1)^2}{4}$, Henon map admits a single equilibrium point : $P = (\frac{b-1}{2a}, \frac{b(b-1)}{2a})$. The eigenvalues of jacobian matrix in this point is $\{1; b\}$ and that gives rise to a saddle node bifurcation.

4.2.2.1 Bifurcation diagram

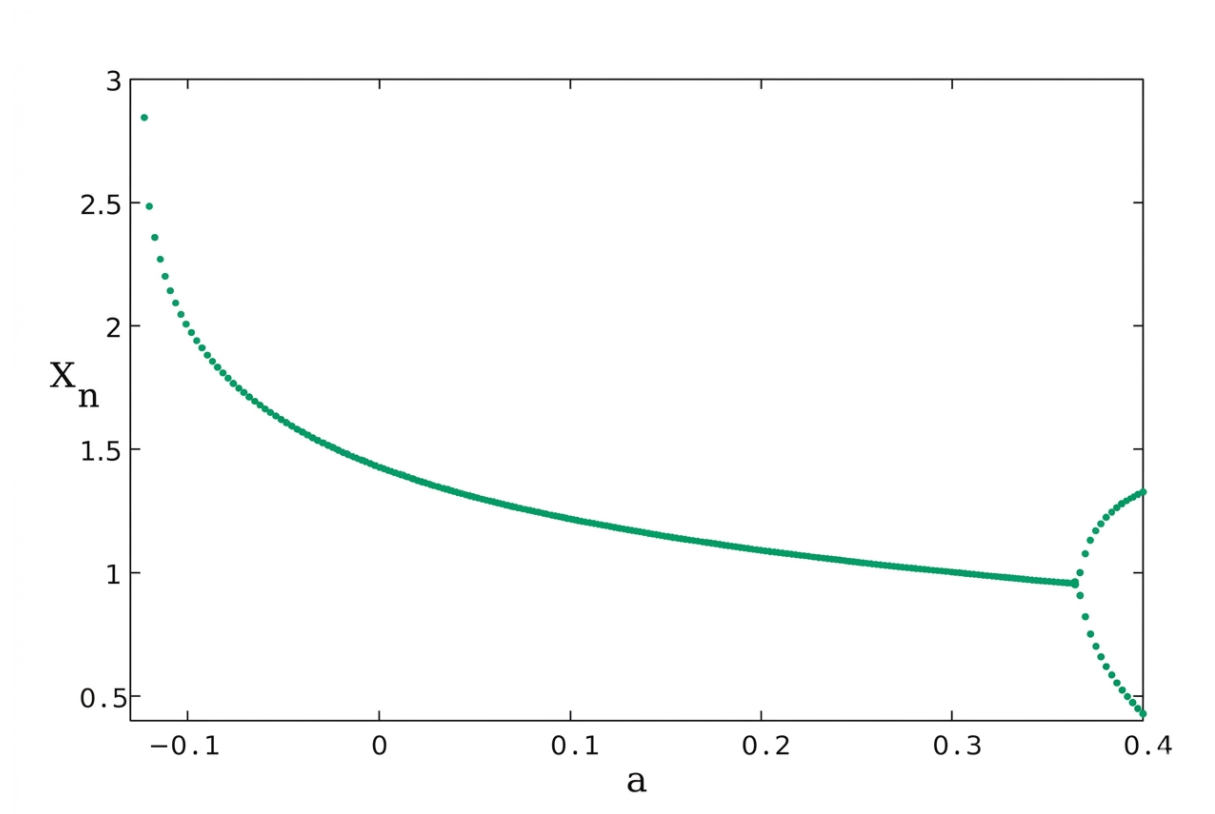


Figure 4.8: Bifurcation diagram of Henon map

4.2.3 Chaos in Henon map

When studying the stability of the Henon system, we find that the eigen values are expressed in terms of the fixed points, and this latter are expressed in terms of a and b . Therefore in order to derermine all regions of stability, the lyapunov exponents must be computed in terms of the parameters a and b .

Let $b = 0.3$ and a vary between 0 and 1.4.

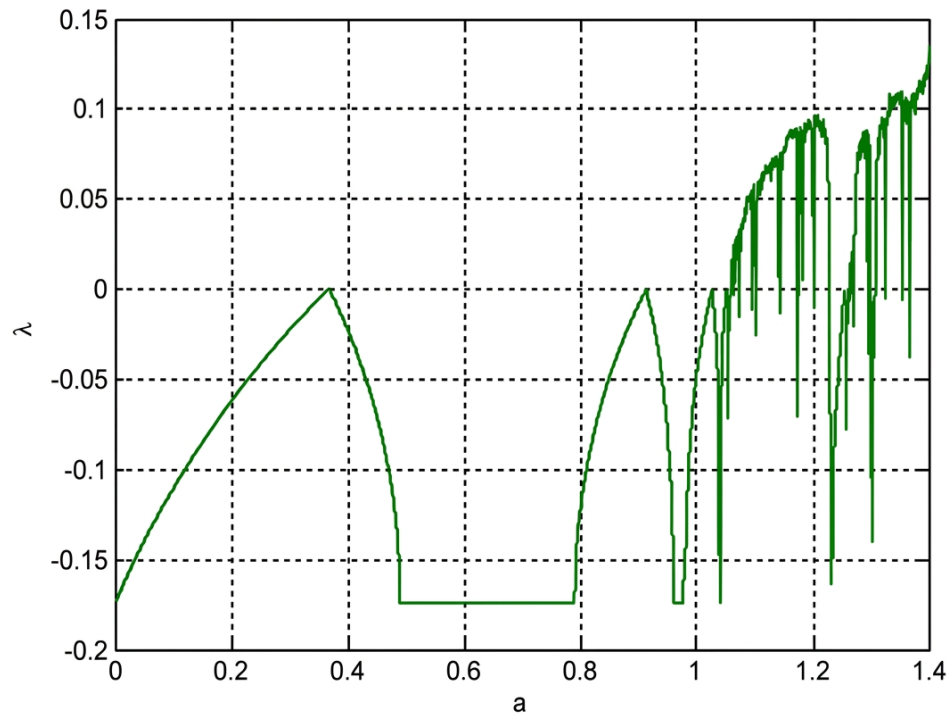


Figure 4.9: Hénon Map : Lyapunov Exponent Evolution

4.3 Lozi Map

Definition 4.3. [16] The *Lozi map* is a two-dimensional discrete-time dynamical system defined by:

$$\begin{cases} x_{n+1} = 1 - a|x_n| + y_n, \\ y_{n+1} = b x_n, \end{cases} \quad (4.16)$$

where $a, b \in \mathbb{R}$. This map was introduced by R. Lozi as a piecewise-linear simplification of the *Hénon map*.

4.3.0.1 Strange Attractor Plot

The long-term behavior of the system reveals a fractal geometric structure known as the *Lozi attractor*. The figure below shows a scatter plot of the trajectory (x_n, y_n) with parameters

$$a = 1.7, \quad b = 0.5.$$

The first 1000 iterates are discarded as transients, and the following 100 000 points are plotted:

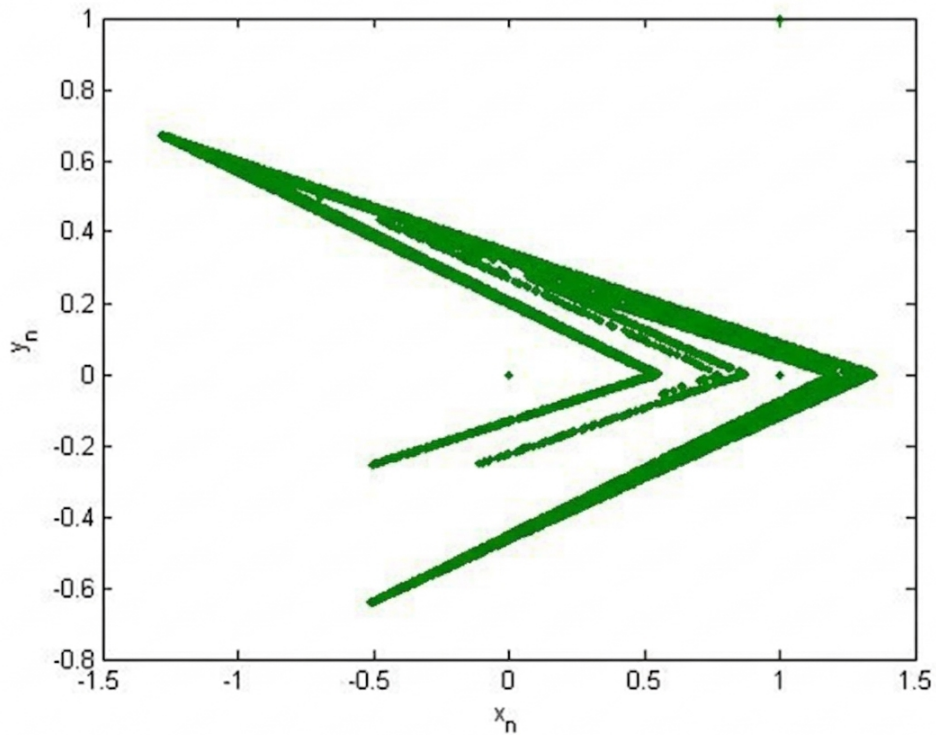


Figure 4.10: Lozi Strange Attractor for $a = 1.7$, $b = 0.5$.

4.3.0.2 First 100 Iterations

Starting from the initial condition $(x_0, y_0) = (0, 0)$, the time series of x_n for the first 100 iterations exhibits irregular and non-periodic fluctuations, indicating the presence of chaotic dynamics:

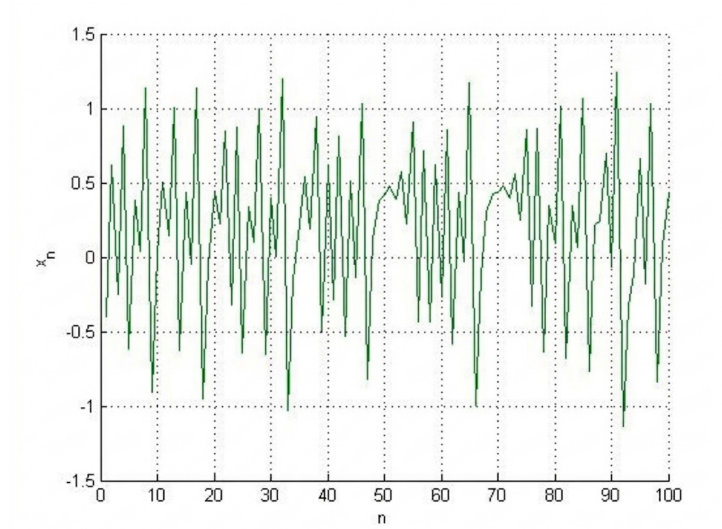


Figure 4.11: Lozi Map – First 100 Iterations of x_n .

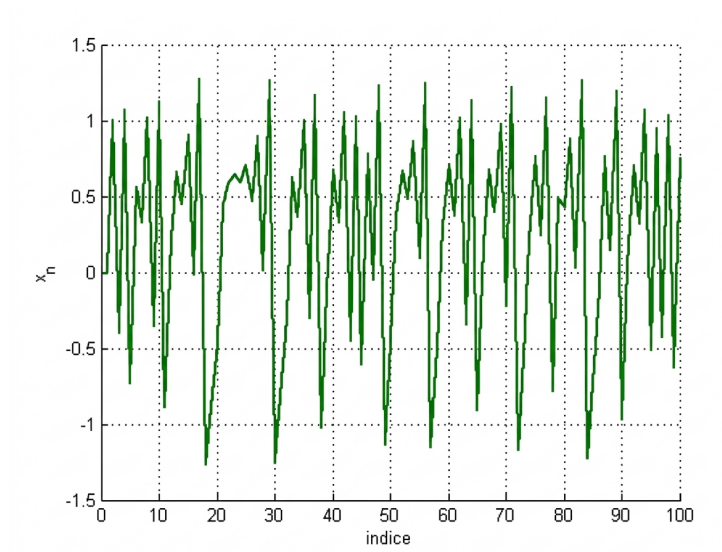


Figure 4.12: Lozi Map – First 100 Iterations of y_n .

4.3.1 Fixed points and stability

We can obtain the fixed points of the Lozi map by setting :

$$L_{a,b}(x, y) = (x, y). \quad (4.17)$$

So :

$$\begin{cases} -a|x| + y + 1 = x, \\ bx = y. \end{cases} \quad (4.18)$$

Then

$$-a|x| + (b - 1)x + 1 = 0. \quad (4.19)$$

We can distinguish two different cases :

$$x > 0 \Rightarrow x = \frac{1}{a - b + 1} \text{ and } a > b - 1.$$

$$x < 0 \Rightarrow x = \frac{1}{1 - a - b} \text{ and } a > 1 - b.$$

Thus the fixed points are :

$$P_1 = \left(\frac{1}{a - b + 1}, \frac{b}{a - b + 1} \right), P_2 = \left(\frac{1}{1 - a - b}, \frac{b}{1 - a - b} \right). \quad (4.20)$$

The Jacobian matrix of Lozi map is :

$$J_{(x,y)} = \begin{pmatrix} -asing(x) & 1 \\ b & 0 \end{pmatrix}. \quad (4.21)$$

At the fixed point P_1 the characteristic polynomial is :

$$\lambda^2 + a\lambda - b. \quad (4.22)$$

The eigenvalues are :

$$\lambda_{1,2} = \frac{-a \pm \sqrt{a^2 + 4b}}{2}. \quad (4.23)$$

At the fixed point P_2 the characteristic polynomial is

$$\lambda^2 - a\lambda - b. \quad (4.24)$$

The eigenvalues are

$$\lambda_{1,2}^* = \frac{a \pm \sqrt{a^2 + 4b}}{2}. \quad (4.25)$$

4.3.1.1 stability of P_1

Proposition. The point P_1 is stable when the pair (a, b) belongs to the open triangle whose vertices are $(0,1), (-2,-1), (2,-1)$.

Proposition. When $b > a + 1$ and $b > a - 1$ the fixed point P_1 becomes a saddle point.

4.3.1.2 stability of P_2

Proposition. The point P_2 is unstable when : $b > -a + 1$ and $b > a + 1$.

Proposition. When $b > -a + 1$ and $b > a + 1$ the fixed point P_2 becomes a saddle point.

4.3.2 Bifurcation diagram

Figure (4.13) represent the bifurcation diagram of the Lozi system, where we observe that the system enters chaotic behavior as a approaches 1.5

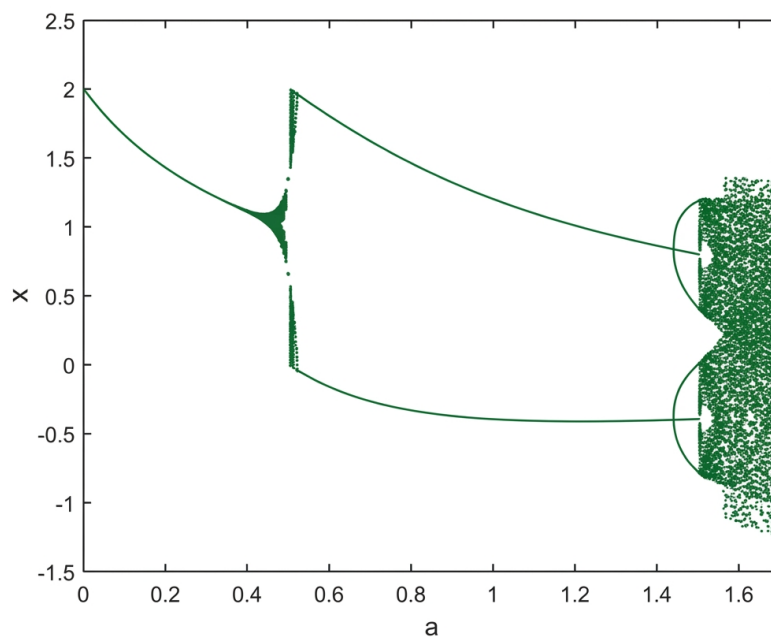


Figure 4.13: Lozi Map : Bifurcation diagram

4.3.3 Chaos in Lozi map

This shows the Lyapunov exponent of the Lozi map as parameter a varies from 0.5 to 1.7 with fixed $b = 0.5$. Note the distinct transition points and regions of chaos.

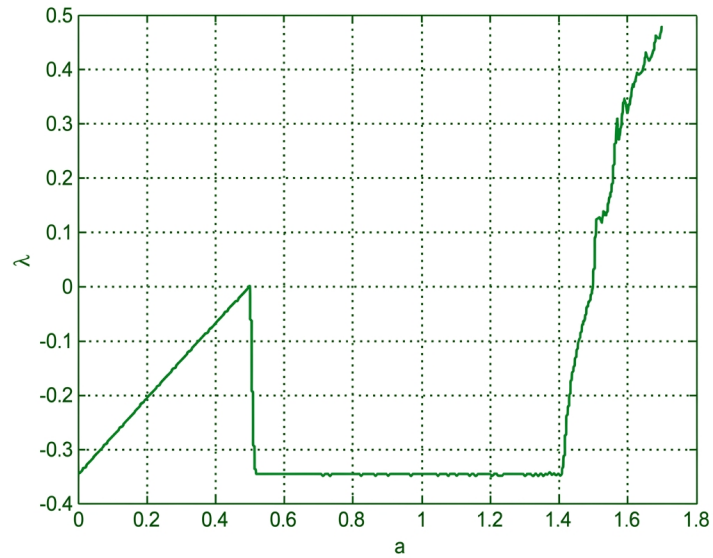


Figure 4.14: Lozi Map : Lyapunov Exponent Evolution

4.4 Boukhalfa map

Definition 4.4. [4] Consider the 2-D discrete dynamical system $B_{a,b}$ defined by:

$$B_{a,b} \begin{cases} x_{n+1} = ax_n(1 - y_n^2), \\ y_{n+1} = bx_n, \end{cases} \quad a, b \in \mathbb{R}. \quad (4.26)$$

4.4.0.1 First 50 iteration

Figure (4.15) illustrates the first fifty iterations of the Boukhalfa map for different initial conditions and varying parameter values.

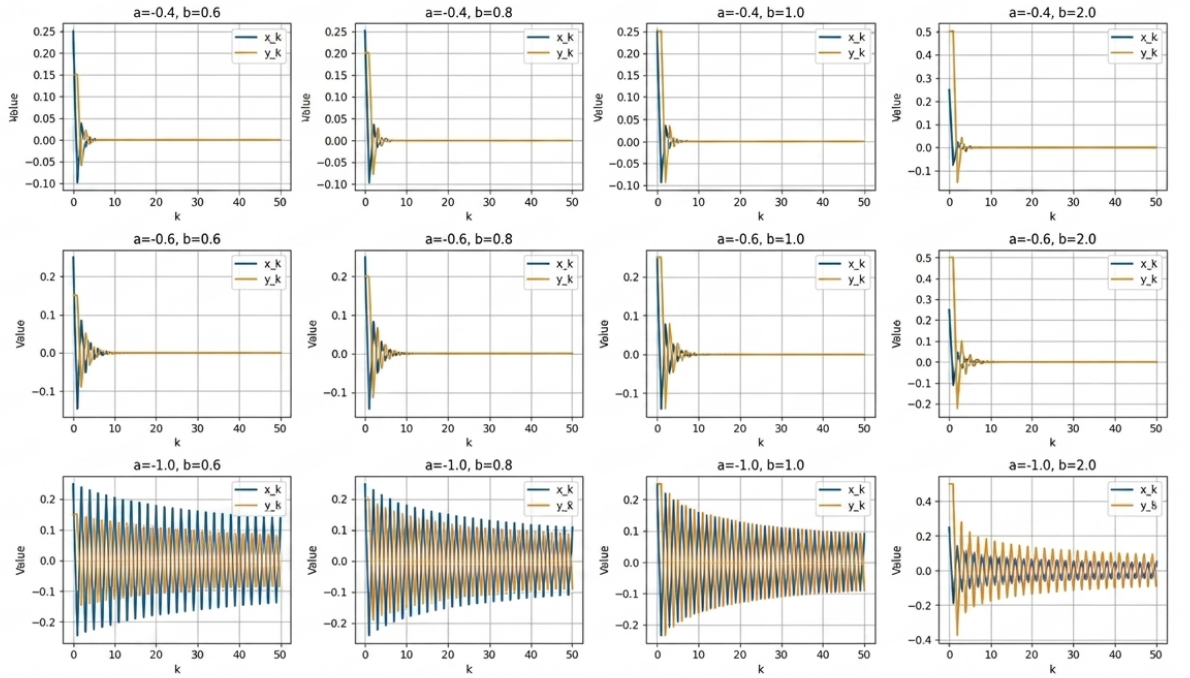


Figure 4.15: first 50 iteration

Proposition. *The system (4.26) has the following properties:*

1. It is defined for all $(x, y) \in \mathbb{R}^2$.
2. It is symmetric for all $(x, y) \in \mathbb{R}^2$.
3. It has a quadratic form.
4. It is defined by a function of class $C^\infty(\mathbb{R}^2)$.

4.4.1 Fixed Points stability

4.4.1.1 fixed point

Let the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be defined by:

$$f(x, y) = \begin{pmatrix} ax(1 - y^2) \\ bx \end{pmatrix}.$$

The fixed points of the system (4.26) satisfy:

$$\begin{cases} x = ax(1 - y^2), \\ y = bx. \end{cases} \quad (4.27)$$

For $x \neq 0$, from the first equation:

$$1 = a(1 - y^2) \implies y^2 = 1 - \frac{1}{a} = \frac{a-1}{a} \implies y = \pm \sqrt{\frac{a-1}{a}}.$$

From the second equation, $y = bx \implies x = \frac{y}{b}$. Substituting $y = \pm \sqrt{\frac{a-1}{a}}$:

$$x = \pm \frac{1}{b} \sqrt{\frac{a-1}{a}}.$$

Thus, the fixed points are:

$$P_1 = \left(\frac{1}{b} \sqrt{\frac{a-1}{a}}, \sqrt{\frac{a-1}{a}} \right), \quad P_2 = \left(-\frac{1}{b} \sqrt{\frac{a-1}{a}}, -\sqrt{\frac{a-1}{a}} \right),$$

provided $a \neq 0$ and $b \neq 0$.

4.4.1.2 stability

The Jacobian matrix of the system (4.26) is:

$$Df(x, y) = \begin{bmatrix} a(1 - y^2) & -2axy \\ b & 0 \end{bmatrix}. \quad (4.28)$$

At the fixed point $P_1\left(\frac{1}{b}\sqrt{\frac{a-1}{a}}, \sqrt{\frac{a-1}{a}}\right)$, the Jacobian is:

$$Df(P_1) = \begin{bmatrix} a\left(1 - \frac{a-1}{a}\right) & -2a \cdot \frac{1}{b}\sqrt{\frac{a-1}{a}} \cdot \sqrt{\frac{a-1}{a}} \\ b & 0 \end{bmatrix} = \begin{bmatrix} 1 & -\frac{2(a-1)}{b} \\ b & 0 \end{bmatrix}.$$

the characteristic polynomial is:

$$\det(A - \lambda I) = \lambda(\lambda - 1) + 2(a - 1) = \lambda^2 - \lambda + 2(a - 1).$$

The discriminant is:

$$\Delta = 1 - 8(a - 1) = 9 - 8a > 0, \quad \text{for } a < \frac{9}{8}. \quad (4.29)$$

The eigenvalues are:

$$\lambda_1 = \frac{1 - \sqrt{9 - 8a}}{2}, \quad \lambda_2 = \frac{1 + \sqrt{9 - 8a}}{2}.$$

For $|\lambda_1| < 1$:

$$-1 < \frac{1 - \sqrt{9 - 8a}}{2} < 1 \implies -3 < -\sqrt{9 - 8a} < 1.$$

$$-3 < -\sqrt{9 - 8a} \implies 3 > \sqrt{9 - 8a} \implies 9 > 9 - 8a \implies a > 0. \quad -\sqrt{9 - 8a} < 1 \implies \sqrt{9 - 8a} > -1, \text{ which is always true.}$$

Thus, $|\lambda_1| < 1$ for $a \in (0, \frac{9}{8})$.

For $|\lambda_2| < 1$:

$$-1 < \frac{1 + \sqrt{9 - 8a}}{2} < 1 \implies -3 < \sqrt{9 - 8a} < 1.$$

$$-\sqrt{9 - 8a} > -3, \text{ which is always true. } -\sqrt{9 - 8a} < 1 \implies 9 - 8a < 1 \implies a > 1.$$

Thus, $|\lambda_2| < 1$ for $a \in (1, \frac{9}{8})$.

4.4.2 Period Doubling

To find 2-cycles, compute $f^2(x, y) = f(f(x, y)) = (x, y)$:

$$f^2(x, y) = \begin{pmatrix} a(ax(1-y^2))(1-(bx)^2) \\ b(ax(1-y^2)) \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}. \quad (4.30)$$

This gives:

$$\begin{cases} a^2x(1-y^2)(1-b^2x^2) = x, \\ bax(1-y^2) = y. \end{cases} \quad (4.31)$$

From the second equation:

$$x = \frac{y}{ab(1-y^2)}, \quad a \neq 0, \quad b \neq 0, \quad y^2 \neq 1. \quad (4.32)$$

Substitute into the first equation:

$$a^2 \left(\frac{y}{ab(1-y^2)} \right) (1-y^2) \left(1 - b^2 \left(\frac{y}{ab(1-y^2)} \right)^2 \right) = \frac{y}{ab(1-y^2)}. \quad (4.33)$$

Simplify:

$$a \left(1 - \frac{y^2}{a^2(1-y^2)^2} \right) = \frac{1}{ab^2(1-y^2)}. \quad (4.34)$$

Multiply through by $ab^2(1-y^2)$:

$$a^2b^2(1-y^2) \left(1 - \frac{y^2}{a^2(1-y^2)^2} \right) = 1. \quad (4.35)$$

This simplifies to:

$$a^2y^4 - 2a^2y^2 + a^2 - 1 = 0. \quad (4.36)$$

Let $t = y^2$:

$$a^2t^2 - 2a^2t + a^2 - 1 = 0. \quad (4.37)$$

Solutions are:

$$t = \frac{a-1}{a}, \quad t = \frac{a+1}{a}, \quad \text{for } a \neq 0. \quad (4.38)$$

Thus:

$$y_{1,2} = \pm \sqrt{\frac{a-1}{a}}, \quad y_{3,4} = \pm \sqrt{\frac{a+1}{a}}. \quad (4.39)$$

Corresponding x -values are:

- For $y_1 = \sqrt{\frac{a-1}{a}}$: $x_1 = \frac{1}{b}\sqrt{\frac{a-1}{a}}$, giving $P_1^2 = P_1$.
- For $y_2 = -\sqrt{\frac{a-1}{a}}$: $x_2 = -\frac{1}{b}\sqrt{\frac{a-1}{a}}$, giving $P_2^2 = P_2$.
- For $y_3 = \sqrt{\frac{a+1}{a}}$: $x_3 = \frac{1}{b}\sqrt{\frac{a+1}{a}}$, giving $P_3^2 = \left(\frac{1}{b}\sqrt{\frac{a+1}{a}}, \sqrt{\frac{a+1}{a}} \right)$.
- For $y_4 = -\sqrt{\frac{a+1}{a}}$: $x_4 = -\frac{1}{b}\sqrt{\frac{a+1}{a}}$, giving $P_4^2 = \left(-\frac{1}{b}\sqrt{\frac{a+1}{a}}, -\sqrt{\frac{a+1}{a}} \right)$.

Thus, the 2-cycle points are P_3^2 and P_4^2 , with P_1^2 and P_2^2 being fixed points.

4.4.3 Bifurcation diagram

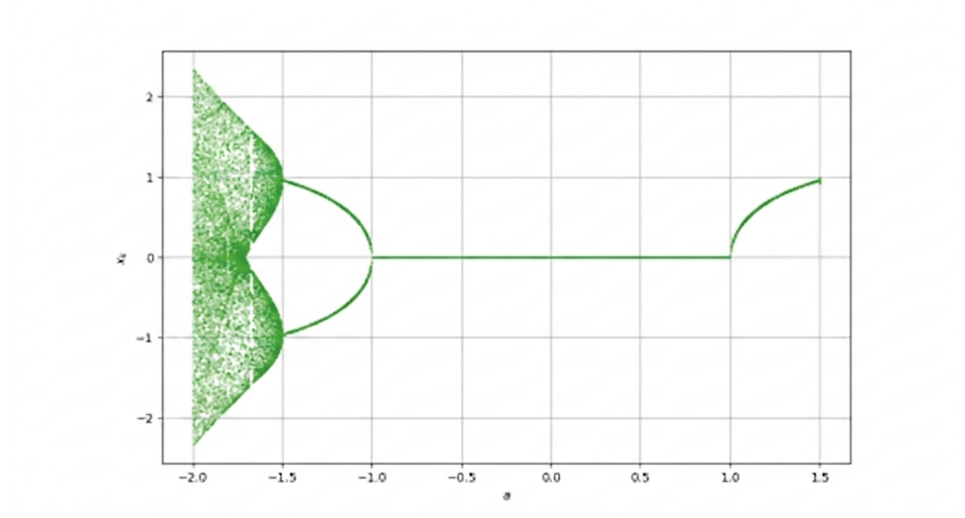


Figure 4.16: Bifurcation diagram of system (4.26) for a with $b = 0.6$

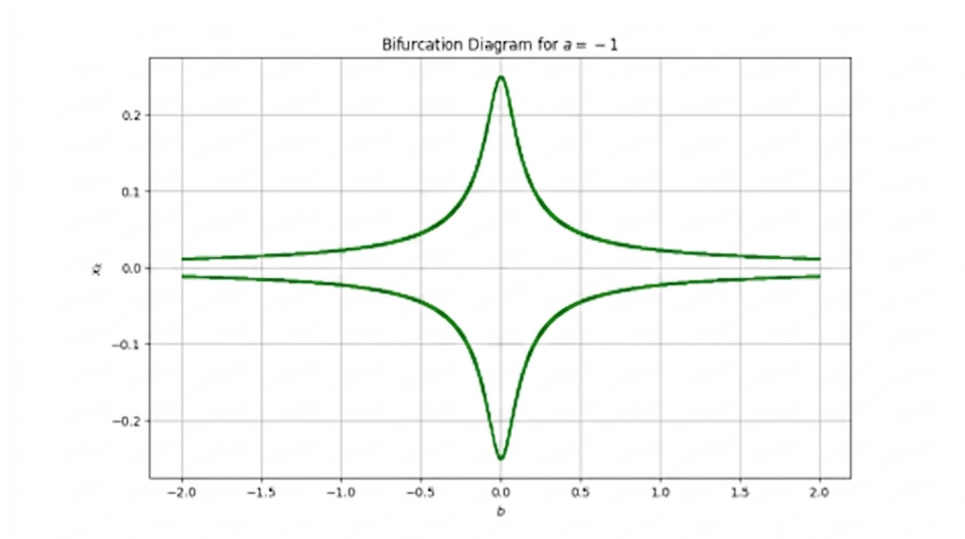


Figure 4.17: Bifurcation diagram of system (4.26) for b with $a = -1$

4.4.4 Chaos in boukhalfa map

4.4.4.1 lyapunov exponents

Lyapunov exponents quantify sensitivity to initial conditions (SIC) and distinguish chaotic from stable behavior:

1. If a Lyapunov exponent is positive, the system exhibits SIC and is chaotic.
2. If all Lyapunov exponents are non-positive, the system is stable or periodic.

The Jacobian matrix is:

$$J(x, y) = \begin{pmatrix} a(1 - y^2) & -2axy \\ b & 0 \end{pmatrix}. \quad (4.40)$$

At P_1 , the Jacobian is:

$$J(P_1) = \begin{pmatrix} 1 & -\frac{2(a-1)}{b} \\ b & 0 \end{pmatrix}. \quad (4.41)$$

The eigenvalues are:

$$\lambda_1 = \frac{1 - \sqrt{9 - 8a}}{2}, \quad \lambda_2 = \frac{1 + \sqrt{9 - 8a}}{2}. \quad (4.42)$$

The Lyapunov exponents are:

$$E_1 = \ln \left| \frac{1 + \sqrt{9 - 8a}}{2} \right|, \quad E_2 = \ln \left| \frac{1 - \sqrt{9 - 8a}}{2} \right|. \quad (4.43)$$

Theorem 4.1. *The system (4.26) is chaotic for $a < 1$.*

Proof.

$$E_1 = \ln \left| \frac{1 + \sqrt{9 - 8a}}{2} \right| > 0 \iff \frac{1 + \sqrt{9 - 8a}}{2} > 1 \iff \sqrt{9 - 8a} > 1 \iff a < 1.$$

□

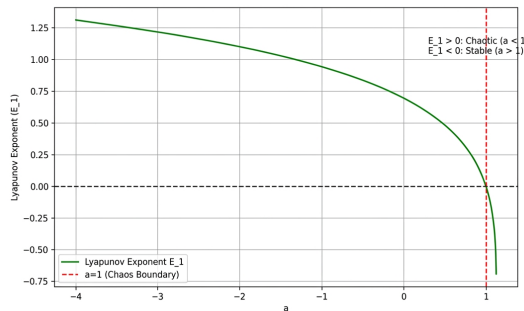


Figure 4.18: Evolution of Lyapunov exponent E_1

4.5 Application of chaotic maps in crypto-graphy

Chaotic systems are designed to generate highly unpredictable patterns. By leveraging chaotic maps as mathematical functions that produce random-like outputs, encryption systems can shuffle and transform pixel values in ways that are extremely difficult to reverse. Even slight changes in the original image can drastically alter the encrypted output, reinforcing security. Key benefits of using chaotic maps in image encryption are: Due to their sensitivity to initial conditions, chaotic systems can generate unpredictable encryption keys. This makes deciphering encrypted images without the correct key virtually impossible. Attackers face a chaotic web of possibilities, making brute-force attempts highly ineffective. Chaos-based algorithms are computationally efficient, making them ideal for encrypting large data sets like high-resolution images. By rapidly generating complex patterns, chaotic encryption systems balance security with performance — a crucial advantage in image-intensive environments.

4.5.1 Definition of a grayscale image

A grayscale image is a digital image in which each pixel is represented by a single intensity value corresponding to a shade of gray, the pixel intensity generally ranges from 0 (black) to 255 (white).

4.5.2 Grayscale levels

A byte consists of 8 bits, where each bit can take either the value 0 or 1, therefore the total number of possible states is: $2^8 = 256$, hence, a single byte can represent 256 different values ranging from 0 to 255.

Grayscale Levels (0 - 255)															
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

Figure 4.19: Grayscale levels

4.5.3 The importance of using the Boukhalfa map

The efficiency of the Boukhalfa map lies in two important aspects:

1. It is a chaotic map that generates random numbers which are difficult to track using statistical methods, in addition its sensitivity to initial conditions means that any small change in them produces completely different results, making it difficult to recover the original image.
2. It provides a second layer of protection, because the Boukhalfa map has not been extensively studied or widely used.

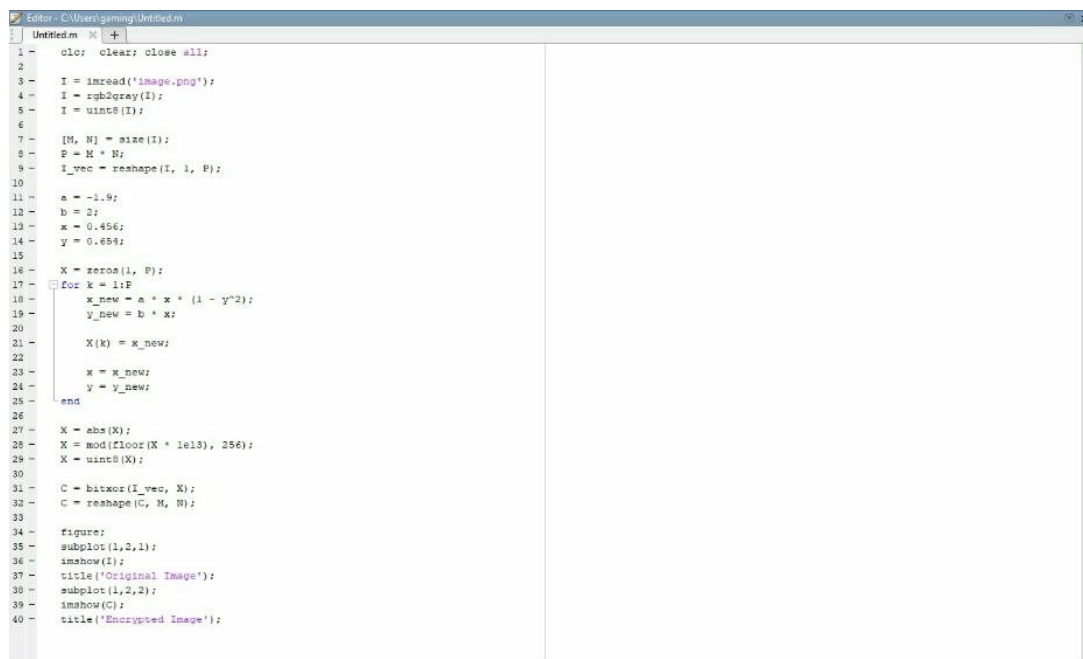
4.5.4 MATLAB code explanation

We can divide the code into six main stages:

- Image reading.
- Converting the image into a vector.
- Entering the parameters of the chaotic system and the initial conditions.
- Generating the sequences based on the Boukhalfa map and forming the chaotic key.
- Encryption using XOR where $C = I \oplus X$.
- Displaying both the original image and the encrypted image.

Remark. Here, the process can be easily reversed when the chaotic key is available, because simply: $I = C \oplus X$

Figure (4.20) represents a MATLAB algorithm for encrypting a grayscale image :



```
1 - clear; close all;
2
3 - I = imread('image.png');
4 - I = rgb2gray(I);
5 - I = uint8(I);
6
7 - [M, N] = size(I);
8 - P = M * N;
9 - I_vec = reshape(I, 1, P);
10
11 - a = -1.9;
12 - b = 2;
13 - x = 0.456;
14 - y = 0.654;
15
16 - X = zeros(1, P);
17 - for k = 1:P
18 -     x_new = a * x * (1 - y^2);
19 -     y_new = b * x;
20
21 -     X(k) = x_new;
22
23 -     x = x_new;
24 -     y = y_new;
25 - end
26
27 - X = abs(X);
28 - X = mod(floor(X * 1e13), 256);
29 - X = uint8(X);
30
31 - C = bitxor(I_vec, X);
32 - C = reshape(C, M, N);
33
34 - figure;
35 - subplot(1,2,1);
36 - imshow(I);
37 - title('Original Image');
38 - subplot(1,2,2);
39 - imshow(C);
40 - title('Encrypted Image');
```

Figure 4.20: MATLAB programme for encrypting a grayscale image

Finally, we present a grayscale image encrypted using the Boukhalfa map.

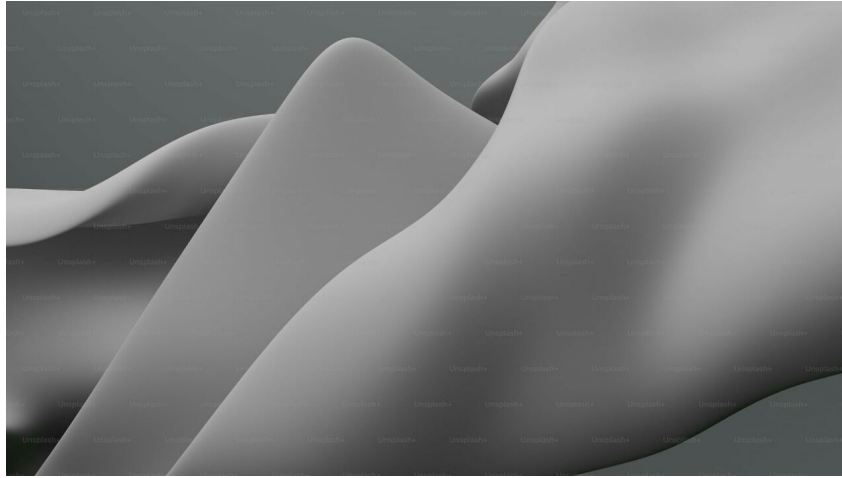


Figure 4.21: Original image

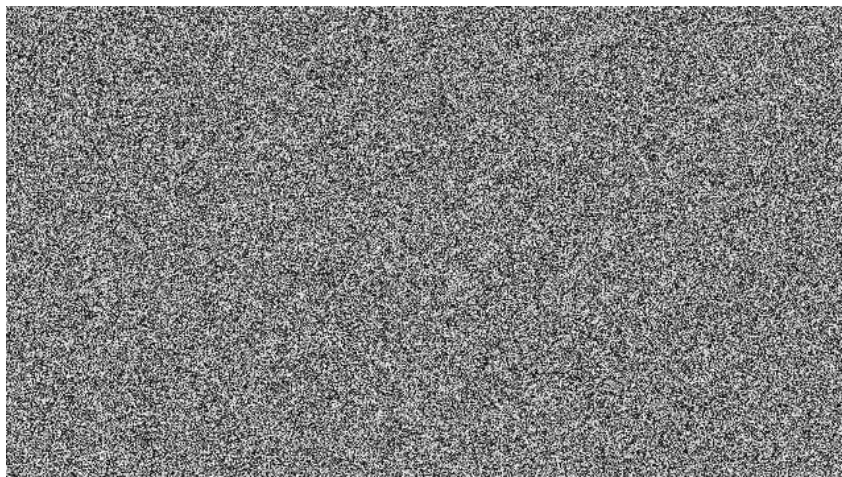


Figure 4.22: Encrypted image

4.6 Summary

In this chapter, we explored the key discrete chaotic maps, focusing on their chaotic behavior. such as the logistic, Hénon, Lozi, and Boukhalfa maps, and illustrated the onset of chaos and its fractal structure through bifurcation and attractor plots, and the evolution of Lyapunov exponents diagrams, finally, the efficiency of the Boukhalfa map in the encryption of grayscale image was rigorously demonstrated.

Conclusion and Open Perspectives

Chaos theory in discrete dynamical systems represents one of the most fascinating and profound branches of modern mathematics, as it combines deterministic structure with seemingly random behavior. Well-known chaotic maps, such as the Logistic map, the Henon, Lozi and Boukhalifa map, have demonstrated that simple mathematical formulations can produce highly complex dynamics characterized by extreme sensitivity to initial conditions, bifurcation and long term unpredictability. This inherent complexity has made such systems powerful tools for understanding natural phenomena and has opened wide horizons for advanced practical applications.

In this context, the application of chaos theory to cryptography has emerged as a prominent and rapidly developing research direction. The intrinsic properties of chaotic systems such as high sensitivity pseudo-randomness, and strong mixing provide a solid foundation for designing efficient encryption algorithms. Chaotic sequences can be employed to generate complex encryption keys or to perform permutation and substitution operations on data, particularly in image and multimedia encryption, where large volumes of structured data must be processed securely.

Despite the significant progress achieved, several challenges remain, particularly regarding the theoretical security of such systems. Issues related to finite precision, quantization, and digital implementation may degrade chaotic behavior or lead to undesirable periodicity. Moreover, evaluating the strength of chaos-based crypto-systems in comparison with classical cryptographic methods remains an open problem that requires more rigorous and comprehensive analytical tools.

In this framework, several promising directions for future research can be identified:

- Developing more complex discrete chaotic models that are resistant to statistical and analytical attacks.
- Investigating the impact of quantization and finite precision on the quality of chaos and the security of encryption systems.
- Establishing a unified theoretical framework that links chaos theory with modern information security requirements.

Thus, chaos theory in discrete dynamical systems is not only a tool for understanding complexity, but also a promising foundation for developing a new generation of encryption systems that combine structural simplicity with strong security.

Bibliography

- [1] B. Aulbach and B. Kieninger, *On three definitions of chaos*, Unpublished manuscript, received April 20, 2000; revised July 18, 2000.
- [2] D. Baptista and R. Severino, *Symbolic dynamics and Lyapunov exponents for Lozi maps*, ESAIM: Proceedings, vol. 36, pp. 121–125, 2012.
- [3] D. Hamri, *Control and synchronization of chaotic systems in dimension 3 or more*, Doctoral thesis, Option: Stationary Problems, 2023.
- [4] E. Boukhalfa and T. Nouioua, *Chaotic Oscillations in a New 2-D Discrete Dynamical System with Hidden Parameter*, Bol. Soc. Paran. Mat. (3s.), vol. 43, no. 4, pp. 1–10, 2025.
- [5] E. Boukhalfa and Z. Elhadj, *Existence of super chaotic attractors in a general piecewise smooth map of the plane*, Interdisciplinary Description of Complex Systems, vol. 12, no. 1, pp. 92–98, 2014.
- [6] E. Boukhalfa, *Sur le chaos et synchronisation dans les systèmes dynamiques discrets*, PhD thesis in Applied Mathematics, 2017.
- [7] E. N. Lorenz, *The Essence of Chaos*, University of Washington Press, 1993.
- [8] G. Álvarez and S. Li, *Some basic cryptographic requirements for chaos-based cryptosystems*, International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129–2151, 2006.
- [9] H. Wen, *A review of the Hénon map and its physical interpretations*, Georgia Institute of Technology, April 21, 2014.
- [10] J. Gleick, *Chaos: Making a New Science*, Penguin Books, 1987.
- [11] L. Jouini, *Quantification et synchronisation de chaos dans les systèmes dynamiques discrets*, Thèse de Doctorat, Université de Tebessa, 2021.
- [12] M. Hénon, *A two-dimensional mapping with a strange attractor*, Communications in Mathematical Physics, vol. 50, pp. 69–77, 1976.
- [13] M. Martelli, *Introduction to discrete dynamical systems and chaos*, California State University, 1999.
- [14] Ö. Akgümüş, *Neimark–Sacker bifurcation and stability of a prey–predator system*, Unpublished manuscript, received June 18, 2020.

- [15] P. Hartman, *A lemma in the theory of structural stability of differential equations*, Proceedings of the American Mathematical Society, vol. 11, no. 4, pp. 610–620, 1960.
- [16] R. Lozi, *Survey of recent applications of the chaotic Lozi map*, Algorithms, 2023.
- [17] R. M. May, *Simple mathematical models with very complicated dynamics*, Nature, vol. 261, pp. 459–467, 1976.
- [18] S. Banerjee, *Border collision bifurcation: theory and applications*, Department of Electrical Engineering, Indian Institute of Technology, Kharagpur.
- [19] T. Yang, *A survey of chaotic secure communication systems*, International Journal of Computational Cognition, vol. 2, no. 2, pp. 81–130, 2004.
- [20] Z. Elhadj, *A new chaotic attractor from 2-D discrete mapping via border-collision period doubling scenario*, Discrete Dynamics in Nature and Society, vol. 2005, pp. 235–238, 2005.